Schlage

Electronic security

Biometric Solutions

Datasheets

Master Index

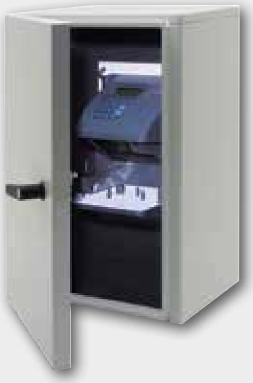
SCHLAGE

Enclosure options

for the HandKey® and HandPunch series

FX enclosure

GX enclosure



TX enclosure

Overview

Schlage biometrics provides various options to protect your HandReader from the elements. Two different, proven solutions are available to ensure your HandReaders keep performing regardless of your environment.

FX Enclosure (FX-ENCL)
Biometric HandKey Enclosure
Time & Attendance HandPunch Enclosure

Constructed from high impact UV resistant polycarbonate material, the FX Enclosure provides a degree of protection against dusty, dirty, or rainy environments. Designed for the HandKey II and the HandPunch F-Series, this enclosure can be added to an existing installation. When used with an integrated heater option (INT-HTR), it provides a comfortable heated platen against a cold climate.

GX Enclosure (GX-ENCL)
Time & Attendance HandPunch Enclosure

Designed for the HandPunch G-Series, this enclosure provides the same high degree of protection for your HandReader as the FX Enclosure.

TX Enclosure (TX-ENCL)
Biometric HandKey Enclosure

The TX Enclosure provides a higher degree of protection against dusty, dirty, or rainy environments. When used with an integrated heater option (INT-HTR), it provides a comfortable heated platen against a cold climate.

Specifications

Enclosure type	FX enclosure	GX enclosure	TX enclosure
Part number	FX-ENCL	GX-ENCL	TX-ENCL
Temperature range	-20F to 120F / -29C to 49C	-20F to 120F / -29C to 49C	-45F to 120F / -43C to 49C
Dimensions (H x W x D)	14.75 in x 12.00 in x 10.50 in 37.5 cm x 30.5 cm x 26.7 cm	14.75 in x 12.00 in x 10.50 in 37.5 cm x 30.5 cm x 26.7 cm	23.00 in x 14.00 in x 11.25 in 58.4 cm x 35.6 cm x 28.6 cm
Cross weight (including reader)	7.3 lbs / 3.3 kg	7.3lbs / 3.3 kg	45.0 lbs / 20.4 kg
HandReader models	HK-2-F3	GT-400	HK-2-F3
Heater	Factory installed option only, Model No. INT-HTR	Factory installed option only, Model No. INT-HTR	Factory installed option only, Model No. INT-HTR

About Allegion

Allegion (NYSE: ALLE) is a global pioneer in safety and security, with leading brands like CISA®, Interflex®, LCN®, Schlage® and Von Duprin®. Focusing on security around the door and adjacent areas, Allegion produces a range of solutions for homes, businesses, schools and other institutions. Allegion is a $2 billion company, with products sold in almost 130 countries. For more, visit **www.allegion.com.**

aptiQ ■ LCN ■ SCHLAGE ■ STEELCRAFT ■ VON DUPRIN

ALLEGION™

HandKey® II

Integrated with System Galaxy by Galaxy Controls

Overview

Schlage HandKey II biometric HandReader seamlessly integrates with Galaxy Controls to provide a secure and convenient biometric access control solution to meet your needs.

System Galaxy is a complete, enterprise-class access control and security management solution that offers unsurpassed ability to satisfy the requirements of any credential management, access control, or security situation. With a user interface that's easy to operate and system features that deploy in any combination, Galaxy easily fits any customer.

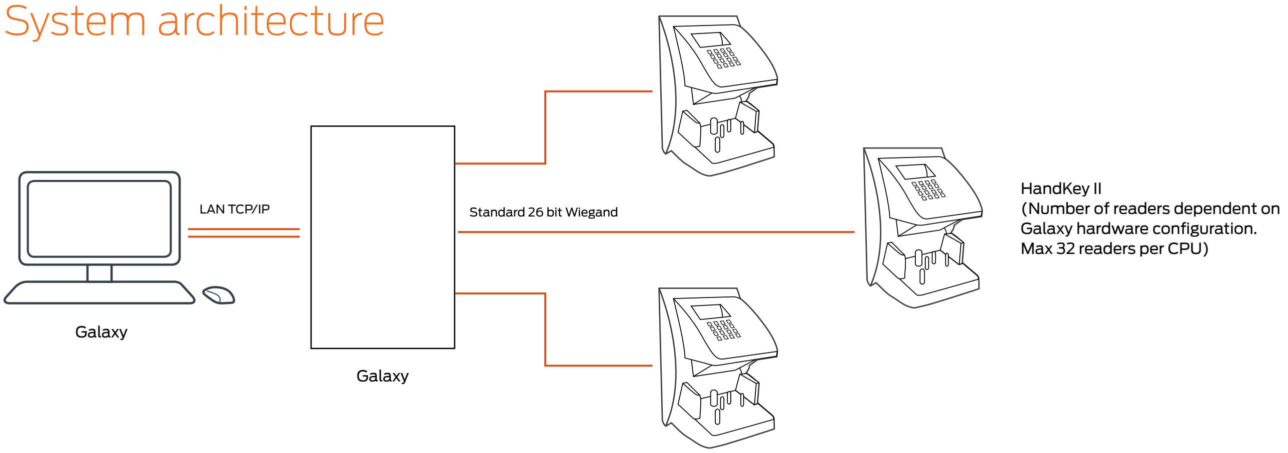
The integration of the HandKey II with Galaxy Controls allows you to add biometric security to critical access points fast, simply, and seamlessly in new and existing systems. The HandKey II measures and verifies the size and shape of a person's hand. Through the use of hand geometry, truly verify who a person is as they access a door. An optional integrated proximity or smart card reader offers multi-factor authentication to provide even higher security for the most critical applications.

Multiple mounting options are available for the HandKey II to suit the requirements of your facility. Optional enclosures provide additional protection in a variety of difficult environments and provide protection from some weather conditions.

Features and benefits

- 512 user memory, expandable up to 259,072 users
- 9 byte template
- RS485, RS422, Ethernet or Modem communications
- On the fly enrollment from any HandKey II
- HandKey II available Reader options System Galaxy:
  - Magnetic stripe
  - Proximity
  - Barcode
  - HID iCLASS®
  - MIFARE®
  - All card readers available with Card + PIN
- Power requirements: 12 to 24 VDC
- Additional enclosure options:
  - FX Enclosure for a degree of protection against dusty, dirty, or rainy environments
  - TX Enclosure for a higher degree of protection against dusty, dirty, or rainy environments
  - When used with an integrated heater option (INT-HTR), either enclosure provides a comfortable heated platen in a cold climate.

System architecture



System Capabilities

Features	
Maximum number of readers supported by controller	Up to 32
Access Granted control decision made by host or HandKey	Local controller
User support	
Maximum number of users supported	259,072
Template management	
Access control software	No
HandNet for Windows	Yes, hand templates stored in HandNet for Windows. Access decision is made at the panel.
Other system requirements	
Access control decision maker	Local controller
Readers - see supported card formats below	
Keypad	Yes
Card + PIN+ hand	Supported by special HandKey II configuration
125 kHz prox card	Yes
13.56 MHz smart card	Supported by special HandKey II configuration
HandNet for Windows Specifications	
Time zones	Available
Reports	Available
Door control	Available
Alarms	Available
Open door remotely	Available
Network readers	Available
Archive actively	Available
Remote enrollment	Available

Please contact Galaxy Controls for additional details on integrated features and credentials supported.

Supported card formats

Proximity cards (125 kHz):

- AWID®
- HID®
- Schlage®
- XceedID®

Smart cards (13.56 MHz):

- HID iCLASS®
- MIFARE®
- PIV and PIV-I compatible

For additional information contact Galaxy Controls: www.galaxysys.com or 800.445.5560

Options

The HandKey II from Schlage is built to provide the convenience and added security of a biometric solution to your access control system. Designed with your application in mind, the HandKey II can be configured with a number of options to suit your needs.

Options	Part number	Description
Memory options	N/A	User records and templates are stored at the panel
Communication options	EN-200	Field upgradable Ethernet communication module (10baseT)
	MD-500	Field upgradable internal dial up modem communication module
Card reader options	PROX	Externally top mounted HID prox reader [1]
	SC-100	MIFARE reader, externally side mounted [1]
	ICLASS	iCLASS reader**
	CR-2	Magnetic stripe reader, wall mountable
	BC-100	Bar code reader, wall mount swipe

1 Factory option only

Additional Information

For additional information contact Galaxy Controls at 800.445.5560 or visit www.galaxysys.com.

Enclosure options

Enclosures are available to protect your HandKey from the elements and to enable use regardless of your environment.

FX Enclosure

TX Enclosure

Mounting options

Schlage offers options to ensure that the HandKey can be mounted in a manner appropriate for your application.

Standard Reader comes with surface wall mount bracket

Table top secure mount for flat surfaces

This page intentionally left blank.

About Allegion

Allegion (NYSE: ALLE) creates peace of mind by pioneering safety and security. As a $2 billion provider of security solutions for homes and businesses, Allegion employs more than 8,000 people and sells products in more than 120 countries across the world. Allegion comprises 27 global brands, including strategic brands CISA®, Interflex®, LCN®, Schlage® and Von Duprin®. For more, visit **www.allegion.com.**

aptiQ ■ LCN ■ SCHLAGE ■ STEELCRAFT ■ VON DUPRIN

ALLEGION™

For additional information contact Galaxy Controls: www.galaxysys.com or 800.445.5560

NEW FEATURES
coming Spring 2016

HandKey® II

Biometric hand geometry reader

Overview

Nothing is tougher!
Our HandKey II product is ideal for applications where consistent and dependable security is of prime importance. The product is easy to maintain, and provides an ideal mix of convenience, security and peace of mind.

Top 10 reasons to select hand geometry

Field proven reliability

- Hundreds of thousands of HandKeys are installed all over the world in diverse applications, providing millions of error free transactions every day

Convenience and cost savings

- Incredibly fast installation and intuitive enrollment increases user convenience
- Verification in less than one second makes it ideal for high throughput applications
- High product quality + low maintenance costs = low total cost of ownership
- Eliminate the worry of lost, stolen or unauthorized transfer of ID cards plus the cost of purchasing and maintaining these cards

Eliminate privacy concerns

- Hand geometry technology is well accepted by end users, as there are no fingerprints or palm prints taken and the user does not leave behind any trace of their biometric data

Amazing versatility

- HandKeys can be used as standalone systems to protect critical access points that can be easily integrated into virtually every new or existing access control system in the market today
- Ability to customize user-specific security levels, time zones, holidays and languages based on your needs
- Optional access control template management software allows the HandKeys to form a system that communicates alarms and transactions in real time, provides activity reports, allows supervised on-site or remote user enrollment and expiring privileges for temporary access
- Environmental enclosures and integrated heater units make the HandKey an ideal solution for outdoor usage

Features and benefits

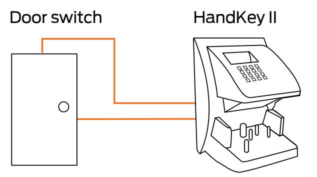
- Convenience of multiple credential options such as proximity, magnetic stripe, barcode, HID iCLASS® and MIFARE®
- Field installable Ethernet module
- Outdoor enclosure options that make the HandKey II an ideal solution for outdoor usage
- Field upgradable and expandable memory options from 512 to 259,072 users for scalable security that grows with your needs
- Three user-definable outputs to connect to auxiliary devices such as audible or silent alarms, door locks or lighting systems
- Ability to write the industry's most compact biometric template on a card instead of in a database results in higher security and unlimited user capacity
- Specially formulated antimicrobial coating with silver ions on the platen to inhibit the growth of bacteria, mold and mildew to mitigate hygiene concerns. The coating is safe and lasts for the life of the product
- Blue hand outline on the platen facilitates easy enrollment and reduces error rates during verification

Door control and monitoring

Each HandKey II is a complete, integrated door controller providing lock operation, request-for-exit and alarm monitoring. Biometric templates and decision-making capability reside locally, ensuring your doors are always secure and will continue to operate properly even if all communication to the main access control system is lost.

Standalone or fully integrated

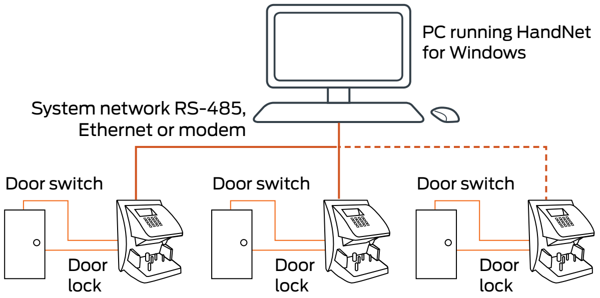
HandKey readers can be used as a stand-alone unit or as part of an integrated access control system. The units easily integrate into existing systems using the card reader emulation mode. Or, by using the HandNet software for template management, thousands of units can be linked together to form a system that communicates alarms and transactions in real time, provides activity, user and systems reports, and allows supervised user enrollment and deletions at any reader. A variety of communications options, including dial-up modems and Ethernet, allow you to design a system that's right for your facilities.



Stand-alone operation lets you provide security to a single door at an affordable price

In a network

Schlage's HandNet software links a virtually unlimited number of HandKey units into an integrated door access control system. All alarms and transactions report back in real time to the central computer, making door and alarm monitoring easy and efficient. Activity, user and system reports can be easily generated. The central computer handles all hand template management allowing supervised enrollment at any reader and system wide deletions. An optional internal modem lets you include remote site operations.


PC running HandNet for Windows
System network RS-485, Ethernet or modem
Door switch
Door lock
Door switch
Door lock
Door switch
Door lock

Base model	HandKey II
Description	HandKey with base memory for 512 users
Verification time	≤ 1 second for comparison to reference template
ID number length	1 – 10 digits
Duress code	1 leading digit, user definable
Communication	RS232: Baud rate 300 bps to 28,800 bps RS422: Baud rate 300 bps to 28,800 bps RS485: Baud rate 300 bps to 28,800 bps Optional ethernet: 10 Base T
Template Size	9 bytes
User memory	512 users field expandable up to 32,512 users Memory module upgrade up to 259,072 users
Inputs	Standard: 26 bit, 9 bit ID Wiegand Optional: Mag stripe, bar code, smart card HandKey input: Request-to-exit, door switch input, 2 auxiliary inputs
Outputs	Door control: Lock output Card reader emulation mode: Wiegand, mag stripe, bar code 1 programmable auxiliary Outputs to peripheral devices: Audible or silent alarms, door locks, lighting systems
Event monitoring	Tamper: HandKey opened or removed ID refused: User not verified after user definable number of tries exceeded Duress: User entered duress code digit Power failure: HandKey switched to optional battery power
Programmable HandKey commands	▪ Add / remove users ▪ Set global operating thresholds ▪ Set individual user data (authority or threshold levels, time zones) ▪ Transmit data from master to remote ▪ Data received by master from remote ▪ Transmit / receive data from optional software ▪ Check status of door (tamper, door monitor switch) ▪ Time zones – 62 total (2 fixed, 60 programmable) ▪ Set language ▪ Set date format, date and time ▪ Edit holidays
Antimicrobial	Available on platen
Blue hand outline	Available on platen
Dimensions H x W x D	11.65 in x 8.85 in x 8.55 in 29.6 cm x 22.5 cm x 21.7 cm
Power requirements	12 to 24 VDC or 12 to 24 VAC 50-60 Hz 7 Watts (without options)
Weight	5.3 lbs (2.4 kgs.) Without battery back-up or wall plate
Temperature	Operating: 0º - 45ºC / 32º - 113ºF ▪ Non-operating (storage): -10º - 60ºC /14º - 140ºF
Relative humidity	Operating: 20% to 80% RH non-condensing Non-operating (storage): 5% to 85% RH Non-condensing

About Allegion

Allegion (NYSE: ALLE) is a global pioneer in safety and security, with leading brands like CISA®, Interflex®, LCN®, Schlage® and Von Duprin®. Focusing on security around the door and adjacent areas, Allegion produces a range of solutions for homes, businesses, schools and other institutions. Allegion is a $2 billion company, with products sold in almost 130 countries. For more, visit **www.allegion.com.**

aptiQ ▪ LCN ▪ SCHLAGE ▪ STEELCRAFT ▪ VON DUPRIN

ALLEGION™

ALLEGION™

SCHLAGE

HandKey II

Access control system alliances

The Schlage HandKey II biometric HandReader seamlessly integrates with a number of access control software platforms to provide a secure and convenient biometric access control solution to meet your needs. The integration of the HandKey II with access control software platforms allows you to add biometric security to critical access control points fast, simply, and seamlessly in new and existing systems. The HandKey II measures and verifies the size and shape of a person's hand. Through the use of hand geometry, you can truly verify who a person is as they access a door.

HandKey II connection to access control system

Template	Wiegand
Hand template management capability via access control system. Additional user and reader capabilities supported through the software.	HandKey simulates card reader output to access control system. Hand templates managed by HandKey or HandNet(R) software via TCP/IP or RS-485.

Template partners			
AMAG TECHNOLOGY	cbord®	Heartland™ Campus Solutions ECSI	InnoSoft
Lenel	OPEN OPTIONS™ ACCESS TECHNOLOGY	RS2® Technologies	
Wiegand partners			
BadgePass™ Revolutionizing ID	Continental Access A Napco Security Group Company	GALAXY	HAMILTON SAFE®
Honeywell	PCSC	SOFTWARE HOUSE	VANDERBILT INDUSTRIES

HandKey II Overview

Nothing is tougher!

Our HandKey II product is ideal for applications where consistent and dependable security is of prime importance. The product is easy to maintain, and provides an ideal mix of convenience, security and peace of mind.

Top 10 reasons to select Hand Geometry

Field proven reliability

- Hundreds of thousands of HandKeys are installed all over the world in diverse applications providing millions of error free transactions every day

Convenience and cost savings

- Incredibly fast installation and intuitive enrollment increases user convenience
- Verification in less than one second makes it ideal for high throughput applications
- High product quality + low maintenance costs = Low total cost of ownership
- Eliminate the worry of lost, stolen or unauthorized transfer of ID cards plus the cost of purchasing and maintaining these cards

Eliminate privacy concerns

- Hand Geometry technology is well accepted by end users as there are no fingerprints or palm prints taken and the user does not leave behind any trace of their biometric data

Amazing versatility

- HandKeys can be used as standalone systems to protect critical access points that can be easily integrated into virtually every new or existing access control system in the market today
- Ability to customize user-specific security levels, time zones, holidays and languages based on your needs
- Optional access control template management software allows the HandKeys to form a system that communicates alarms and transactions in real time, provides activity reports, allows supervised on-site or remote user enrollment and expiring privileges for temporary access
- Environmental enclosures and integrated heater units make the HandKey an ideal solution for outdoor usage

Basic specificaitons

Base model	HandKey II
Description	HandKey with base memory for 512 users
Verification time	≤ 1 second for comparison to reference template
ID number length	1-10 digits
Duress code	1 leading digit, user definable
Communication	RS232: Baud rate 300 bps to 28,000 bps RS422: Baud rate 300 bps to 28,000 bps RS485: Baud rate 300 bps to 28,800 bps Optional modem: Baud rate 300 bps to 14,400 bps Optional ethernet: 10 Base T
Template size	9 bytes
User memory	512 users field expandable up to 32,512 users Memory module upgrade up to 259,072 users
Antimicrobial	Available on platen
Blue hand outline	Available on platen
Dimensions H x W x D	11.65 in x 8.85 in x 8.55 in 29.6 cm x 22.5 cm x 21.7 cm
Power requirements	12 to 24 VDC or 12 to 24 VAC 50-60 Hz 7 Watts (without options)
Weight	5.3 lbs (2.4 kgs.) Without battery back-up or wall plate
Temperature	Operating: 0º - 45ºC / 32º - 113ºF Non-operating (storage): -10º - 60ºC / 14º - 140ºF
Relative humidity	Operating: 20% to 80% RH non-condensing Non-operating (storage): 5% to 85% RH Non-condensing

About Allegion

Allegion (NYSE: ALLE) creates peace of mind by pioneering safety and security. As a $2 billion provider of security solutions for homes and businesses, Allegion employs more than 8,000 people and sells products in more than 120 countries across the world. Allegion comprises 27 global brands, including strategic brands CISA®, Interflex®, LCN®, Schlage® and Von Duprin®. For more, visit **www.allegion.com.**

aptiQ ■ LCN ■ SCHLAGE ■ STEELCRAFT ■ VON DUPRIN

ALLEGION™

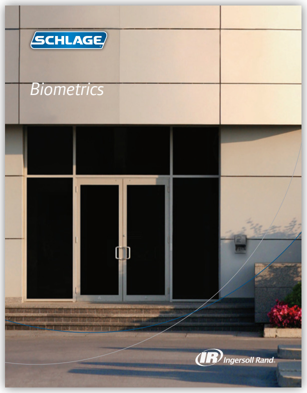
Biometric HandKey II Resources

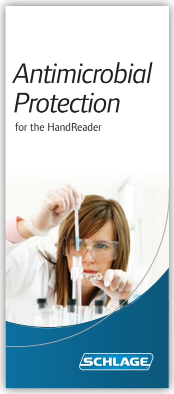
Literature

biometrics.schlage.com

CLICK HERE

Utilize the search bar on the biometrics page link above to find each piece of literature by typing the parenthesized document number. For the online version, each literature title is a link to that piece.





Brochures:

- Solutions for K-12 Schools and Day Care Centers (109582)
- Biometrics Brochure (109090)
- Antimicrobial Brochure (100453)
- Biometric HandKey II FAQ (106210)
- HandReader Concerns (106228)

Data Sheets:

- HandKey II (104535)
- Quick Reference Sheet (104397)
- Terminal Options (104400)
- Enclosure Options (104398)

Case Studies:

Available under the Downloads Tab of the biometrics link above

Distributor Tools

My Security Technologies Portal

CLICK HERE

Registered Users

Biometrics information can be found at: Products > Biometrics

- Resources available only to registered partners include
  - Pricebooks
  - Selling Guides
  - FAQs
  - Product Notifications
  - And more!

New Users

The portal is only accessible to registered users. Contact your company's portal administrator or your local sales representative to request access

Ingersoll Rand
Security Technologies

Biometric HandKey II Resources

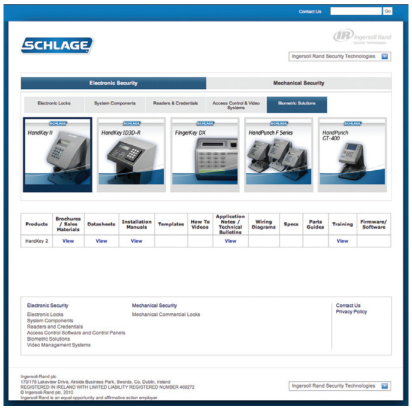
Training

YouTube and schlage.com/support

CLICK HERE

Manuals:
Available under the Installation Manuals tab on the support page link above

- HandKey II Manual (106238)
- HandNet for Windows Manual (105141)
- HandNet Lite Manual (106221)
- TM-100 Installation (109425)


Contact Us Go

Ingersoll Rand Security Technologies

Electronic Security | Mechanical Security

Electronic Locks | System Components | Readers & Credentials | Access Control & Video Systems | Biometric Solutions

HandKey II | HandKey ID3D-R | FingerKey DX | HandPunch F Series | HandPunch GT-400

Products	Brochures / Sales Materials	Datasheets	Installation Manuals	Templates	How To Videos	Application Notes / Technical Bulletins	Wiring Diagrams	Specs	Parts Guides	Training	Firmware/ Software
HandKey 2	View	View	View			View				View	

Electronic Security
Electronic Locks
System Components
Readers and Credentials
Access Control Software and Control Panels
Biometric Solutions
Video Management Systems

Mechanical Security
Mechanical Commercial Locks

Contact Us
Privacy Policy

Ingersoll-Rand plc
170/175 Lakeview Drive, Airside Business Park, Swords, Co. Dublin, Ireland
REGISTERED IN IRELAND WITH LIMITED LIABILITY REGISTERED NUMBER 469272
© Ingersoll-Rand plc, 2010
Ingersoll Rand is an equal opportunity and affirmative action employer.

Ingersoll Rand Security Technologies

Courses:
Available under the Training tab on the support page link above

- HandKey Hardware Course (106526)
- HandNet for Windows Software Course (106527)
- Access Control Training Course Outline (102872)

YouTube (Ingersoll RandST & Schlage Security):

- How a HandReader Works
- HandReader Installed in IBX
- How to Clean the Platen

Time & Attendance by Ingersoll RandST

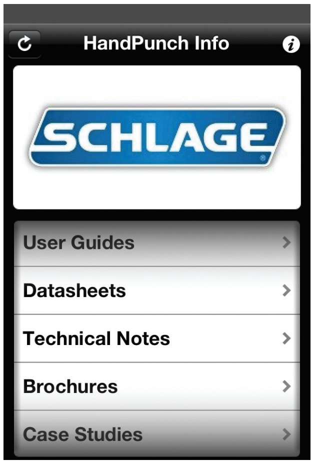
1:07 / 2:25

Technical Documents:

- HandNet Software (105365)
- HandKey II Biometric Reader Specification (105364)
- Electronic Access Control Catalog
- Additional documents available under the Application Notes tab on the support page link above

Additional Resources

- Schlage Electronics How-To App
  - How-To Videos
  - User Guides
  - Installation Guides
  - Data Sheets
  - Tech Notes
- Contact Us at Security Technologies > Contact Us
- Technical Library at schlage.com/support


HandPunch Info

User Guides

Datasheets

Technical Notes

Brochures

Case Studies

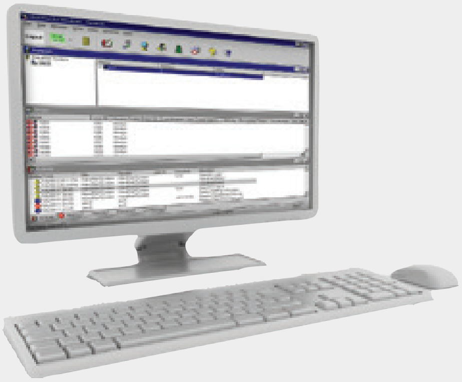
Available in Android Market

Available on the App Store

Ingersoll Rand
Security Technologies

HandNet®

for Windows



Overview

HandNet for Windows lets you control and monitor a network of HandKey readers. With just one comprehensive program, you can monitor activity and alarms on all readers, and control the access of each user.

Features and benefits

- Automatic hand template management feature allows template distribution from an enrollment HandKey to other selected HandKeys thus eliminating the need for a user to be enrolled at every HandReader
- Independent door control capability without the need for an access control panel
- Monitor multiple remote sites from the convenience of your PC
- Remote enrollment feature enables a HandKey to be controlled from the software. For example, a guard behind a glass partition or a supervisor in a distant office can enroll new users without physically going to the HandKey
- Assign temporary access to selected users by specifying a user's access start and stop days and times
- Manage archive activity to keep old information
available for reports
- Manage alarms for additional security

Specifications	HandNet For Windows	HandNet Lite
Computer	Intel Pentium 1 GHz or higher, AMD Athlon 1GHz or higher	Intel Pentium 1 GHz or higher, AMD Athlon 1 GHz or higher
Operating system	▪ Windows XP SP3 32-bit ▪ Windows 7 Professional SP1 32-bit and 64-bit ▪ Windows 8 Professional 32-bit and 64-bit	▪ Windows XP SP3 32-bit ▪ Windows 7 Professional SP1 32-bit and 64-bit ▪ Windows Server 2003 SP3 32-bit ▪ Windows 8 Professional 32-bit and 64-bit
Hard disk	2 GB minimum, 1 GB Free space	60 GB minimum, 10 GB free space
Monitor	Minimum resolution 1024 x 768	Minimum resolution 1024 x 768
Memory	2 GB (minimum 1 GB)	4 GB (minimum 2 GB)
Database	MS Access	MS SQL Server 2000 MSDE
Products supported	HK-2-F3	HK-2-F3
Template managements	Available	Available
Supported communications	RS232, RS485, Ethernet	RS232, RS485, Ethernet
Time zones	Available	Available
Reports	Available	Limited – use reports from an access control panel
Door control	Available	NA – use panel door control
Alarms	Available	NA – use panel alarms
Open door remotely	Available	NA – use panel door control
Network readers	Available	Available
Archive activity	Available	Available – database backup
Remote enrollment	Available	Available

Options

- **HN-2-T1** - Manages up to 5 HandKeys
- **HN-2-T2 -** Manages up to 25 HandKeys
- **HN-2-T3 -** Manages an unlimited number of HandKeys
- **HandNet Lite -** Software program to manage up to 64 HandKeys

About Allegion

Allegion (NYSE: ALLE) is a global pioneer in safety and security, with leading brands like CISA®, Interflex®, LCN®, Schlage® and Von Duprin®. Focusing on security around the door and adjacent areas, Allegion produces a range of solutions for homes, businesses, schools and other institutions. Allegion is a $2 billion company, with products sold in almost 130 countries. For more, visit **www.allegion.com.**

aptiQ ▪ LCN ▪ SCHLAGE ▪ STEELCRAFT ▪ VON DUPRIN

ALLEGION™

Biometric terminal options and accessories

for HandKey®

Schlage offers a number of accessories for access control HandReader terminals. From networking options to memory expansions, we'll help you create the solution to meet your specific needs.

Base Model	HandKey II
Card readers	▪ **PROX:** Externally top mounted HID proximity reader, factory option only ▪ **SC-100:** Mifare Classic (r) reader, factory option only ▪ **iCLASS®**: HID Legacy iCLASS reader, factory option only ▪ **CR-2**: Mag stripe wall mount card reader ▪ **BC-100**: Bar code reader, wall mount swipe
Memory	▪ **EM-801-F3**: Field upgradable memory expansion up to 9,728 users ▪ **EM-803-F3**: Field upgradable memory expansion up to 32,512 users
Communication	▪ **EN-201:** Field upgradeable Ethernet communication module 10baseT ▪ **MD-500:** Internal dial-up modem
Power options	▪ **PS-110**: Power supply, 120VAC to 13.5 VDC ▪ **PS-220**: Power supply, 220VAC to 13.5 VDC ▪ **BB-250**: Optional battery backup
Mounting	▪ **TM-100**: Table top secure mount for flat surfaces
Left hand option	▪ NA
Network accessories	▪ **DC-102**: Data converter for 4 wire system, RS-232 to RS-422 with 120V, 60Hz power supply ▪ **DC-102 with 220V**, 50Hz power supply

This page intentionally left blank.

© 2016 Allegion
004400, Rev. 07/16
www.allegion.com

SCHLAGE

Enclosure options

for the HandKey® and HandPunch series

FX enclosure

GX enclosure

TX enclosure

Overview

Schlage biometrics provides various options to protect your HandReader from the elements. Two different, proven solutions are available to ensure your HandReaders keep performing regardless of your environment.

FX Enclosure (FX-ENCL)

Biometric HandKey Enclosure
Time & Attendance HandPunch Enclosure

Constructed from high impact UV resistant polycarbonate material, the FX Enclosure provides a degree of protection against dusty, dirty, or rainy environments. Designed for the HandKey II and the HandPunch F-Series, this enclosure can be added to an existing installation. When used with an integrated heater option (INT-HTR), it provides a comfortable heated platen against a cold climate.

GX Enclosure (GX-ENCL)

Time & Attendance HandPunch Enclosure

Designed for the HandPunch G-Series, this enclosure provides the same high degree of protection for your HandReader as the FX Enclosure.

TX Enclosure (TX-ENCL)

Biometric HandKey Enclosure

The TX Enclosure provides a higher degree of protection against dusty, dirty, or rainy environments. When used with an integrated heater option (INT-HTR), it provides a comfortable heated platen against a cold climate.

Specifications

Enclosure type	FX enclosure	GX enclosure	TX enclosure
Part number	FX-ENCL	GX-ENCL	TX-ENCL
Temperature range	-20F to 120F / -29C to 49C	-20F to 120F / -29C to 49C	-45F to 120F / -43C to 49C
Dimensions (H x W x D)	14.75 in x 12.00 in x 10.50 in 37.5 cm x 30.5 cm x 26.7 cm	14.75 in x 12.00 in x 10.50 in 37.5 cm x 30.5 cm x 26.7 cm	23.00 in x 14.00 in x 11.25 in 58.4 cm x 35.6 cm x 28.6 cm
Cross weight (including reader)	7.3 lbs / 3.3 kg	7.3lbs / 3.3 kg	45.0 lbs / 20.4 kg
HandReader models	HK-2-F3	GT-400	HK-2-F3
Heater	Factory installed option only, Model No. INT-HTR	Factory installed option only, Model No. INT-HTR	Factory installed option only, Model No. INT-HTR

About Allegion

Allegion (NYSE: ALLE) is a global pioneer in safety and security, with leading brands like CISA®, Interflex®, LCN®, Schlage® and Von Duprin®. Focusing on security around the door and adjacent areas, Allegion produces a range of solutions for homes, businesses, schools and other institutions. Allegion is a $2 billion company, with products sold in almost 130 countries. For more, visit **www.allegion.com.**

aptiQ ■ LCN ■ SCHLAGE ■ STEELCRAFT ■ VON DUPRIN

ALLEGION™

HandKey® ID3D-R

Biometric Hand Geometry Reader

Nothing is tougher!

At Schlage biometrics we know that every product you specify has to stand up to constant use and abuse. The all-metal HandKeys ID3D-R and ID3D-RW are able to withstand the rigors of daily use and abuse without fail.

Top 10 reasons to select Hand Geometry

FIELD PROVEN RELIABILITY

1. Hundreds of thousands of HandKeys are installed all over the world in diverse applications providing millions of error free transactions every day

CONVENIENCE AND COST SAVINGS

2. Incredibly fast installation & intuitive enrollment increases user convenience
3. Verification in less than 1 second makes it ideal for high throughput applications
4. High product quality + Low maintenance costs = Low total cost of ownership
5. Eliminate the worry of lost, stolen or unauthorized transfer of ID cards plus the cost of purchasing and maintaining these cards

ELIMINATE PRIVACY CONCERNS

6. Hand Geometry technology is well accepted by end users as there are NO fingerprints or palm prints taken and the user does not leave behind any trace of their biometric data

AMAZING VERSATILITY

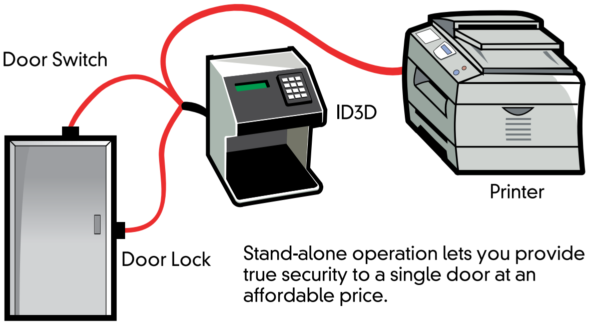
7. HandKeys can be used as standalone systems to protect critical access points that can be easily integrated into virtually every new or existing access control system in the market today
8. Ability to customize user specific security levels, time zones, holidays and languages based on your needs
9. Optional access control template management software allows the HandKeys to form a system that communicates alarms and transactions in real time, provides activity reports, allows supervised on-site or remote user enrollment and expiring privileges for temporary access
10. Environmental enclosures and integrated heater units make the HandKey an ideal solution for outdoor usage

Features and Benefits

- All-metal housing for increased durability and toughness
- Left handed configuration option for drive-through applications and entrance gates
- Recess-mount option for reduced obstruction at high traffic areas
- Convenience of multiple credential options such as magnetic stripe, bar code
- Integrated unit with heater and enclosure makes ID3D-RW ideal for outdoor environments
- Two user definable outputs to connect to auxiliary devices such as audible or silent alarms, door locks or lighting systems

Stand Alone System

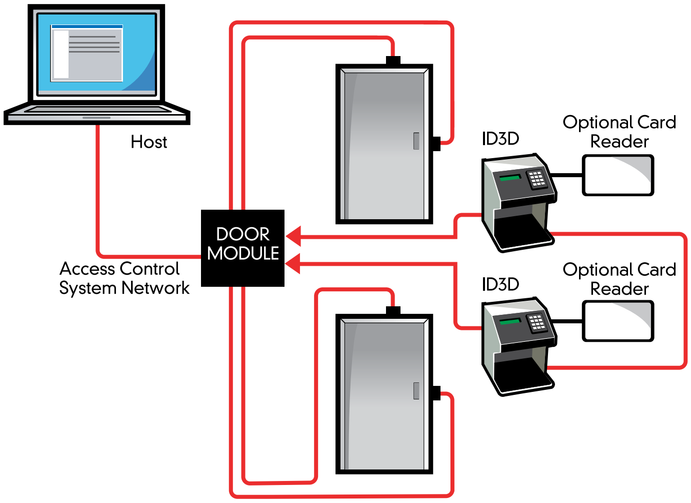
The HandKey can operate as a complete stand-alone access control station. Door lock operation and alarm monitoring of the door status is provided. An external alarm circuit is included for operating an audio or visual alarm.



Stand-alone operation lets you provide true security to a single door at an affordable price.

Third Party System Interface

The HandKey can easily be integrated into new or existing third party access control systems using its card reader emulation output. All Wiegand, proximity and magnetic stripe formats can be accommodated. No modifications are needed to the third party system. The HandKeys can be interconnected via RS-485 twisted pair for hand data transfer.

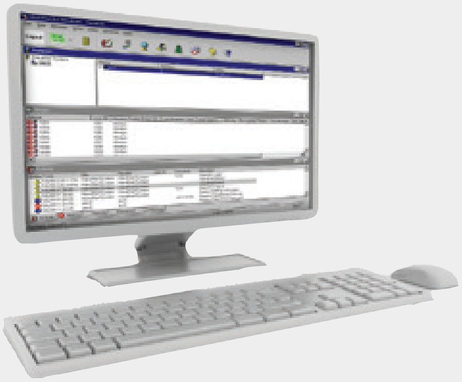


Base Model	ID3D-R / ID3D-RW
Description	HandKey with base memory for 256 users
Verification Time	≤ 1 second for comparison to reference template
ID Number Length	1 – 10 digits
Duress Code	1 leading digit, user definable
Communication	RS232 (Printer output only): Baud rate 300 bps to 19,200 bps RS422: Baud rate 300 bps to 19,200 bps RS485: Baud rate 300 bps to 19,200 bps Optional Ethernet: 10 Base T
Template Size	9 bytes
User Memory	256 users expandable to 27,904 users
Inputs	Standard: 26 bit, 9 bit ID Wiegand Optional: Mag stripe, bar code HandKey Input: Request to Exit, Door switch input, 1 Auxilary input
Outputs	Door control: Lock output Card reader emulation mode: Wiegand, mag stripe, bar code 1 programmable auxiliary Outputs to peripheral devices: Audible or silent alarms, door locks, lighting systems
Event Monitoring	Tamper: HandKey opened or removed ID refused: User not verified after user definable number of tries exceeded Duress: User entered duress code digit Power failure: HandKey switched to optional battery power
Programmable HandKey Commands	· Add / remove users · Set global operating thresholds · Set individual user data (authority or threshold levels, time zones) · Transmit data from Master to Remote · Data received by Master from Remote · Transmit / receive data from optional software · Check status of door (Tamper, Door monitor switch) · Time zones – 62 total (2 fixed, 60 programmable) · Set language · Set date format, date and time · Edit holidays
Antimicrobial	NA
Blue Hand Outline	NA
Dimensions HxWxD	8.30 in. x 6.50 in. x 7.17 in. (ID3D-R Dimensions) 21.3 cm x 16.5 cm x 18.7 cm (ID3D-R Dimensions)
Power Requirements	12 to 24 VDC or 12 to 24 VAC 50-60 Hz 7 Watts (without options)
Weight	7.2 lbs. (3.3 kgs.) (Without back plate)
Temperature	Operating: 0 deg C to +45 deg C / 32 deg F to 113 deg F Non-Operating (Storage): -10 deg C to +60 deg C / 14 deg F to 140 deg F
Relative Humidity	Operating: 20% to 80% RH Non-condensing Non-operating (Storage): 5% to 85% RH Non-condensing

Ingersoll Rand
Security Technologies

HandNet®

for Windows



Overview

HandNet for Windows lets you control and monitor a network of HandKey readers. With just one comprehensive program, you can monitor activity and alarms on all readers, and control the access of each user.

Features and benefits

- Automatic hand template management feature allows template distribution from an enrollment HandKey to other selected HandKeys thus eliminating the need for a user to be enrolled at every HandReader
- Independent door control capability without the need for an access control panel
- Monitor multiple remote sites from the convenience of your PC
- Remote enrollment feature enables a HandKey to be controlled from the software. For example, a guard behind a glass partition or a supervisor in a distant office can enroll new users without physically going to the HandKey
- Assign temporary access to selected users by specifying a user's access start and stop days and times
- Manage archive activity to keep old information
  available for reports
- Manage alarms for additional security

Specifications	HandNet For Windows	HandNet Lite
Computer	Intel Pentium 1 GHz or higher, AMD Athlon 1GHz or higher	Intel Pentium 1 GHz or higher, AMD Athlon 1 GHz or higher
Operating system	▪ Windows XP SP3 32-bit ▪ Windows 7 Professional SP1 32-bit and 64-bit ▪ Windows 8 Professional 32-bit and 64-bit	▪ Windows XP SP3 32-bit ▪ Windows 7 Professional SP1 32-bit and 64-bit ▪ Windows Server 2003 SP3 32-bit ▪ Windows 8 Professional 32-bit and 64-bit
Hard disk	2 GB minimum, 1 GB Free space	60 GB minimum, 10 GB free space
Monitor	Minimum resolution 1024 x 768	Minimum resolution 1024 x 768
Memory	2 GB (minimum 1 GB)	4 GB (minimum 2 GB)
Database	MS Access	MS SQL Server 2000 MSDE
Products supported	HK-2-F3	HK-2-F3
Template managements	Available	Available
Supported communications	RS232, RS485, Ethernet	RS232, RS485, Ethernet
Time zones	Available	Available
Reports	Available	Limited – use reports from an access control panel
Door control	Available	NA – use panel door control
Alarms	Available	NA – use panel alarms
Open door remotely	Available	NA – use panel door control
Network readers	Available	Available
Archive activity	Available	Available – database backup
Remote enrollment	Available	Available

Options

- **HN-2-T1** - Manages up to 5 HandKeys
- **HN-2-T2 -** Manages up to 25 HandKeys
- **HN-2-T3 -** Manages an unlimited number of HandKeys
- **HandNet Lite -** Software program to manage up to 64 HandKeys

Allegion, the Allegion logo, Schlage, the Schlage logo, and HandKey are trademarks of Allegion plc, its subsidiaries and/or affiliates in the United States and other countries. All other trademarks are the property of their respective owners.

© 2016 Allegion
004399, Rev. 07/16
www.allegion.com/us

Biometric terminal options and accessories

for HandKey®

Schlage offers a number of accessories for access control HandReader terminals. From networking options to memory expansions, we'll help you create the solution to meet your specific needs.

Base Model	HandKey II
Card readers	▪ **PROX:** Externally top mounted HID proximity reader, factory option only ▪ **SC-100:** Mifare Classic (r) reader, factory option only ▪ **iCLASS®**: HID Legacy iCLASS reader, factory option only ▪ **CR-2**: Mag stripe wall mount card reader ▪ **BC-100**: Bar code reader, wall mount swipe
Memory	▪ **EM-801-F3**: Field upgradable memory expansion up to 9,728 users ▪ **EM-803-F3**: Field upgradable memory expansion up to 32,512 users
Communication	▪ **EN-201:** Field upgradeable Ethernet communication module 10baseT ▪ **MD-500:** Internal dial-up modem
Power options	▪ **PS-110**: Power supply, 120VAC to 13.5 VDC ▪ **PS-220**: Power supply, 220VAC to 13.5 VDC ▪ **BB-250**: Optional battery backup
Mounting	▪ **TM-100**: Table top secure mount for flat surfaces
Left hand option	▪ NA
Network accessories	▪ **DC-102**: Data converter for 4 wire system, RS-232 to RS-422 with 120V, 60Hz power supply ▪ **DC-102 with 220V**, 50Hz power supply

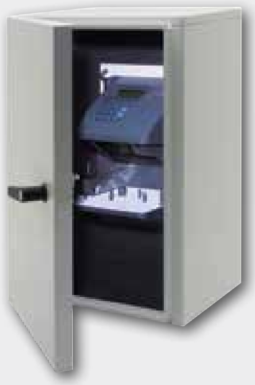
This page intentionally left blank.

Enclosure options

for the HandKey® and HandPunch series

FX enclosure

GX enclosure



TX enclosure

Overview

Schlage biometrics provides various options to protect your HandReader from the elements. Two different, proven solutions are available to ensure your HandReaders keep performing regardless of your environment.

FX Enclosure (FX-ENCL)
Biometric HandKey Enclosure
Time & Attendance HandPunch Enclosure

Constructed from high impact UV resistant polycarbonate material, the FX Enclosure provides a degree of protection against dusty, dirty, or rainy environments. Designed for the HandKey II and the HandPunch F-Series, this enclosure can be added to an existing installation. When used with an integrated heater option (INT-HTR), it provides a comfortable heated platen against a cold climate.

GX Enclosure (GX-ENCL)
Time & Attendance HandPunch Enclosure

Designed for the HandPunch G-Series, this enclosure provides the same high degree of protection for your HandReader as the FX Enclosure.

TX Enclosure (TX-ENCL)
Biometric HandKey Enclosure

The TX Enclosure provides a higher degree of protection against dusty, dirty, or rainy environments. When used with an integrated heater option (INT-HTR), it provides a comfortable heated platen against a cold climate.

Specifications

Enclosure type	FX enclosure	GX enclosure	TX enclosure
Part number	FX-ENCL	GX-ENCL	TX-ENCL
Temperature range	-20F to 120F / -29C to 49C	-20F to 120F / -29C to 49C	-45F to 120F / -43C to 49C
Dimensions (H x W x D)	14.75 in x 12.00 in x 10.50 in 37.5 cm x 30.5 cm x 26.7 cm	14.75 in x 12.00 in x 10.50 in 37.5 cm x 30.5 cm x 26.7 cm	23.00 in x 14.00 in x 11.25 in 58.4 cm x 35.6 cm x 28.6 cm
Cross weight (including reader)	7.3 lbs / 3.3 kg	7.3lbs / 3.3 kg	45.0 lbs / 20.4 kg
HandReader models	HK-2-F3	GT-400	HK-2-F3
Heater	Factory installed option only, Model No. INT-HTR	Factory installed option only, Model No. INT-HTR	Factory installed option only, Model No. INT-HTR

About Allegion

Allegion (NYSE: ALLE) is a global pioneer in safety and security, with leading brands like CISA®, Interflex®, LCN®, Schlage® and Von Duprin® Focusing on security around the door and adjacent areas, Allegion produces a range of solutions for homes, businesses, schools and other institutions. Allegion is a $2 billion company, with products sold in almost 130 countries. For more, visit **www.allegion.com.**

aptiQ ■ LCN ■ SCHLAGE ■ STEELCRAFT ■ VON DUPRIN

ALLEGION™

FingerKey® DX Series

Fingerprint Readers

Fingerprint

The FingerKey product measures unique fingerprint pattern characteristics to verify the person's identity.
In conjunction with a pin or smart card, the enrolled individual can gain access to the facility.

How to verify

- Enter ID
- Place finger on sensor using ridge lock to ensure correct placement
- Optical sensor captures an image of your fingerprint
- Algorithm extracts unique points from the image
- Algorithm then converts the data into a unique mathematical template
- FingerKey compares the information with the original template
- User's identity verified and their access control privileges checked

Style, quality and lots of options

With the FingerKeys, your fingerprint

is your credential for reliable one to one matching.

- High quality optical sensor
- Stylish terminal with keypad and LCD easily blends into any environment
- Various options for external card reader inputs
- Flexibility to write template on smart card instead of on a database for higher security and unlimited user population
- Field upgradeable and expandable memory options from 250 to 2,000 users for scalable security that grows with your needs
- Configurable Wiegand output to suit your specific needs
- Field upgradeable Ethernet
- Tough polycarbonate construction

Models	DX-2000	DX-2100	DX-2200	DX-2400
Description	FingerKey with 250 user memory	FingerKey with integrated HID Prox. reader	FingerKey with integrated HID iClass reader	FingerKey with integrated MIFARE or Desfire reader

Ingersoll Rand
Security Technologies

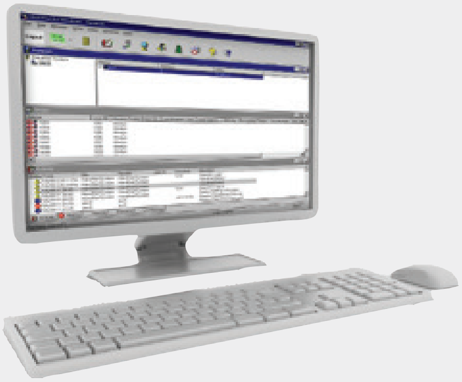
Base Model	DX-2000
Description	Fingerprint reader with base memory for 250 users
Verification Time	≤ to 2 seconds for comparison to reference template
ID Number Length	1 – 15 digits
Duress Code	Alternate finger
Communication	RS-232: Baud rate 4900 to 57600 bps RS-422: Baud rate 4900 to 57600 bps Optional Ethernet: 10 Base T
Template Size	400 bytes per template, 2 templates per finger
User Memory	250 users expandable to 2,000 users
Inputs	Card reader inputs: Standard: 26 bit, 9 bit ID Wiegand Optional: Mag stripe, bar code, smart card
Outputs	Card reader emulation mode: Wiegand, mag stripe
Event Monitoring	Tamper: FingerKey opened or removed ID refused: User not verified after user definable number of tries exceeded Duress: User entered duress code digit
Programmable FingerKey Commands	· Add / remove users · Set global operating thresholds · Set individual user data (authority or threshold levels, time zones) · Transmit data from Master to Remote · Data received by Master from Remote · Transmit / receive data from optional software · Check status of door (Tamper, Door monitor switch) · Set language
Antimicrobial	NA
Blue Hand Outline	NA
Dimensions WxHxD	5.31 in. x 5.03 in. x 2.98 in. 13.49 cm x 12.78 cm x 7.57 cm
Power Requirements	12 VDC +- 10% reg. 0.5A max
Weight	1.00 lbs (0.45 kgs)
Temperature	Operating: 0 deg C to + 45 deg C / 32 deg F to 113 deg F Non-Operating (Storage): -10 deg C to + 60 deg C
Relative Humidity	Operating: 20% to 80% RH Non-condensing Non-operating (Storage): 5% to 85% RH Non-condensing

HandKey® is a registered trademark of Schlage. Specifications subject to change. Please check with your system vendor for details.

IR Ingersoll Rand
Security Technologies

HandNet®

for Windows



Overview

HandNet for Windows lets you control and monitor a network of HandKey readers. With just one comprehensive program, you can monitor activity and alarms on all readers, and control the access of each user.

Features and benefits

- Automatic hand template management feature allows template distribution from an enrollment HandKey to other selected HandKeys thus eliminating the need for a user to be enrolled at every HandReader
- Independent door control capability without the need for an access control panel
- Monitor multiple remote sites from the convenience of your PC
- Remote enrollment feature enables a HandKey to be controlled from the software. For example, a guard behind a glass partition or a supervisor in a distant office can enroll new users without physically going to the HandKey
- Assign temporary access to selected users by specifying a user's access start and stop days and times
- Manage archive activity to keep old information
  available for reports
- Manage alarms for additional security

Specifications	HandNet For Windows	HandNet Lite
Computer	Intel Pentium 1 GHz or higher, AMD Athlon 1GHz or higher	Intel Pentium 1 GHz or higher, AMD Athlon 1 GHz or higher
Operating system	▪ Windows XP SP3 32-bit ▪ Windows 7 Professional SP1 32-bit and 64-bit ▪ Windows 8 Professional 32-bit and 64-bit	▪ Windows XP SP3 32-bit ▪ Windows 7 Professional SP1 32-bit and 64-bit ▪ Windows Server 2003 SP3 32-bit ▪ Windows 8 Professional 32-bit and 64-bit
Hard disk	2 GB minimum, 1 GB Free space	60 GB minimum, 10 GB free space
Monitor	Minimum resolution 1024 x 768	Minimum resolution 1024 x 768
Memory	2 GB (minimum 1 GB)	4 GB (minimum 2 GB)
Database	MS Access	MS SQL Server 2000 MSDE
Products supported	HK-2-F3	HK-2-F3
Template managements	Available	Available
Supported communications	RS232, RS485, Ethernet	RS232, RS485, Ethernet
Time zones	Available	Available
Reports	Available	Limited – use reports from an access control panel
Door control	Available	NA – use panel door control
Alarms	Available	NA – use panel alarms
Open door remotely	Available	NA – use panel door control
Network readers	Available	Available
Archive activity	Available	Available – database backup
Remote enrollment	Available	Available

Options

- **HN-2-T1** - Manages up to 5 HandKeys
- **HN-2-T2 -** Manages up to 25 HandKeys
- **HN-2-T3 -** Manages an unlimited number of HandKeys
- **HandNet Lite -** Software program to manage up to 64 HandKeys

About Allegion

Allegion (NYSE: ALLE) is a global pioneer in safety and security, with leading brands like CISA®, Interflex®, LCN®, Schlage® and Von Duprin®. Focusing on security around the door and adjacent areas, Allegion produces a range of solutions for homes, businesses, schools and other institutions. Allegion is a $2 billion company, with products sold in almost 130 countries. For more, visit **www.allegion.com.**

aptiQ ■ LCN ■ SCHLAGE ■ STEELCRAFT ■ VON DUPRIN

ALLEGION™

Biometric terminal options and accessories

for HandKey®

Schlage offers a number of accessories for access control HandReader terminals. From networking options to memory expansions, we'll help you create the solution to meet your specific needs.

Base Model	HandKey II
Card readers	▪ **PROX:** Externally top mounted HID proximity reader, factory option only ▪ **SC-100:** Mifare Classic (r) reader, factory option only ▪ **iCLASS®**: HID Legacy iCLASS reader, factory option only ▪ **CR-2**: Mag stripe wall mount card reader ▪ **BC-100**: Bar code reader, wall mount swipe
Memory	▪ **EM-801-F3**: Field upgradable memory expansion up to 9,728 users ▪ **EM-803-F3**: Field upgradable memory expansion up to 32,512 users
Communication	▪ **EN-201:** Field upgradeable Ethernet communication module 10baseT ▪ **MD-500:** Internal dial-up modem
Power options	▪ **PS-110**: Power supply, 120VAC to 13.5 VDC ▪ **PS-220**: Power supply, 220VAC to 13.5 VDC ▪ **BB-250**: Optional battery backup
Mounting	▪ **TM-100**: Table top secure mount for flat surfaces
Left hand option	▪ NA
Network accessories	▪ **DC-102**: Data converter for 4 wire system, RS-232 to RS-422 with 120V, 60Hz power supply ▪ **DC-102 with 220V**, 50Hz power supply

This page intentionally left blank.

© 2016 Allegion
004400, Rev. 07/16
www.allegion.com

HandPunch® 4000-S

Biometric time and attendance terminal

Overview

Full function time and attendance...at the palm of your hand
The HandPunch 4000-S brings the flexibility of a full function time and attendance terminal together with the sophistication of the most accurate identification technology available. Using Schlage's field-proven hand geometry biometric technology, the HandPunch 4000 uses the size and shape of your employee's hand to verify their identity each time they punch. No fingerprints or palm prints are utilized.

Facilitate shop floor data collection
The HandPunch 4000-S combines the technology of the popular HandPunch 4000 with an integrated handheld laser barcode scanner. Through the use of the scanner, you can utilize the additional versatility of a job costing and job-tracking device.

Features and benefits

- Provides the most accurate time and attendance solution available
- Shop floor data collection
- Fast and easy to use
- Complete flexibility through 10 data management keys
- Eliminates badges
- Eliminates buddy punching
- Reduces supervisor workload

HH-LAST handheld barcode scanner option for HP-4000-S

The laser scanner plugs directly into the HP-4000-S drawing power from the HandPunch, so there are no extra wires or power supply. Handheld Scanners will be configured to read code 3 of 9 (code 39) and interleaved 2 of 5 (I - 2 of 5) formats. Up to 10 digits are used for the ID number and up to 8 digits for data entry values (accessed through function key menus).

Metrlogic® MS9540 Voyager CG

- Lightweight handheld bar code scanner
- Equipped with trigger for accurate reads (can be deactivated)
- Decodes common numeric 1D formats including Code39 and Interleaved 2 of 5
- High-visibility laser diode (650 nm +/- 10) allows easy placement of line on bar code
- Rapid single line scan speed of 72 +/- 2 lines per second
- Bright green/red LED for easy read verification
- User-replaceable detachable cables
- Durable - shock resistant to 5'
- Not field installable

Specifications

Part number	HP-4000-S
Size (W x H x D)	8.85 in x 11.65 in x 8.55 in (22.3 cm x 29.6 cm x 21.7 cm)
Weight	6 lbs (2.7 kg)
Power	12 to 24 VDC or 12 to 24 VAC 50-60 Hz, 7 watts
Environment	Operating: 32˚F to 113˚F (0˚C to 45˚C) Relative humidity: 20% to 80% NC Non-operating (storage): 14˚F to 140˚F (-10˚C to 60˚C) Relative humidity: 5% to 85% NC
Verification time	Less than one second
Memory retention	Up to 5 years via the standard internal lithium battery
Transaction storage	7680 transactions
Id number length	1 to 10 digits from keypad or card
User capacity	530 users with field upgrade up to 3,498 users Memory module upgrade up to 51,516 users
Template size	9 bytes
User record size	77 bytes
Communications	RS-485 (4 wire) RS-232 serial printer support or PC communication
Baud rate	300 to 28.8 Kbps
Card reader input	Proximity, Wiegand, magnetic stripe, bar code (5 VDC provided by HandReader)
Card reader output	Wiegand, magnetic stripe, bar code
Data management keys	10 keys, user definable Supports ▪ Validation tables ▪ Employee information fields, 24 max ▪ Multi-level prompting ▪ Key restriction by employee ▪ Decision menus ▪ Punch review
Employee messaging	32 characters per message per employee
Employee name	16 characters
Employee schedule	Schedules definable for each employee
Internal barcode reader	Code 39 Interleaved 2 of 5
Door controls	Door lock output (sinks 0-24VDC, 100mA max) Door switch monitoring Bell ring output (sinks 0-24VDC, 100mA max)
Time zones	60 user definable time zones
Options	**BB-250** - Operational battery backup **DC-102** - Data converter(RS-232 to RS-485) **EM-805** - Memory expansion - 3,498 users **EN-200** - Ethernet communications module **MD-500** - Internal 14.4 baud dial-up modem **WAR-EXT** - 1 year extended warranty

Specifications subject to change. Please check with your system vendor for details.

About Allegion

Allegion (NYSE: ALLE) creates peace of mind by pioneering safety and security. As a $2 billion provider of security solutions for homes and businesses, Allegion employs more than 7,800 people and sells products in more than 120 countries across the world. Allegion comprises 23 global brands, including strategic brands CISA®, Interflex®, LCN®, Schlage® and Von Duprin®. For more, visit **www.allegion.com.**

aptiQ ▪ LCN ▪ SCHLAGE ▪ STEELCRAFT ▪ VON DUPRIN

ALLEGION™

SCHLAGE

HandPunch®

Biometric Time & Attendance Terminal

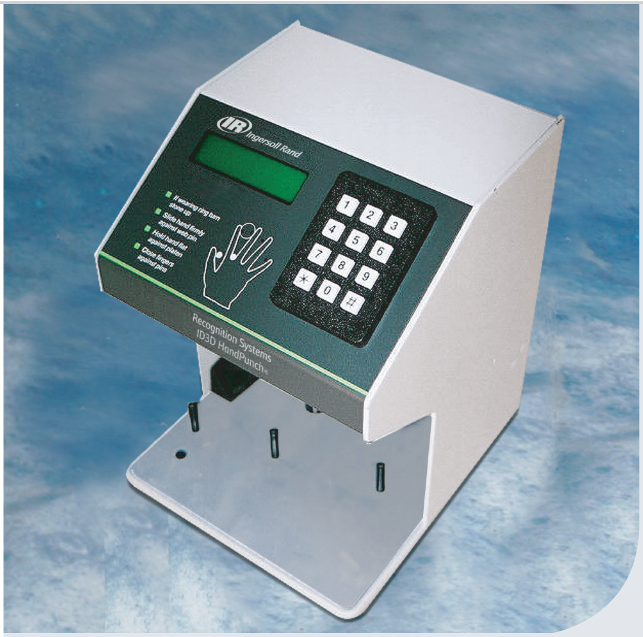
If your payroll accuracy is important... Do it by hand.

No timecards or badges are needed to use the HandPunch® reader. The employee's hand is their card. Their hand can't be lost or forgotten, which reduces your administrative costs. In addition, you'll never have to pay for another card.

The HandPunch is a fully featured time clock complete with operational battery backup and user capacity expandable to 27,904. No other terminal positively verifies each employee and gives you the additional savings generated by eliminating time theft and fraud.

Each time an employee uses the HandPunch, their identity is positively verified by the unique size and shape of their hand. No one can punch in or out for them, which gives you the most accurate payroll possible.

The HandPunch is fast and easy to use. Verification time is typically one second. Restricting the time an employee may use the HandPunch eliminates early IN punches or unauthorized overtime punches. If an employee attempts to use the system during an unauthorized time, the system will display "TIME RESTRICTION".



FEATURES & BENEFITS

- Saves money over card-based systems
- Eliminates Badges
- Eliminates Buddy Punching
- Fast and easy to use
- Provides the most accurate time and attendance solution available

Edit at the Clock

Supervisor override mode allows input at the clock of items such as missed punches, planned vacations, sick time, tips, etc. User restrictions may also be overridden via this mode. This increases supervisor flexibility and eliminates having all edits done at the computer. This mode is password protected and an audit trail identifying who entered the transactions is available.

Department Transfers

To assure you will get the data you need for an accurate payroll, the HandPunch® can automatically request department information for every punch or can be set to only request department data when asked by the employee. If a home department can be assumed for most transactions in your workplace, the user request mode minimizes data input for the majority of employees.

ID Number Input

Employees simply enter an ID number in the HandPunch's built-in keypad and place their hand for verification. Once verified the clock displays "OKAY" followed by the user's ID number. Using the keypad can eliminate the costs associated with cards including administrative costs. Cards or bar codes may also be used to enter the ID number. The HandPunch can be ordered with an optional mag stripe, Wiegand or bar code reader. In this case, the employee would just swipe their badge and the HandPunch would ask them to place their hand for verification.

Explicit Punch Menu

Some workplaces cannot work with assumed schedules. If yours is one of them, turning this menu on makes sure your system gets the data required for accurate application of time and attendance rules and ultimately an accurate payroll. Selections such as In, Out and Back from Break or Lunch are available.

Off-Line Operation

Using the system in an off-line mode allows you to use the time and attendance computer for other purposes. For remote sites, there is no need for expensive dedicated telephone lines. When information needs to be downloaded, just call the HandPunch's optional internal modem over a standard dial-up phone line.

Daylight Savings

Specify the date and time for daylight savings to take effect and the HandPunch will automatically add or subtract one hour at the clock.

Bell Schedule

The bell schedule allows the user to program the day, time and duration for a series of bell rings. These rings may be used to signal the start or end of a shift, lunch or break.

Operational Battery Backup

The system will accept punches for 2 to 3 hours after power is lost. All hand template data and reader setup data will be maintained for up to 5 years by the standard lithium battery backup internal to the HandPunch.

SPECIFICATIONS

Part Number:	HP-RR Recessed Mount HP-RS Surface Mount HP-RT Table Top	
Size:	6.46 in (16.4 cm) wide 8.25 in (21.0 cm) high 7.20 in (18.5 cm) deep	
Weight:	8 lbs (3.6 kg)	
Power:	12-14 VDC max, allowable @0.5 Amps min.	
Environment:	Operating: 32°F to 100°F Relative Humidity: 95% Max. NC	
Verification Time:	Less than 1 second	
Memory Retention:	5 years with internal lithium battery	
Transaction Storage:	3,405 transactions	
ID Number Length:	1 to 10 digits from keypad or card	
User Capacity:	256 standard, expandable to over 27,904	
Template Size:	9 bytes	
Communications:	RS-485 (4 and 2 wire) RS-232 Serial Printer Support	
Baud Rate:	300 to 28.8 Kbps	
Card Reader Input:	Wiegand, magnetic stripe, barcode or proximity	
Card Reader Output:	Wiegand or magnetic stripe	
Door Controls:	Door Lock Output (Sinks 0-24VDC, 100mA max.) Door Switch Monitoring Bell Ring Output (Sinks 0-24VDC, 100mA max.)	
Options	EN-100	Ethernet Communications Module
	EM-600	Memory Expansion - 3,328 users
	EM-602	Memory Expansion - 9,728 users
	EM-604	Memory Expansion - 27,904 users
	MD-200	Internal Dial-Up Modem
	WAR-EXT	1 year extended warranty

HandPunch® is a registered trademark of Schlage. Specifications subject to change.
Please check with your system vendor for details.

ALLEGION™

SCHLAGE®

HandPunch® 1000-E

Biometric time and attendance terminal

Overview

A biometric time clock that is truly affordable for small to midsize businesses
Schlage now brings the accuracy and convenience of biometric technology easily within reach of any time and attendance application. In operations that range from the corner deli to franchise chains, Schlage HandReaders have proven themselves to be a practical and precise solution. Our terminals are so affordable, they make card-based systems seem obsolete.

Your hand is your card
There are no cards to create, administer, carry, or lose. The HandPunch® 1000-E verifies employees' identities in less than one second, based on the unique size and shape of their hands. For small companies, the HandPunch 1000-E provides a quick return on investment by eliminating the cost associated with administrating and managing cards. For companies that have small, multiple locations, minimal supervision leaves opportunity for buddy punching and time fraud. With the HandPunch 1000-E, one employee can't punch for the other. Time fraud is eliminated thereby reducing payroll costs and increasing the company's bottom line.

Small enterprise solution
The HandPunch 1000-E provides a solution for companies with 100 employees or less per terminal or location. Just because you run a small company doesn't mean you don't have time fraud issues. The HandPunch 1000-E terminal allows small companies to put an end to time fraud and begin utilizing biometric technology. The added benefit of standard Ethernet allows easy connectivity to most time and attendance applications. With the HandPunch 1000-E, small companies no longer need to worry about lost timecards, making new cards, or employees clocking in for another employee.

Features and benefits

- Saves money over card-based systems
- Dramatically reduces payroll costs
- Easily integrates into existing network infrastructures
- Eliminates badges
- Eliminates buddy punching
- Fast and easy to use
- Comes standard with an Ethernet card
- Up to 100 users
- Platen also comes standard with a printed hand outline to ensure accurate hand placement while punching

Hand geometry technology

The HandPunch 1000-E uses Schlage's field-proven hand geometry biometric technology. The terminal captures an image of the hand each time the employee punches. The hand's size and the shape are used to verify their identity with unparalleled accuracy. No fingerprints or palm prints are utilized. Green and red lights notify the employee of the status of each punch. There's no question, employees have to be there to punch in.

Affordable ethernet solution

The HandPunch 1000-E comes standard with a built-in Ethernet connection allowing for quick integration into your time & attendance application and existing network infrastructure.

Antimicrobial protection

Every HandPunch contains a silver-based antimicrobial agent which is embedded into the materials used to produce the platen, providing a finish that inhibits the growth of a broad spectrum of bacteria, mold, and fungi and remains active for the life of the HandPunch.

Hand outline

The HandPunch comes standard with a blue hand outline printed on the platen. This hand outline will help new users place their hand accurately on the platen when using the terminal and decrease initial enrollment time.

Specifications

Part number	HP-1000E
Size (W x H x D)	8.85" x 11.65" x 8.55" (22.3 cm x 29.6 cm x 21.7 cm)
Weight	6 lbs (2.7 kg)
Power	12 to 24 VDC or 12 to 24 VAC 50-60 Hz, 7 watts
Environment	Operating: 32˚F to 113˚F (0˚C to 45˚C) Relative humidity: 20% to 80% NC Non-operating (storage): 14˚F to 140˚F (-10˚C to 60˚C) Relative humidity: 5% to 85% NC
Verification time	Less than one second
Memory retention	Up to 5 years via the standard internal lithium battery
Transaction storage	5120 transactions
ID number length	1 to 10 digits from keypad or card
User capacity	100 users
Template size	9 bytes
User record size	Standard units 16 bytes, -XL models 77 bytes
Communications	Ethernet 10 Base-T (TCP/IP) RS-232 serial printer support
Options	**BB-250** - Operational battery backup **WAR-EXT** - 1 year extended warranty

Specifications subject to change. Please check with you system vendor for details

About Allegion

Allegion (NYSE: ALLE) creates peace of mind by pioneering safety and security. As a $2 billion provider of security solutions for homes and businesses, Allegion employs more than 7,800 people and sells products in more than 120 countries across the world. Allegion comprises 23 global brands, including strategic brands CISA®, Interflex®, LCN®, Schlage® and Von Duprin®. For more, visit **www.allegion.com.**

aptiQ ■ LCN ■ SCHLAGE ■ STEELCRAFT ■ VON DUPRIN

ALLEGION™

© 2014 Allegion
004521, Rev. 04/14
www.allegion.com/us

SCHLAGE

HandPunch® 1000

Biometric time and attendance terminal

Overview

A biometric time clock that is truly affordable for small to midsize businesses
Schlage now brings the accuracy and convenience of biometric technology easily within reach of any time and attendance applications. In operations that range from the corner deli to franchise chains, Schlage products have proven themselves to be a practical and precise solution. Our terminals are so affordable, card-based systems seem obsolete.

Your hand is your card
There are no cards to create, administer, carry, or lose. The HandPunch® 1000 verifies employees' identities in less than one second, based on the unique size and shape of their hands. For small companies, the HandPunch 1000 provides a quick return on investment by eliminating the cost associated with administrating and managing cards. For companies that have small, multiple locations, minimal supervision leaves opportunity for buddy punching and time fraud. With the HandPunch 1000 one employee can't punch for the other. Time fraud is eliminated thereby reducing payroll costs and increasing the company's bottom line.

Pay as you grow
Designed to grow with your business, the user capacity of the HandPunch 1000 can be easily expanded in the field. Standard user memory provides for up to 50 employees with the expandability to grow to 512 users.

Features and benefits

- Saves money over card-based systems
- Eliminates badges
- Eliminates buddy punching
- Fast and easy to use
- Provides the most accurate time and attendance solution available

Hand geometry technology

The HandPunch 1000 uses Schlage's field-proven hand geometry biometric technology. The terminal captures an image of the hand each time the employee punches. The hand's size and the shape are used to verify their identity with unparalleled accuracy. No fingerprints or palm prints are utilized. Green and red lights notify the employee of the status of each punch. There's no question any more; employees have to be there to punch.

Small enterprise solution

The HandPunch 1000 provides a new solution for companies with 50 employees or less per terminal or location. The HandPunch 1000 terminal allows for collection of in and out punches plus allows easy connectivity to any time and attendance application. With the HandPunch 1000 small companies no longer need to worry about lost timecards, making new cards, or employees punching for another employee.

Pay for only what you need

The HandPunch 1000 comes standard with user capacity for 50 users. As your business grows, so can the user capacity of the HandPunch 1000. Memory upgrades are available to expand to 100 or even up to 512 users. The upgrade can be easily performed in the field without removing the unit from the wall. With a built-in transaction memory to store over 5,000 punches, the HandPunch 1000 ensures your employees' data is safe.

Communication options

The HandPunch 1000 connects quickly to the time and attendance PC via a provided 50-foot RS232 communications cable. An optional internal 14.4 K baud dial-up modem is available for remote sites.

Antimicrobial protection

Every HandPunch contains a silver-based antimicrobial agent - which is embedded into the materials used to produce the platen, providing a finish that inhibits the growth of a broad spectrum of bacteria, mold, and fungi and remains active for the life of the HandPunch.

Hand outline

The HandPunch comes standard with a blue hand outline printed on the platen. This hand outline will help new users place their hand accurately on the platen when using the terminal and decrease initial enrollment time.

Specifications

Part number	HP-1000
Size (W X H X D)	8.85 in x 11.65 in x 8.55 in (22.3 cm x 29.6 cm x 21.7 cm)
Weight	6 lbs (2.7 kg)
Power	12 to 24 VDC or 12 to 24 VAC 50-60 Hz, 7 watts
Environment	Operating: 32˚F to 113˚F (0˚C to 45˚C) Relative humidity: 20% to 80% NC Non-operating (storage): 14˚F to 140˚F (-10˚C to 60˚C) Relative humidity: 5% to 85% NC
Verification time	Less than one second
Memory retention	Up to 5 years via the standard internal lithium battery
Transaction storage	5120 transactions
ID number length	1 to 10 digits from keypad or card
User capacity	50 users expandable to 512 users
Template size	9 bytes
User record size	Standard units 16 bytes, -XL models 77 bytes
Communications	RS-232, 50 foot cable included
Options	**BB-250** - Operational battery backup **EM-701** - Memory expansion - 50 to 100 users **EM-702** - Memory expansion - 50 to 512 users **MD-500** - Internal 14.4 baud dial-up modem **WAR-EXT** - 1 year extended warranty

Specifications subject to change. Please check with your system vendor for details.

About Allegion

Allegion (NYSE: ALLE) creates peace of mind by pioneering safety and security. As a $2 billion provider of security solutions for homes and businesses, Allegion employs more than 7,800 people and sells products in more than 120 countries across the world. Allegion comprises 23 global brands, including strategic brands CISA®, Interflex®, LCN®, Schlage® and Von Duprin®. For more, visit **www.allegion.com.**

aptiQ ■ LCN ■ SCHLAGE ■ STEELCRAFT ■ VON DUPRIN

ALLEGION™

© 2014 Allegion
004525, Rev. 04/14
www.allegion.com/us

ALLEGION™

SCHLAGE®

HandPunch® 2000

Biometric time and attendance terminal

Overview

Put your hands on the accurate, affordable solution
Schlage now brings the accuracy and convenience of biometric technology easily within reach of any time and attendance applications. In operations that range from coal mines to clean rooms, Schlage have proven themselves to be a practical and precise solution. Our terminals are so affordable, it doesn't make sense to consider any other technology.

Smarter than card-based terminals
There are no cards to create, administer, carry, or lose. The HandPunch® 2000 verifies employees' identities in less than one second, based on the unique size and shape of their hands. HandPunch 2000 clearly notifies each user of a match using red and green indicator lights. Because no one can punch in or out for your employees, the system reduces time theft and improves payroll accuracy.

Versatile and programmable
Programmable beyond a simple time clock, the HandPunch 2000 provides definable data management keys that allow data collection when employees punch. The systems transmit data to the time and attendance host PC through a variety of options, depending on the model. Model differences let you tailor the right system for your company's size and needs. When you want to cut time and attendance costs... do it by hand.

Features and benefits

- Saves money over card-based systems
- Eliminates badges
- Eliminates buddy punching
- Fast and easy to use
- Provides the most accurate time and attendance solution available

Hand geometry technology

The HandPunch 2000 uses Schlage's field-proven hand geometry biometric technology. The terminal captures an image of the hand each time the employee punches. The hand's size and the shape are used to verify their identity with unparalleled accuracy. No fingerprints or palm prints are utilized. Green and red lights notify the employee of the status of each punch. There's no question any more; employees have to be there to punch.

Programmable data management keys

The HandPunch 2000 has two user-definable data management keys that let you collect data as employees punch. Common uses include department transfers, tips collected, job codes, or pay codes. Multi-level data entry sequences may be defined. You can also set the data management keys to allow employees to review their past punches. To reduce keystrokes, the keys can also be set to automatically enter data such as a frequently used department number or in/out status.

Communication options

The HandPunch 2000 connects quickly to the time and attendance system via RS-232 communications. An optional Ethernet module or dial-up high speed modem is available for alternative communications options.

Antimicrobial protection

Every HandPunch contains a silver-based antimicrobial agent - which is embedded into the materials used to produce the platen, providing a finish that inhibits the growth of a broad spectrum of bacteria, mold, and fungi and remains active for the life of the HandPunch.

Hand outline

The HandPunch comes standard with a blue hand outline printed on the platen. This hand outline will help new users place their hand accurately on the platen when using the terminal and decrease initial enrollment time.

Specifications

Part number	HP-2000
Size (W x H x D)	8.85 in x 11.65 in x 8.55 in (22.3 cm x 29.6 cm x 21.7 cm)
Weight	6 lbs (2.7 kg)
Power	12 to 24 VDC or 12 to 24 VAC 50-60 Hz, 7 watts
Environment	Operating: 32˚F to 113˚F (0˚C to 45˚C) Relative humidity: 20% to 80% NC Non-operating (storage): 14˚F to 140˚F (-10˚C to 60˚C) Relative humidity: 5% to 85% NC
Verification time	Less than one second
Memory retention	Up to 5 years via the standard internal lithium battery
Transaction storage	5120 transactions
ID number length	1 to 10 digits from keypad or card
User capacity	512 users
Template size	9 bytes
User record size	Standard units 16 bytes, -XL models 77 bytes
Communications	RS-232 serial printer support or PC communication
Options	**BB-250** - Operational battery backup **EN-200** - Ethernet module **MD-500** - Internal 14.4 baud dial-up modem **WAR-EXT** - 1 year extended warranty

Specifications subject to change. Please check with your system vendor for details.

About Allegion

Allegion (NYSE: ALLE) creates peace of mind by pioneering safety and security. As a $2 billion provider of security solutions for homes and businesses, Allegion employs more than 7,800 people and sells products in more than 120 countries across the world. Allegion comprises 23 global brands, including strategic brands CISA®, Interflex®, LCN®, Schlage® and Von Duprin®. For more, visit **www.allegion.com.**

aptiQ ■ LCN ■ SCHLAGE ■ STEELCRAFT ■ VON DUPRIN

ALLEGION™

© 2014 Allegion
004524, Rev. 04/14
www.allegion.com/us

ALLEGION™

SCHLAGE

HandPunch® 3000

Biometric time and attendance terminal

Overview

Put your hands on the accurate, affordable solution

Schlage now brings the accuracy and convenience of biometric technology easily within reach of any time and attendance applications. In operations that range from coal mines to clean rooms, Schlage HandPunches have proven themselves to be a practical and precise solution. Our terminals are so affordable, it doesn't make sense to consider any other technology.

Smarter than card-based terminals

There are no cards to create, administer, carry, or lose. The HandPunch® 3000 verifies employees' identities in less than one second, based on the unique size and shape of their hands. HandPunch 3000 clearly notifies each user of a match using red and green indicator lights. Because no one can punch in or out for your employees, the system reduces time theft and improves payroll accuracy.

Versatile and programmable

Beyond a simple time clock, the HandPunch 3000 provides definable data management keys that allow data collection when employees punch. The readers transmit data to the time and attendance host PC through a variety of methods including direct wiring, modem and Ethernet. The HandPunch 3000 also has the ability to control a door. When you want to cut time and attendance costs… do it by hand.

Features and benefits

- Saves money over card-based systems
- Eliminates badges
- Eliminates buddy punching
- Fast and easy to use
- Provides the most accurate time and attendance solution available

Hand geometry technology

The HandPunch 3000 uses Schlage's field-proven hand geometry biometric technology. The terminal captures an image of the hand each time the employee punches. The hand's size and the shape are used to verify their identity with unparalleled accuracy. No fingerprints or palm prints are utilized. Green and red lights notify the employee of the status of each punch. There's no question any more; employees have to be there to punch.

Programmable data management keys

The HandPunch 3000 has two user-definable data management keys that let you collect data as employees punch. Common uses include department transfers, tips collected, job codes, or pay codes. Multi-level data entry sequences may be defined. You can also set the data management keys to allow employees to review their past punches. To reduce keystrokes, the keys can also be set to automatically enter data such as a frequently used department number or in/out status.

Communication options

Whether your application calls for one terminal or thousands, the HandPunch 3000 can meet the need. Multiple terminals can be networked together at a site via RS-485 wiring. An optional Ethernet communications module or dial up modem are also available. Both options are internal to the terminal making installation fast and simple.

Edit-at-the-clock functions

The HandPunch 3000 allows supervisors to override user restrictions and to input such items as missed punches, planned vacations, and sick time at the terminal. The password-protected mode provides greater supervisor flexibility by lessening the need for computer edits. Audit trails documenting the use of these functions are generated to ensure security.

Bell schedules

The bell schedule lets you program the day, time, and duration of a series of bells. The bells can be programmed to signal the beginning or end of a shift, lunch, or break.

Door control

The HandPunch 3000 provides the capability to unlock and monitor a door. Global timezones may be used to restrict employee access.

Antimicrobial protection

Every HandPunch contains a silver-based antimicrobial agent, which is embedded into the materials used to produce the platen, providing a finish that inhibits the growth of a broad spectrum of bacteria, mold, and fungi and remains active for the life of the HandPunch.

Hand outline

The HandPunch comes standard with a blue hand outline printed on the platen. This hand outline will help new users place their hand accurately on the platen when using the terminal and decrease initial enrollment time.

Specifications

Part number	HP-3000
Size (W x H x D)	8.85 in x 11.65 in x 8.55 in (22.3 cm x 29.6 cm x 21.7 cm)
Weight	6 lbs (2.7 kg)
Power	12 to 24 VDC or 12 to 24 VAC 50-60 Hz, 7 watts
Environment	Operating: 32˚F to 113˚F (0˚C to 45˚C) Relative humidity: 20% to 80% NC Non-operating (storage): 14˚F to 140˚F (-10˚C to 60˚C) Relative humidity: 5% to 85% NC
Verification time	Less than one second
Memory retention	Up to 5 years via the standard internal lithium battery
Transaction storage	5120 transactions
ID number length	1 to 10 digits from keypad or card
User capacity	512 users with field upgrade up to 32,512 users Memory module upgrade up to 259,072 users
Template size	9 bytes
User record size	Standard units 16 bytes, -XL models 77 bytes
Communications	RS-485 (4 wire) RS-232 serial printer support or PC communication
Baud rate	300 to 28.8 Kbps
Card reader input	Proximity, Wiegand, magnetic stripe, bar code (5 VDC provided by HandReader)
Card reader output	Wiegand, magnetic stripe, bar code
Door controls	Door lock output (sinks 0-24VDC, 100mA max) Door switch monitoring Bell ring output (sinks 0-24VDC, 100mA max)
Time zones	60 user definable time zones
Options	**BB-250** - Operational battery backup **DC-200** - Data converter (RS-232 to RS-485) **EM-801** - Memory expansion - 9,728 users **EM-803** - Memory expansion - 32,512 users **EN-200** - Ethernet communications module **MD-500** - Internal 14.4 baud dial-up modem **WAR-EXT** - 1 year extended warranty

Specifications subject to change. Please check with your system vendor for details.

Allegion, the Allegion logo, Schlage, the Schlage logo, and HandPunch are trademarks of Allegion plc, its subsidiaries and/or affiliates in the United States and other countries. All other trademarks are the property of their respective owners.

About Allegion

Allegion (NYSE: ALLE) creates peace of mind by pioneering safety and security. As a $2 billion provider of security solutions for homes and businesses, Allegion employs more than 7,800 people and sells products in more than 120 countries across the world. Allegion comprises 23 global brands, including strategic brands CISA®, Interflex®, LCN®, Schlage® and Von Duprin®. For more, visit **www.allegion.com.**

aptiQ ■ LCN ■ SCHLAGE ■ STEELCRAFT ■ VON DUPRIN

ALLEGION™

HandPunch® 4000

Biometric time and attendance terminal

Overview

Full function time and attendance . . . at the palm of your hand

The HandPunch® 4000 brings the flexibility of a full function time and attendance terminal together with the sophistication of the most accurate identification technology available. Using Schlage's field-proven hand geometry biometric technology, the HandPunch 4000 uses the size and shape of your employee's hand to verify their identity each time they punch. No fingerprints or palm prints are utilized.

A cost-saving, easy-to-use solution

With the HandPunch 4000, your hand is your badge. The cost of creating and administering badges is eliminated along with buddy punching. The system ensures payroll accuracy by simply requiring each employee to be there to punch. The terminal is fast and easy for anyone to use. An employee's identity is verified in less than one second.

An important HR communication tool

More than a simple time and attendance terminal, the HandPunch 4000 lets you tailor the system to meet your precise needs. The system provides the ability to send messages to employees when they punch. In addition, employees can view up to 24 information fields to find out about their schedule, total hours worked, and more.

Features and benefits

- Provides the most accurate time and attendance solution available
- Fast and easy to use
- Complete flexibility through 10 data management keys
- Eliminates badges
- Eliminates buddy punching
- Reduces supervisor workload

10 Programmable data management keys

Ten user-definable data management keys let you collect and/or display data as employees punch. Common data collection uses include department transfers, tips collected, job codes, or pay codes. The keys can also be defined to allow employees to review punches or find out about their schedules, vacation time accumulated, hours worked, and other programmed information. To reduce keystrokes, the keys can also be set to automatically enter data such as a frequently used department number or in/out status. Other data management key features include:

- Employee messaging
- Review of employee information fields
- Validation tables to ensure proper data entry
- Restrict employee access to specific data management keys
- User defined prompts
  - Multi-level input sequence definable per key
- Decision menus to minimize keystrokes

Schedules by employee

Employee schedules may be downloaded to the HandPunch 4000 to restrict the times that an employee can punch. This can reduce unauthorized overtime as well as early “in” punches. A separate schedule can be defined for each employee providing the ultimate in flexibility.

Built-in bar code reader

Some installations require the use of a badge. For these situations, the HandPunch 4000 includes an integrated bar code reader that can be used for ID number entry. The swipe-type reader supports the most popular bar code formats and allows for infrared badges.

Communications and networking

Whether your needs are to network two terminals or thousands, the HandPunch 4000 can be configured to meet your needs. Standard RS-485 communications makes networking terminals easy and reliable. Options include Ethernet communications modules and a high speed internal modem for remote sites. Each unit also provides RS-232 serial printer support.

Edit-at-the-clock functions

The HandPunch 4000 allows supervisors to override user restrictions and to input such items as missed punches, planned vacations, and sick time at the terminal. The password-protected mode provides greater supervisor flexibility by lessening the need for computer edits. Audit trails documenting the use of these functions are generated to ensure security.

Bell schedules

The bell schedule lets you program the day, time, and duration of a series of bells. The bells can be programmed to signal the beginning or end of a shift, lunch, or break.

Door control

The HandPunch 4000 provides the capability to unlock and monitor a door. An employee’s individual schedule may be used to restrict access.

Antimicrobial protection

Every HandPunch contains a silver-based antimicrobial agent which is embedded into the materials used to produce the platen, providing a finish that inhibits the growth of a broad spectrum of bacteria, mold, and fungi and remains active for the life of the HandPunch.

Hand outline

The HandPunch comes standard with a blue hand outline printed on the platen. This hand outline will help new users place their hand accurately on the platen when using the terminal and decrease initial enrollment time. HandPunch® is a registered trademark of Schlage.

Specifications

Part number	HP-4000
Size (W x H x D)	8.85 in x 11.65 in x 8.55 in (22.3 cm x 29.6 cm x 21.7 cm)
Weight	6 lbs (2.7 kg)
Power	12 to 24 VDC or 12 to 24 VAC 50-60 Hz, 7 watts
Environment	Operating: 32˚F to 113˚F (0˚C to 45˚C) Relative humidity: 20% to 80% NC Non-operating (storage): 14˚F to 140˚F (-10˚C to 60˚C) Relative humidity: 5% to 85% NC
Verification time	Less than one second
Memory retention	Up to 5 years via the standard internal lithium battery
Transaction storage	7680 transactions
Id number length	1 to 10 digits from keypad or card
User capacity	530 users with field upgrade up to 3,498 users Memory module upgrade up to 51,516 users
Template size	9 bytes
User record size	77 bytes
Communications	RS-485 (4 wire) RS-232 serial printer support or PC communication
Baud rate	300 to 28.8 Kbps
Card reader input	Proximity, Wiegand, magnetic stripe, bar code (5 VDC provided by HandReader)
Card reader output	Wiegand, magnetic stripe, bar code
Data management keys	10 keys, user definable Supports ▪ Validation tables ▪ Employee information fields, 24 max ▪ Multi-level prompting ▪ Key restriction by employee ▪ Decision menus ▪ Punch review
Employee messaging	32 characters per message per employee
Employee name	16 characters
Employee schedule	Schedules definable for each employee
Internal barcode reader	Code 39 Interleaved 2 of 5
Door controls	Door lock output (sinks 0-24VDC, 100mA max) Door switch monitoring Bell ring output (sinks 0-24VDC, 100mA max)
Time zones	60 user definable time zones
Options	**BB-250** - Operational battery backup **DC-102** - Data converter(RS-232 to RS-485) **EM-805** - Memory expansion - 3,498 users **EN-200** - Ethernet communications module **MD-500** - Internal 14.4 baud dial-up modem **WAR-EXT** - 1 year extended warranty

Specifications subject to change. Please check with your system vendor for details.

About Allegion

Allegion (NYSE: ALLE) creates peace of mind by pioneering safety and security. As a $2 billion provider of security solutions for homes and businesses, Allegion employs more than 7,800 people and sells products in more than 120 countries across the world. Allegion comprises 23 global brands, including strategic brands CISA®, Interflex®, LCN®, Schlage® and Von Duprin®. For more, visit **www.allegion.com.**

aptiQ ■ LCN ■ SCHLAGE ■ STEELCRAFT ■ VON DUPRIN

ALLEGION™

Enclosure Options
for the HandPunch Series

Overview

Schlage biometrics provides various options to protect your HandPunch time clocks from the elements. Three different, proven solutions are available to ensure your HandReaders keep performing regardless of your environment.

FX Enclosure (FX-ENCL)
GX Enclosure (GX-ENCL)
Time & Attendance HandPunch Enclosure

Constructed from high impact UV resistant polycarbonate material, the FX Enclosure provides a degree of protection against dusty, dirty, or rainy environments. Designed for the HandPunch F and G-Series, this enclosure has been designed so that it can be added to an existing installation. When used with an integrated heater option (INT-HTR), it provides a comfortable heated platen against a cold climate.

FX and GX Enclosure

TX Enclosure (TX-ENCL)
Time & Attendance HandPunch Enclosure

The TX Enclosure provides a higher degree of protection against dusty, dirty, or rainy environments. Designed for the HandPunch F-Series, when used with an integrated heater option (INT-HTR), it provides a comfortable heated platen against a cold climate.

TX Enclosure

Specifications

	FX Enclosure	GX Enclosure	TX Enclosure
Part Number	FX-ENCL	GX-ENCL	TX-ENCL
Temperature Range	-20F to 120F / -29C to 49C	-20F to 120F / -29C to 49C	-45F to 120F / -43C to 49C
Dimensions H x W x D	14.75 in x 12.00 in x 10.50 in 37.5 cm x 30.5 cm x 26.7 cm	14.75 in x 12.00 in x 10.50 in 37.5 cm x 30.5 cm x 26.7 cm	23.00 in x 14.00 in x 11.25 in 58.4 cm x 35.6 cm x 28.6 cm
Cross Weight (including reader)	7.3 lbs / 3.3 kg	7.3 lbs / 3.3 kg	45.0 lbs / 20.4 kg
HandReader Models	HP-1000 through HP-4000	GT-400	HP-1000 through HP-4000, GT-400
Heater	Factory installed option only, Model No. INT-HTR	Factory installed option only, Model No. INT-HTR	Factory installed option only, Model No. INT-HTR

Ingersoll Rand Security Technologies

ALLEGION™

SCHLAGE®

Biometric terminal options and accessories

for HandKey®

Schlage offers a number of accessories for access control HandReader terminals. From networking options to memory expansions, we'll help you create the solution to meet your specific needs.

Base Model	HandKey II
Card readers	▪ **PROX:** Externally top mounted HID proximity reader, factory option only ▪ **SC-100:** Mifare Classic (r) reader, factory option only ▪ **iCLASS®**: HID Legacy iCLASS reader, factory option only ▪ **CR-2**: Mag stripe wall mount card reader ▪ **BC-100**: Bar code reader, wall mount swipe
Memory	▪ **EM-801-F3**: Field upgradable memory expansion up to 9,728 users ▪ **EM-803-F3**: Field upgradable memory expansion up to 32,512 users
Communication	▪ **EN-201:** Field upgradeable Ethernet communication module 10baseT ▪ **MD-500:** Internal dial-up modem
Power options	▪ **PS-110**: Power supply, 120VAC to 13.5 VDC ▪ **PS-220**: Power supply, 220VAC to 13.5 VDC ▪ **BB-250**: Optional battery backup
Mounting	▪ **TM-100**: Table top secure mount for flat surfaces
Left hand option	▪ NA
Network accessories	▪ **DC-102**: Data converter for 4 wire system, RS-232 to RS-422 with 120V, 60Hz power supply ▪ **DC-102 with 220V**, 50Hz power supply

This page intentionally left blank.

ALLEGION™

SCHLAGE

HandPunch® GT-400

Biometric time and attendance terminal

Overview

The industry's most reliable biometric just got better

The HandPunch® GT-400 brings the flexibility of a full-function time and attendance terminal together with the sophistication of the most robust verification technology available. To eliminate employees from punching in for one another, the HandPunch GT-400 uses the size and shape of your employee's hand to verify their identity each time they punch. No fingerprints or palm prints are utilized ensuring the privacy of each user.

A cost-saving, easy-to-use solution

With the HandPunch GT-400, your hand is your badge. The cost of creating and administering badges is eliminated along with buddy punching (when one employee clocks in for another). The system ensures payroll accuracy by simply requiring each employee to be there to punch. The terminal is fast and easy for anyone to use.

Cutting edge technology with a rich feature set

The HandPunch GT-400 uses an open architecture design coupled with standard features like a large display, programmable soft function keys and Ethernet connectivity to set a new standard in terminal.

Features and benefits

- Dramatically reduces payroll costs
- Easily integrates with workforce management software packages
- 8 ATM-style soft function keys make dynamic labeling a snap
- 3.8 inch QVGA display lets users access more information per screen
- Large LED light bar for easier visual response
- Antimicrobial-infused platen, keypads and chassis

Advanced communications and networking (Ethernet only)

The HandPunch GT-400 can be configured to meet virtually any networking need or online operation. Each terminal comes standard with 10/100 Ethernet connectivity.

Programmable soft function keys

The HandPunch GT-400 comes standard with eight ATM-style programmable soft function keys, making dynamic labeling a snap. Validation tables, multi-level prompting, decision menus, and punch reviews are just some of the functions that can be programmed into the terminal with these soft keys.

Large display and LED bar

The HandPunch GT-400 features a large 3.8" QVGA display. This display gives users the ability to access more information per screen. The standard four-color LED bar provides users with instant visual feedback of punch verification and indicates online connectivity.

Levels of integration

The HandPunch GT-400 enables users to integrate their time and attendance or payroll applications in many ways ranging from using the terminal's operating system to get transactions, to developing a complete end-to-end solution.

Platen, keypad and chassis features

The platen, keypad and chassis of the HandPunch GT-400 are all integrated with an antimicrobial agent to ensure protection through the punching process. The platen also comes standard with a printed hand outline to ensure accurate hand placement while punching.

Specifications

Part number	GT-400 (standard model with Ethernet)
Size (W x H x D)	8.0 in x 11.18 in x 7.52 in (20.32 cm x 28.40 cm x 19.10 cm)
Weight	5.8 lbs (2.63 kg)
Power	10.8 to 13.5 VDC
Environment	Operating: 32˚F to 113˚F (0˚C to 45˚C) Relative humidity: 5% to 85% NC Non-operating (storage): 14˚F to 140˚F (-10˚C to 60˚C)
Verification time	Less than one second
Template size	20 bytes
Communications	Standard Ethernet 10/100 RJ-45 type connector
Data management keys	8 programmable soft keys, user definable, supports ▪ Validation tables ▪ Employee information fields ▪ Multi-level prompting ▪ Key restriction by employee ▪ Decision menus ▪ Punch review
Miscellaneous options	**BB-300** - Battery backup **GX-ENCL** - Enclosure **INT-HTR-G** - Integrated heated platen
Internal credential	**GT-BCR** - Barcode reader **MTR-G** - Multi-technology card reader option
Development options	▪ Integrate the Schlage time and attendance terminal application with our host ▪ Port or develop your own application on the terminal and integrate with your host

Specifications subject to change. Please check with your system vendor for details.

About Allegion

Allegion (NYSE: ALLE) creates peace of mind by pioneering safety and security. As a $2 billion provider of security solutions for homes and businesses, Allegion employs more than 7,800 people and sells products in more than 120 countries across the world. Allegion comprises 23 global brands, including strategic brands CISA®, Interflex®, LCN®, Schlage® and Von Duprin®. For more, visit **www.allegion.com.**

aptiQ ■ LCN ■ SCHLAGE ■ STEELCRAFT ■ VON DUPRIN

ALLEGION™

Enclosure Options

for the HandPunch Series

Overview

Schlage biometrics provides various options to protect your HandPunch time clocks from the elements. Three different, proven solutions are available to ensure your HandReaders keep performing regardless of your environment.

FX Enclosure (FX-ENCL)
GX Enclosure (GX-ENCL)
Time & Attendance HandPunch Enclosure

Constructed from high impact UV resistant polycarbonate material, the FX Enclosure provides a degree of protection against dusty, dirty, or rainy environments. Designed for the HandPunch F and G-Series, this enclosure has been designed so that it can be added to an existing installation. When used with an integrated heater option (INT-HTR), it provides a comfortable heated platen against a cold climate.

TX Enclosure (TX-ENCL)
Time & Attendance HandPunch Enclosure

The TX Enclosure provides a higher degree of protection against dusty, dirty, or rainy environments. Designed for the HandPunch F-Series, when used with an integrated heater option (INT-HTR), it provides a comfortable heated platen against a cold climate.

FX and GX Enclosure

TX Enclosure

Specifications

	FX Enclosure	GX Enclosure	TX Enclosure
Part Number	FX-ENCL	GX-ENCL	TX-ENCL
Temperature Range	-20F to 120F / -29C to 49C	-20F to 120F / -29C to 49C	-45F to 120F / -43C to 49C
Dimensions H x W x D	14.75 in x 12.00 in x 10.50 in 37.5 cm x 30.5 cm x 26.7 cm	14.75 in x 12.00 in x 10.50 in 37.5 cm x 30.5 cm x 26.7 cm	23.00 in x 14.00 in x 11.25 in 58.4 cm x 35.6 cm x 28.6 cm
Cross Weight (including reader)	7.3 lbs / 3.3 kg	7.3 lbs / 3.3 kg	45.0 lbs / 20.4 kg
HandReader Models	HP-1000 through HP-4000	GT-400	HP-1000 through HP-4000, GT-400
Heater	Factory installed option only, Model No. INT-HTR	Factory installed option only, Model No. INT-HTR	Factory installed option only, Model No. INT-HTR

Ingersoll Rand
Security Technologies

SCHLAGE

HandPunch® GT-400 + MTR-G

Biometric Time & Attendance Terminal with Multi-Technology Reader featuring aptiQ™

Overview

The industry's most reliable biometric just got better. The HandPunch® GT-400 brings the flexibility of a full-function time and attendance terminal together with versatile proximity, smart, and multi-technology credential reader options. Now your employees can clock-in using the same card they use to enter your building. With a multi-technology reader module embedded inside, the HandReader contains both 125 kHz proximity and 13.56 MHz contactless smart card capability, and supports ISO standard 14443 technology.

The MTR-G embedded reader module provides compatibility with HID® proximity, GE/CASI ProxLite®, AWID® proximity, LENEL® proximity, and many 13.56 MHz smart card technologies, including our aptiQ smart credentials. If you upgrade your existing card based access control system from proximity to smart technology, our HandReader can upgrade with you. Additionally, aptiQ™ smart technology is NFC (near field communication) compatible and able to communicate with NFC-enabled phones whenever you're ready to take that step.

The HandPunch GT-400 uses the size and shape of your employee's hand to verify their identity each time they punch. No fingerprints or palm prints are utilized, ensuring the privacy of each user. The terminal is fast and easy for anyone to use. And it eliminates buddy punching (when one employee clocks in for another), helping you save money.

The HandPunch GT-400 uses an open architecture design coupled with standard features like a large display, programmable soft function keys and Ethernet connectivity to set a new standard in terminal.

Features and Benefits

- Embedded reader module operates on 125 kHz frequency and 13.56 MHz frequency
- Recognizes most proximity credentials and aptiQ™ smart credentials (MIFARE® Classic and MIFARE DESFire™ EV1)
- Dramatically reduces payroll costs
- Easily integrates with workforce management software packages
- 8 ATM-style soft function keys make dynamic labeling a snap
- 3.8 inch QVGA display lets users access more information per screen
- Large LED light bar for easier visual response
- Antimicrobial-infused platen, keypads and chassis

Ingersoll Rand
Security Technologies

Advanced Communications and Networking (Ethernet only)

The HandPunch® GT-400 can be configured to meet virtually any networking need or online operation. Each terminal comes standard with 10/100 Ethernet connectivity.

Programmable Soft Function Keys

The HandPunch GT-400 comes standard with eight ATM-style programmable soft function keys, making dynamic labeling a snap. Validation tables, multi-level prompting, decision menus, and punch reviews are just some of the functions that can be programmed into the terminal with these soft keys.

Large Display and LED Bar

The HandPunch GT-400 features a large 3.8″ QVGA display. This display gives users the ability to access more information per screen. The standard four-color LED bar provides users with instant visual feedback of punch verification and indicates online connectivity.

Levels of Integration

The HandPunch GT-400 enables users to integrate their time and attendance or payroll applications in many ways ranging from using the terminal's operating system to get transactions, to developing a complete end-to-end solution.

Platen, Keypad & Chassis Features

The platen, keypad and chassis of the HandPunch GT-400 are all integrated with an antimicrobial agent to ensure protection through the punching process. The platen also comes standard with a printed hand outline to ensure accurate hand placement while punching.

Specifications

Part Number	GT-400 (standard model w/ Ethernet) MTR-G Multi-Technology Card Reader Option
Size	8.0 in (20.32 cm) wide 11.18 in (28.40 cm) high 7.52 in (19.10 cm) deep
Weight	5.8 lbs (2.63 kg)
Power	10.8 to 13.5 VDC
Environment	Operating: 32˚F to 113˚F (0˚C to 45˚C) Relative Humidity: 5% to 85% NC Non-operating (storage): 14˚F to 140˚F (-10˚C to 60˚C)
Verification Time	Less than one second
Template Size	20 bytes
Communications	Standard Ethernet 10/100 RJ-45 type connector
Data Management Keys	8 programmable soft keys, user definable, supports: Validation Tables Employee Information Fields Multi-Level Prompting Key Restriction by Employee Decision Menus & Punch Review
Miscellaneous Options	BB-300 Battery Backup GX-ENCL Enclosure INT-HTR-G Integrated Heated Platen
Internal Credential	The MTR-G supports the following credential technologies: 125 kHz technologies supported: • GE/CASI ProxLite® • HID® Proximity • AWID® Proximity • LENEL® Proximity 13.56 MHz technologies supported: • ISO 14443 aptiQ™ featuring MIFARE DESFire™ EV1 (with PACSA enabled) • ISO 14443 aptiQ™ featuring MIFARE® Classic • ISO 14443 PIV (FASC-N output options) • ISO 14443 PIV-1 (GUID output options) • CSN for HID iClass®, ISO 15693, ISO 14443
Development Options	Integrate the Schlage Time and Attendance terminal application with our host Port or develop your own application on the terminal and integrate with your host

aptiQ™ Smart Technology from Ingersoll Rand enhances the intelligence of products through a secure, open architecture design in readers, credentials, and smart phone applications. aptiQ™ seamlessly interfaces and communicates with a variety of products, and provides a platform that easily adapts as new innovations enter the marketplace.

Ingersoll Rand
Security Technologies

Schlage

Electronic security

Biometric Solutions

Application Notes / Technical Bulletins

Master Index

3rd Party Biometric Testing on the HandReader

The HandReader has existed for over 20 years and has seen consistent and superior biometric performance. However, some error rates seen at a particular site are very dependent on several factors, most notably:

- population
- training and habituation
- threshold setting

Due to the variability of factors involved at individual sites, Allegion does not quote static performance rates. However, we often refer customers to two well-respected tests run by independent third-parties. The attached documents describe test methodology and state the corresponding performance metrics. Customers with similar use case environments can reasonably expect similar results.

In brief summary, the attached reports will show the following 3-try results:

a.	Type I error rate (false rejection rate) -		
	as low as	<0.1% (Sandia)	0.25% (CESG)
b.	Type II error rate (false acceptance rate) -		
	as low as	0% (Sandia)	0.001% (CESG)
c.	Crossover error rate (CER) -		
	as low as	0.1% (Sandia)	0.5% (CESG)

The two reports are attached for your reference.

CESG Biometric Product Testing Final Report
Sandia Report

CESG contract X92A/4009309

Biometric Product Testing Final Report

Issue 1.0
19 March 2001

Tony Mansfield
Gavin Kelly
David Chandler
Jan Kane

Centre for Mathematics and Scientific Computing
National Physical Laboratory
Queen’s Road
Teddington
Middlesex
TW11 0LW

Tel: 020 8943 7029
Fax: 020 8977 7091

EXECUTIVE SUMMARY

This is a report of a performance evaluation of seven biometric systems conducted by NPL over the period May to December 2000. The test programme was sponsored by the Communications Electronics Security Group (CESG) as part of their Biometrics Work Programme in support of the "Modernising Government" and other initiatives.

The objectives of the test programme were:
- To show the level of performance attainable by a selection of biometric systems;
- To determine the feasibility of demonstrating satisfactory performance through testing;
- To encourage more testing to be sponsored, and to promote methodologies contributing to the improvement of biometric testing.

Face, Fingerprint, Hand Geometry, Iris, Vein and Voice recognition systems were tested for a scenario of positive identification in a normal office environment, with cooperative non-habituated users. The evaluation was conducted in accordance with the "Best Practices in Testing and Reporting Performance of Biometric Devices" produced by the UK Government Biometrics Working Group, and used 200 volunteers over a three-month period.

Results presented include:
- Failure to Enrol and Failure to Acquire Rates;
- The trade-off between matching errors (False Match Rate vs. False Non Match Rate) and between decision errors (False Acceptance Rate vs False Rejection Rate) over a range of decision criteria;
- Throughput rates of users in the live application, and of the matching algorithm in off-line processing;
- Sensitivity of the systems' performance to environmental conditions, and the differences in performance over different classes of users.

Biometric system performance is dependent on the application, environment and population. Therefore the performance results presented here should not be expected to hold for all other applications, or in all environmental conditions. In particular caution should be exercised when comparing these results with those of other systems tested under different conditions.

CONTENTS

FIGURES

TABLES

1 INTRODUCTION

1. This is a report of a performance evaluation of seven biometric systems conducted by NPL over the period May to December 2000. The test programme was sponsored by the Communications Electronics Security Group (CESG) as part of their Biometrics Work Programme in support of the "Modernising Government" and other initiatives.

2. The test programme had three main objectives:
   a. To show the level of performance attainable by a selection of biometric systems;
   b. To determine the feasibility of demonstrating satisfactory performance through testing;
   c. To encourage more testing to be sponsored, and to promote methodologies contributing to improvement of biometric testing.

3. The tests provide factual, vendor-independent data on the performance of biometric devices. This will inform CESG on the general capability of biometric technology, and will help in the development of policy on the use of biometrics in Government. It will also assist members of the UK Government Biometrics Working Group (BWG) in the assessment of the applicability of biometric technology to their potential applications.

4. The tests will implement and validate the BWG proposed methodology for biometric testing. The outcome will support the further development of this methodology for use with Common Criteria evaluations of biometric products and systems.

5. It is also hoped that this initial evaluation will, by example:
   a. Promote the methodology to a wider audience and contribute to the improvement of biometric testing by other organisations; and
   b. Encourage further testing to be sponsored.

   To allow wider dissemination of the results (given that open publication of results was not a requirement for vendors participating in the trials), the report has been organised into two parts with different restrictive markings. The intention is that Part I excludes any commercially sensitive information and can be made publicly accessible, while Part II contains full details for CESG and Government Departments.

2 SELECTION OF SYSTEMS

6. The Test Programme was announced on the Biometrics Consortium list server, and some thirty companies responded to the call for submission of devices for testing. Because of overlap in terms of devices proposed, about twenty different systems were considered for inclusion in the test programme.

7. The criteria for selection of systems to test were agreed by CESG and the Biometrics Working Group.
   a. Fingerprint, hand and iris technologies must be included. Other systems tested should use different technologies, except for fingerprint where two systems might be tested.
   b. Within a technology, selection should be on the basis of wide availability and commonality of use.
   c. Systems should be capable of meeting basic CESG performance requirements.
   d. Systems should be testable under the agreed methodology (and, implicitly, the system performance should not be adversely affected by the proposed test protocol).
   e. The vendor should be able to support the trials within the required timescales.

8. Using these criteria, seven systems were selected for testing, using face, fingerprint, hand geometry, iris, vein pattern, and voice and recognition. There were two fingerprint systems: one using optical fingerprint capture, the other a chip sensor. Table 1 gives brief details of the tested systems. Systems have been named where vendors are happy for their results to be publicly available. (Full details of all systems are given in Part II of this report, which has a more restricted circulation.).

Short name	Brief description
Face Face (2)	Visionics – FaceIt Verification Demo Alternative enrolment and matching algorithms for this system
FP-chip FP-chip (2)	VeriTouch – vr-3(U) Alternative enrolment and matching algorithms provided by Infineon
FP-optical	*Fingerprint recognition system.*
Hand	Recognition Systems – HandKey II
Iris	Iridian Technologies – IriScan system 2200
Vein	Neusciences-Biometrics – Veincheck development prototype
Voice	OTG – SecurPBX Demonstration System

Table 1. Brief details of systems tested

9. As there is just one device per technology, it should be noted that the performance results presented are not necessarily fully representative of all systems of the same type. Indeed, even relatively minor modifications to the systems tested can give considerably different performance.

3 TEST SCENARIO

10. The test scenario was one of positive verification in a "normal office environment", with co-operative non-habituated users. The tests were conducted with 200 volunteers, over a three-month period. The typical separation between enrolment and a verification transaction was one to two months.

3.1 Volunteer crew

11. To obtain participants, a call for volunteers was issued by e-mail and in the NPL in-house newsletter. A small payment offered as an incentive for participation (and adherence to the trial "rules"). All those responding were invited to participate, though some withdrew when they could not attend an appointment for enrolment. A limited further call was issued to some staff of the other laboratories on site (NWML and LGC) to achieve slightly over 200 participants. The volunteer crew were thus self-selecting, consisting mostly of staff working on the NPL site. The age and gender profile is shown in Figure 1. This approximates that of the workforce on site.

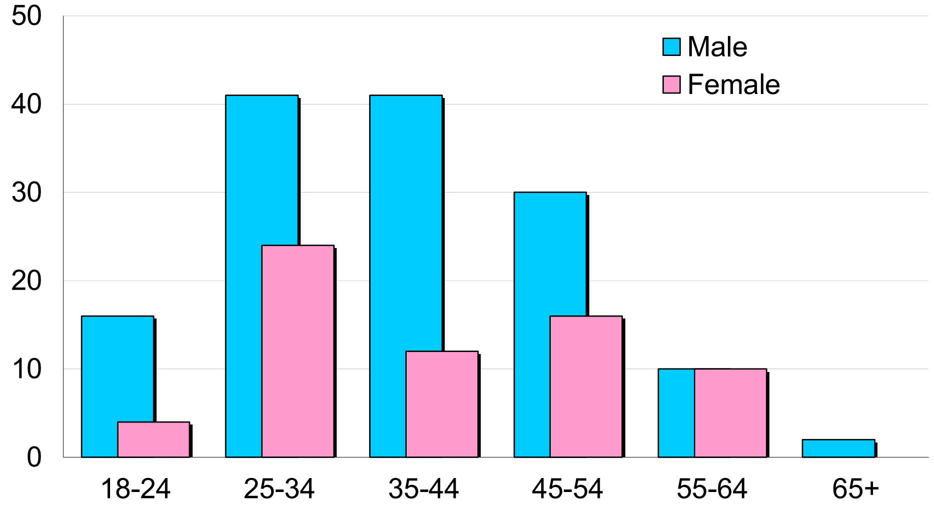


Figure 1: Age and gender of volunteer crew

12. This volunteer crew is not fully representative of the general UK adult population. Women and those older than 45 are under-represented, also the balance between different ethnic

groups is probably incorrect (ethnic origin of volunteers was not recorded). Moreover, as the volunteer crew are used to working in a scientific environment, they are more accepting of technology than the population at large. Potentially this might reduce errors due to the behavioural element in biometric system use.

3.2 Environment.

13. The tests were conducted in a room previously in normal office use.

14. Lighting levels were controlled. The room's fluorescent lighting was always on, and the window blinds kept down to reduce effects of daylight variations. The devices were sited in accordance with recommendations of the product suppliers, and those most sensitive to changes in illumination were positioned away from the window. Similarly one device whose use was sensitive to background noise was located in a quieter area off the main test laboratory. These adjustments are documented with the test results for each device.

15. The temperature and humidity of the test laboratory were not controlled. Figure 2 indicates how outdoor temperature[1] and humidity[2] varied between the days of the trials

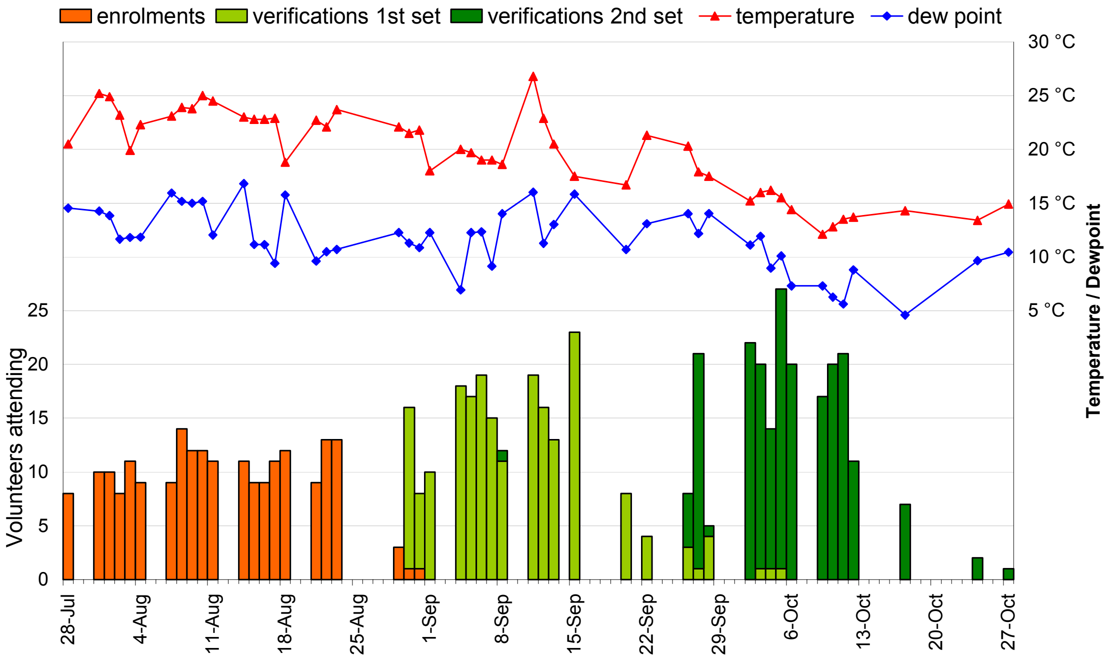


Figure 2. Environmental conditions during the trials

3.3 Enrolments & verifications

16. Figure 2 also shows the daily distribution of enrolment and verification transactions. On average the first set of verifications was made 29 days after enrolment, and the second set of verifications, 55 days after enrolment.

3.3.1 Order effects

17. The order in which the devices were used could potentially affect performance.

[1] Figures based on readings from local weather station.

[2] Dew point is plotted instead of relative humidity. This removes the strong (inverse) correlation with temperature, and to allows the same °C scale to be used.

a. On arriving at the test laboratory, volunteers could be out of breath (if they have hurried to make their appointment) or have cold hands/fingers (when cold outside), recovering to a more normal state after a few minutes.

b. The illumination for the face recognition system increased the amount of iris visible (i.e. reduces pupil size) with a potential effect on iris recognition when this occurs shortly after.

c. Feedback from one fingerprint device might affect user behaviour (e.g. finger pressure) on the other.

18. Other than volunteers attempting speaker verification when out of breath, these order effects did not appear significant. Further order effects may also exist, but are also believed to be insignificant. In view of this, a complex fully randomised sampling plan was not adopted.

a. Transactions on the Voice system were not conducted until the volunteer had regained their breath.

b. The order in which the devices were used alternated between a clockwise order around the room, and anti-clockwise. However, this ordering was often modified to avoid queuing at any system. There were no order correlations between visits.

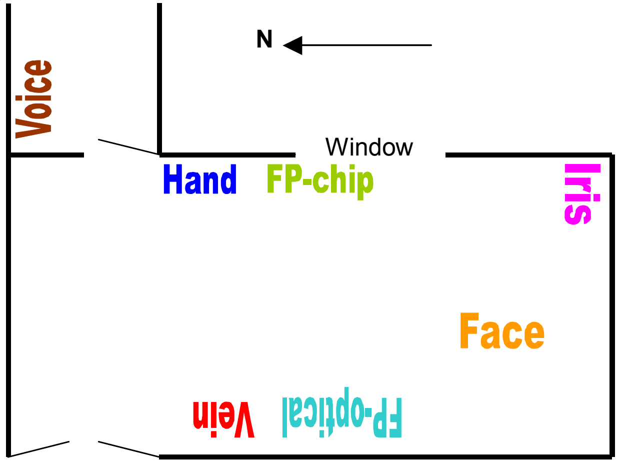


Figure 3. Positioning of systems in test laboratory

4 TEST METHODOLOGY

19. The performance trials were conducted in accordance with

Best Practices in Testing and Reporting Performance of Biometric Devices[3]

produced by UK Government Biometrics Working Group. The test protocol followed is described in

A test protocol for the Technical Performance Evaluation of Biometric Devices

For completeness this Test Protocol is included in Appendix A.

20. Modifications and enhancements to the general test protocol are discussed below.

4.1 Dealing with enrolment failures

21. Observations during preliminary testing showed:

a. Often more than two attempts would be required to obtain an enrolment. This seemed to be particularly the case with the Voice and both Fingerprint systems, where obtaining a good quality "image" is more dependent on user behaviour and familiarity.

b. For some systems, the enrolment software did not provide for re-enrolment. In such cases, problem enrolments needed to be deleted, using the underlying operating system, before re-enrolment was possible. For data-integrity reasons, we were reluctant to do this

[3] Available at http://www.cesg.gov.uk/biometrics/

while under the pressure of processing volunteers, and as a result re-enrolments had to occur on a subsequent visit.

c. Some systems did not automatically record every enrolment attempt failure.

22. The protocol for dealing with enrolment failures was therefore modified. Where practical, immediate re-enrolment was attempted, (as previously). However, at subsequent visits, whenever a volunteer had failed to enrol on one of the devices, they were asked to try re-enrolling regardless of the number of previous enrolment attempts.

4.2 Avoiding data collection errors

23. Additional procedures were put in place to help avoid data collection errors:

a. Errors due to the use of the wrong hand, finger, etc.

b. Errors due to attributing the attempt to the wrong identity.

4.2.1 Avoiding use of wrong hand, finger, etc.

24. Users were asked to always use their right index finger, eye or hand as appropriate. Without this consistency, it would be difficult for supervisors to observe and prevent use of the wrong finger, hand or eye at enrolment or verification. The saved images allow further checks that the correct iris, hand or finger was used, though this is easier for iris and hand images than for fingerprint images.

4.2.2 Avoiding attribution of attempt to wrong identity.

25. Each user was allocated a PIN for the trials, which was shown on the named data sheet collected by the user at each session (see e.g. Appendix C). The following possibilities for attributing attempts to the wrong identity must be addressed by checking procedures.

a. The user picks up the wrong data sheet[4].

b. The user mistypes their PIN, producing another valid PIN[5].

c. The user forgets to enter their PIN on a system where the PIN is not cleared between attempts. As a result the attempt is made against the previous user's identity[6].

These were addressed as follows.

26. **Feedback on claimed identity**
The Voice, Face and Iris systems provided feedback on the claimed identity. This would show the individual and supervisor that failures were due to the wrong PIN being used.

27. **Error detecting PINs**
The PINs used to claim an identity were chosen to minimise the chance that mistyping would produce another valid identity. This was done using the ISBN error-detection scheme (though avoiding use of "X" as the check digit). The 4-digit PINs `abcd` have the property that `4a+3b+2c+d` is exactly divisible by eleven. This detects all single digit errors and transpositions. From the available PINs, the set used was as widely spaced as possible, in the range 1000 – 9999, giving robustness against more complex typing errors.

28. **User makes at least 3 attempts per device per session**
If a PIN not being entered causes attempts to be recorded against the previous user's identity, these will be the 4th or subsequent attempts. However, these will be ignored as only the first 3 attempts per user per session are analysed.

29. Any incorrect attempts were recorded on the user's data sheet, allowing for annotation of the logged data and exclusion from analysis. Where possible, prior to conducting analyses, the

[4] This happened twice (of a possible 412 occasions), where the volunteers had very similar names.

[5] One of the systems recorded when incorrect PINs were entered. Of some 2000 entered PINs, 5 were entered incorrectly. Two single digit errors, one transposition, and two 2-digit errors.

[6] This could happen on three of the systems tested, occurring twice, once, and no times (of a possible approx 400 occasions).

data saved for verification failures were checked further, to determine if the cause of failure was a mis-acquisition or a mis-labelling.

5 RESULTS OVERVIEW

5.1 Failure to enrol

30. The "failure to enrol" rate measures the proportion of individuals for whom the system is unable to generate repeatable templates. This includes those unable to present the required biometric feature (for example the Iris system failed to enrol the iris of a blind eye), those unable to produce an image of sufficient quality at enrolment, as well as those unable to reproduce their biometric feature consistently. Enrolment failure rates for the systems tested are shown in Table 2. Note that, in cases of difficulty, several attempts were allowed to achieve an enrolment. If necessary, these further enrolment attempts were made at subsequent visits by the volunteer.

System	Failure to enrol rate
Face	0.0%
Fingerprint – Chip	1.0%
Fingerprint – Optical	2.0%
Hand	0.0%
Iris	0.5%
Vein	0.0%
Voice	0.0%

Table 2. Failure to enrol rates

5.2 Failure to acquire

31. The "failure to acquire rate" measures the proportion of attempts for which the system is unable to capture or locate an image of sufficient quality. This includes cases where the user is unable to present the required biometric feature (e.g. having a plaster covering his or her fingerprint); and cases where an image is captured, but does not pass the quality checks. Failure-to-acquire rates for the systems tested are shown in Table 3. The figures exclude cases where the image was not captured due to user error (e.g. the user not positioning themselves correctly) as in these cases the attempt was simply restarted.

System	Failure to acquire rate
Fingerprint – Chip FP-chip (2)	2.8% 0.4%[7]
Face	0.0%
Fingerprint – Optical	0.8%
Hand	0.0%
Iris	0.0%
Vein	0.0%
Voice	2.5%

Table 3. Failure to acquire rates

5.3 False match rate (FMR) vs false non-match rate (FNMR)

32. The fundamental operation of a biometric system is the comparison of a captured biometric image against an enrolment template. The false match and false non-match rates measure the

[7] For verification, minimal quality checks were performed.

accuracy of this matching process. By adjusting the decision criteria there can be a trade-off between false match and false non-match errors; so the performance is best represented by plotting the relationship between these error rates in a detection error trade-off graph.

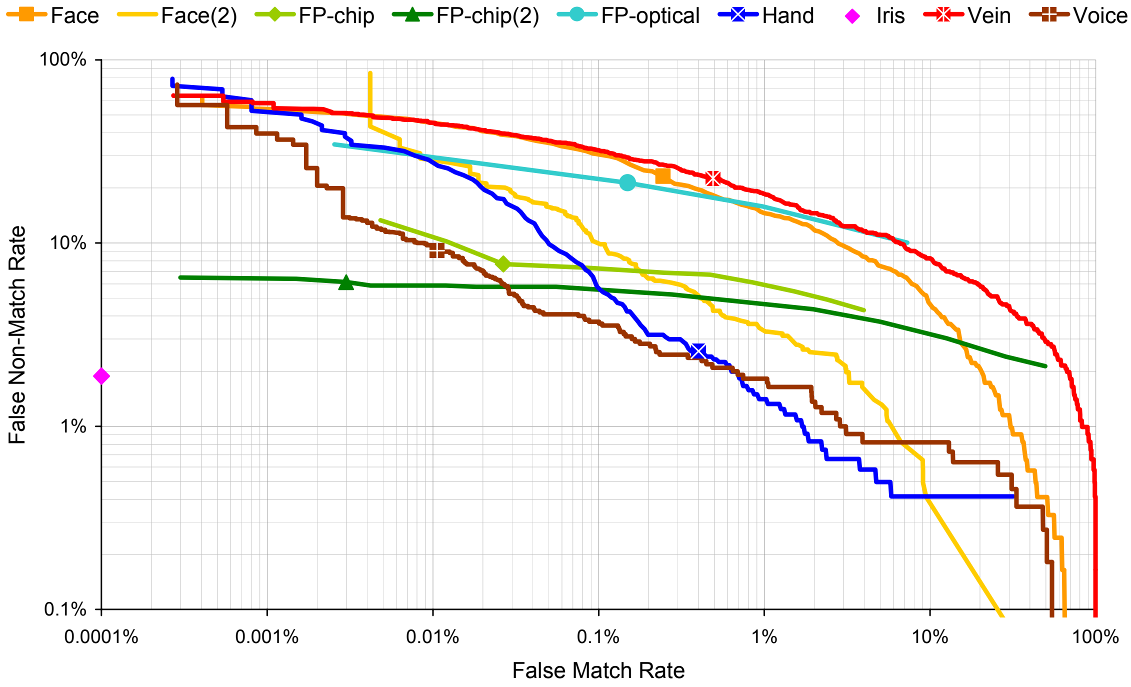


Figure 4. Detection error trade-off: FMR vs FNMR

33. Matching algorithm performance for each system, over a range of decision criteria, is shown in Figure 4. (The lower and further left on the graph, the better the performance). The node on each curve shows performance at the default decision threshold. No curve is shown for the Iris system, which operates with a pre-determined threshold. The iris system had no false matches in over 2 million cross-comparisons. For all the other systems the leftmost point on each curve represents a single false match in the total number of cross-comparisons made.

34. Observing images corresponding to false non-matches showed that some of matching failures were due to poor quality images. Systems vary in how they deal with poor quality images, some will "fail to acquire" such images, while systems will often cope with poor image quality. Therefore the matching error rates should not be considered in isolation from the failure to acquire and failure to enrol rates.

5.4 False acceptance rate (FAR) vs. false rejection rate (FRR)

35. False acceptance and rejection rates measure the decision errors for the whole system. These measures combine matching error rates, and failure to acquire rates in accordance with the system decision policy. When the verification decision is based on a single attempt:

$$\mathrm{FAR}(\tau) = (1\text{-}\ \mathrm{FTA})\ \mathrm{FMR}(\tau)$$
$$\mathrm{FRR}(\tau) = (1\text{-}\ \mathrm{FTA})\ \mathrm{FNMR}(\tau) + \mathrm{FTA}$$

where τ is the decision threshold, and FMR, FNMR, FTA, FAR and FRR are the false match rate, false non-match rate, failure to acquire rate, false acceptance rate and false rejection rate respectively.

36. The false acceptance false rejection trade-off curve is shown in Figure 5. The curves for the face, hand geometry, iris and vein systems are unchanged, as these systems had no failures to acquire.

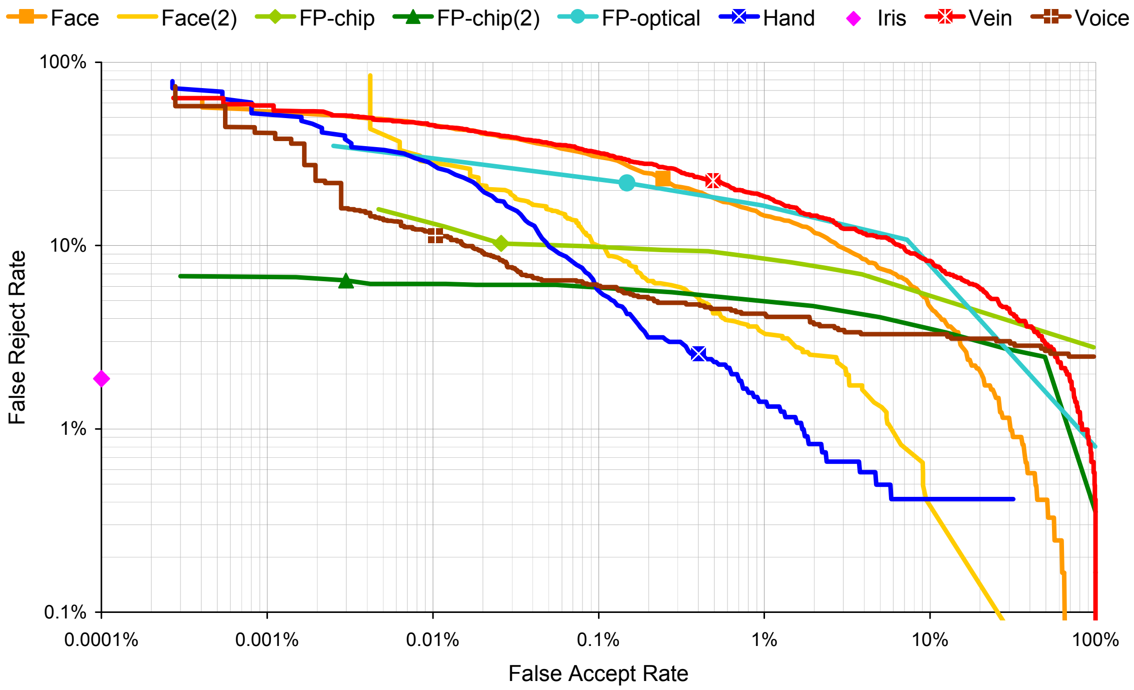


Figure 5. Detection error trade-off: FAR vs FRR

5.5 Multiple attempt error rates

37. Many systems allow multiple attempts, in their normal mode of operation. The effects on error rates of a "best-of-3" decision policy are examined in this section.

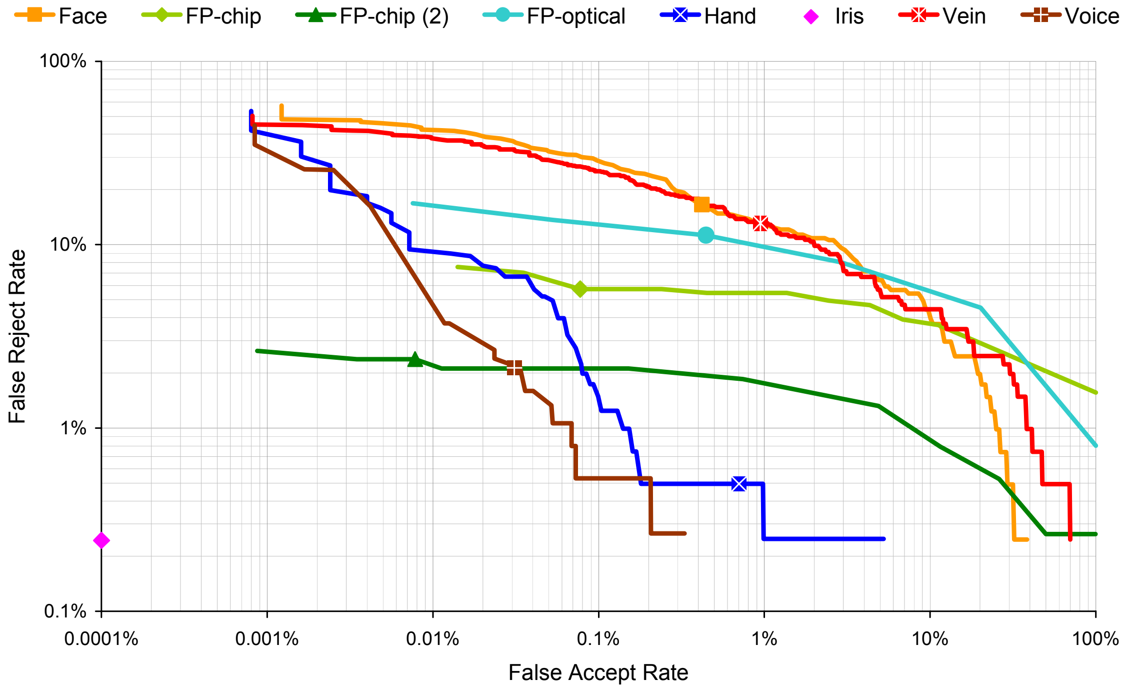


Figure 6. Detection error trade-off: Best of 3 attempts

38. The 3-attempt genuine and impostor scores are the best matching score from the 3 attempts made at the person-visit (scored against the chosen template). The resulting detection error trade-off (DET) curves are shown in Figure 6.

39. This method of obtaining the DET curve is appropriate when all attempts are constrained to use the same finger, face or hand etc. In real life, it may be possible to substitute a different finger, face, hand, etc at the second or third attempt. If so (and assuming the individual impostor attempts are fully independent) the 3-attempt false acceptance rate at any decision threshold is given by $1-(1-\alpha)^3$ where α is the false acceptance rate for a single attempt at the same threshold. Thus, two detection error trade-off curves may be shown:

a. Where all three attempts are constrained to use the same finger, hand, face, etc; and
b. Where substitutions are allowed between attempts.

In the case of the trial systems and data, the two curves follow each other closely[8], so Figure 6 shows a single curve for each system[9].

5.6 User throughput

System	Transaction Time (Seconds)			Time includes entry of PIN?
	Mean	*Median*	*Minimum*	
Face	15	14	10	Excluded
Fingerprint-Optical	9	8	2	Excluded
Fingerprint-Chip	19	15	9	Excluded
Hand	10	8	4	Included
Iris	12	10	4	Included
Vein	18	16	11	Included
Voice	12	11	10	Excluded

Table 4. User transaction times

40. The time for a user transaction has been calculated using the time differences logged between consecutive transactions (as detailed in Appendix A.6.7). Table 4 shows the mean, median and minimum transaction times to indicate the spread of results. The differences in operation of the trial systems accounts for much of the difference in timings.

a. The Face system collected a sequence of images over a 10 second period, saving the best match obtained. The transaction times would be somewhat shorter if the system stopped when the threshold was first exceeded; however, this would not have allowed us to examine performance over a range of decision thresholds.
b. The Iris system would normally work in identification mode, not requiring PIN entry. This would reduce transaction times.
c. The keypad of the Vein system could not cope with rapid entry of the PIN. The time to do this dominates the overall transaction time.
d. The transaction times for the Voice system were dominated by the time taken in giving user prompts and feedback. The prompting and speeds were chosen to be suitable for users unaccustomed to the system, rather than for maximum throughput.

5.7 Matching algorithm throughput

41. The measured throughput of the programs for batch mode running of the matching algorithms is shown in Table 5. These diagnostic programs had significant overheads, for example logging all matching attempts to a file, or handling the Windows interfaces. Therefore, the matching algorithm throughput may be significantly higher than those shown, perhaps by a factor exceeding 100. (In the case of the chip-based fingerprint system, the difference in throughput of the two diagnostic programs illustrates the improvement possible. In an

[8] The ratio FAR_b/FAR_a of the false acceptance rates derived under the different assumptions varies from 1 to 1.3 for the voice system and fingerprint systems; from 1 to 1.7 for the vein system, and from 1 to 2 for the hand and face systems.

[9] For the FP-chip, and FP-optical systems, a cross-comparison scoring of all attempts against each template was not available, and the curve shown is derived as detailed in paragraph 39. For FP-chip (2) and all the other systems, the curve was derived using a full set of genuine and impostor scores.

equivalent implementation, the basic FP-chip algorithm would be faster than the more complex alternative FP-chip(2).)

System	Matches per minute	Program interface	System, processor speed, memory, & OS			
Face	800	Windows	Pentium			Win2K
FP-chip	60	Windows	Pentium	133MHz	32Mb	Win98
FP-chip (2)	2,500	Command Line	Pentium	500MHz	64Mb	Win95
FP-optical	50	Windows	Pentium	500MHz	64Mb	Win95
Hand	80,000	Command Line	SunUltra5	270MHz	128Mb	SunOS5.8
Iris	1,500,000	Command Line	SunUltra5	270MHz	128Mb	SunOS5.8
Vein	130	Windows	Pentium	500MHz	64Mb	Win95
Voice	680	Command-Line	Pentium	500MHz	64Mb	Win95

Table 5. Diagnostic program throughput

5.8 Performance differences by user & attempt type

42. Attempts can be categorised by:

a. Whether made at enrolment visit or at the second or third visit by the volunteer;
b. The gender of the volunteer;
c. The age of the volunteer;
d. Whether the volunteer was wearing spectacles in the case of Face and Iris systems;
e. The length of the user's pass-phrase in the case of the Voice system.

Performance differences between these subsets have been analysed, and are reported for each system in Part II. The general findings are summarised in Table 6.

System	Gender	Age	Visit	Other
	Observations:		lowerFRR<higherFRR	Less significant
			lowerFRR<higherFRR	**More significant**[10]
Face	**male<female**	younger<older	**enrol<later**	without<with glasses
FP-chip	male<female	**younger<older**	**enrol<later**	
FP-chip(2)	male<female	younger<older	enrol<later	
FP-optical	male<female	**younger<older**	**enrol<later**	
Hand	male<female			
Iris				without<with glasses
Vein	**male<female**	younger<older	**enrol<later**	
Voice	female<male	younger<older	**enrol<later**	

Table 6. Summary of performance differences by user type

43. False rejection rates for attempts made immediately following enrolment were generally significantly lower than (less than half) those made at volunteer's second or third visit.

44. Generally men had a lower false rejection rate than women (the voice system being the only exception), and younger volunteers a lower false rejection rate than their older colleagues. The gender differences appeared the more significant for the Face, Hand and Vein systems, and the age differences the more significant for the Fingerprint systems.

45. As women and over 45's were under-represented in our volunteer crew, our results may be biased. For a given threshold, with equal numbers of men and women, a slightly higher false non-match rate might be expected. However since false matches are more likely within the same gender class, the equalisation would reduce the false match rate at the same threshold.

[10] The more significant observations have a χ^2 value exceeding 15. (See Appendix D for details.) The probability of such observations being due to the random nature of the sample is in the range 0.01% - 20% dependent on the degree of correlation between different attempts by the same person.

6 VALIDATION OF METHODOLOGY & FUTURE ENHANCEMENTS

46. The evaluation has implemented the BWG proposed methodology for biometric testing, validating many aspects of this methodology. For example:

a. Demonstrating the feasibility of the methodology;

b. Showing that the number of volunteers used (200) is sufficient to evaluate performance of biometric systems at their current level of accuracy;

c. The practical significance of issues described in "Best Practices" has been demonstrated:
The need for time separation between enrolments and verification attempts;
The need to minimise the chance of labelling errors;
The modified procedures to simulate unknown impostor attempts when there are dependencies between templates.

A single evaluation cannot demonstrate repeatability of the results. However, some of the devices evaluated have been tested elsewhere in similar scenarios, and the results are consistent.

47. The evaluation revealed further issues concerning the applicability of the test protocol, and enhancements to best practices. These are noted below.

6.1 The requirement for additional system functionality

48. The test protocol required systems to save data for off-line calculation of genuine and impostor matching scores. This capability is often not provided in a vendor's standard supplied system. This raises the following issues:

a. Some systems will be unable to meet this requirement for testing (for example standalone systems which store templates are stored locally, but have insufficient memory to log transaction attempts). This point was raised by some of the vendors who initially expressed an interest in participation in the trials.

b. When the required functionality is achievable with vendor support, it is important that protocols are sufficiently consistent across testing organisations. Otherwise the vendor needs to develop a different customisation for each test, and support costs can be very significant.

c. Sometimes achieving the desired functionality can affect system performance. For example the time taken in logging images may slow the system and affect user behaviour. It is also possible that implementing the required functionality at minimal cost will introduce errors into the system.

49. If all testing, including impostor tests, are conducted "live" these problems are avoided. However, this requires:

a. Data collection to be very closely supervised as all results must be logged by the supervisor;

b. Extra attempts to be made to show performance at a variety of decision thresholds; and

c. Extra attempts to be made for live impostor tests.

6.2 One attempt may involve a sequence of images

50. With many biometric systems, a sequence of images is processed in a single verification attempt. For example, with the trial system it appears that:

a. The Face system collects images over a period of 10 seconds, and gives the best match obtained;

b. The Chip-based Fingerprint system collects images until a match is obtained, or until timeout;

c. The Optical Fingerprint system scans for fingerprints until an image of sufficient quality is obtained, or the timeout is reached;

d. The Hand Geometry system occasionally requires a second hand placement, when the score is very close to the decision threshold;

e. The Iris system collects images until a match is achieved or until timeout.

51. The current version of “Best Practices” does not explicitly deal with these cases, yet this mode of operation can sometimes bias off-line calculations using the collected data. For example with the face system, in a real impostor attempt the score would be based on the image that best matches the impersonated template. A cross-comparison of stored genuine images uses the image that best matches the genuine template, and therefore may underestimate the false match rate.

52. The questions that must be addressed are:

a. Would the decision be based on a different image if comparison were against a different template?

b. If so, would live impostor attempt scores be higher/lower than off-line scoring with genuine attempt images?

In the case of the tested Optical Fingerprint, Hand Geometry and Iris systems, the image collected does not depend on the template being matched. With the Fingerprint Chip, the collected image might instead be last before timeout; and, apart from image quality, should be equivalent to the image saved from a genuine attempt.

6.3 Failure to acquire

53. As noted in Section 5.3 (paragraph 34), different systems handle poor quality input in different ways. With some systems this may result in a failure to acquire, and with others a matching failure. In this respect the FAR-FRR trade-off graph provides a better comparison of performance than the FMR-FNMR trade-off graph.

6.4 Other performance trade-offs

54. Systems may have other adjustable parameters affecting performance in addition to (or instead of) an adjustable decision threshold. These allow different performance trade-offs (which, depending on the application, may be more important than the FAR-FRR trade-off). For example, with the Face, Iris, and Chip-Fingerprint systems, which try to match collected images over a fixed time period, there is a trade-off between the time allowed and the false rejection rate.

APPENDIX A. TEST PROTOCOL

A.1 Introduction

This report describes the test protocol planned for the UK Government Biometric Test Programme. The protocol is for "scenario testing" and conforms to the guidelines in "Best Practices in Testing and Reporting Performance of Biometric Devices". The protocol is intended to be practical in terms of effort and costs, and applicable to many of today's commercially available biometric devices when operating in their intended environments.

Several systems will be tested at the same time, in a standard indoor (office) environment and using a volunteer crew similar to the general adult UK population. The trials will involve approximately 200 volunteers using each of the systems being tested. Volunteers will attend the trials on three occasions: firstly for enrolment and practice attempts; and later, one and two months after enrolment, to collect "genuine" attempts Detection Error Trade-off (ROC) analysis.

Impostor attempts will be simulated using cross-comparison of genuine attempts against enrolment templates for other enrolees. This will be carried out off-line using vendor-provided software with the collected enrolments and genuine-attempt images and data.

A.1.1 Applicability of this protocol

Biometric limitations — The protocol cannot be used if it takes much longer than a few seconds for the system to extract the required biometric features. For example we could not test a system that uses 10 minutes of typing at a keyboard to make an identity decision. The separation between enrolment and test attempts will be approximately 1 month. If we are interested in the effects of template ageing time over a timespan much greater than this, the protocol may also be inappropriate.

System functionality — We can only test complete systems. These must be able to operate in "verification" mode, matching a single attempt against a single stored template. It is also necessary for the system to log specific information about each attempt, and there must be a capability for off-line generation of matching scores

System Error Rates — We shall not be able to measure error rates to values of 1% or below with any certainty. For example, if 1% of the population have (or lack) some feature causing enrolment failure, there is a 13% chance that no-one in a 200 person sample have that peculiarity. On the other hand to measure error rates exceeding 10% we may be using more volunteers than required, and a smaller test may be more cost effective.

A.1.2 Modelled Scenario

The scenario modelled is that of a verification application in an indoor environment.

Co-operative users — It is hard to replicate the actions and motivations of an uncooperative user.

Overt system — We shall be using volunteers who will be brought to a specific location for testing, and who will test several devices. This effectively rules out covert testing.

Non-habituated users — Our volunteers will use the system a few times only, with gaps of a few weeks between each use. The level of habituation will therefore be quite low. We shall avoid using volunteers who have extensively used one of the systems under test, so that comparisons are fair. We do not propose replicating a higher level of habituation by allowing practice attempts: this would create additional complexities to be able to separate practice attempts from the real test attempts.

Supervised enrolment, lightly-attended use — Enrolment will be supervised. Subsequent attempts will be lightly attended: there will be someone on hand to sort out problems should these occur. However, it should be noted that, after enrolment, the main role of the supervisor is to ensure the integrity of the data collection process rather than to assist volunteers in their attempts.

Standard environment — The tests will be conducted indoors, in a standard office environment. It is harder, and more costly to conduct the trials in an outdoor environment, and currently relatively few devices will operate satisfactorily in an outdoor environment.

Public users (UK adults) — Volunteer user attitudes are likely to be closer to those of the general public, than that of company employee. Also, volunteers will be local to the testing laboratory, and their biometric features will reflect the UK demographics. Results may be different with other population demographics. We note that our volunteers are probably more scientifically aware (and perhaps better able to follow instruction) than the general public.

Closed system — We shall enrol and test using the same system. Note that if the system would normally used several sensors, where there are considerable variations between sensors, the proposed protocol may not be appropriate.

A.1.3 Performance Measures

The proposed tests will measure the following aspects of performance (where applicable).

- Failure to enrol rate
- Failure to acquire rate
- Detection error trade-off graph (i.e. ROC)
- System false match and false non-match rates
- Penetration rate (where appropriate)
- Binning error rate (where appropriate)
- User throughput
- Matching algorithm throughput (reported with processing system used)
- Sensitivity of performance to (potentially problematic) changes in environment, population, or usage

A.2 Device setup

We allow vendor involvement during device set-up to help ensure that the systems are correctly installed and operating optimally.

A.2.1 Install systems & familiarisation

The complete system will be installed at the test site. Account will be taken of vendor recommendations regarding positioning, illumination, and background noise etc. in so far as these are realistically achievable in a general office/indoor environment. Threshold, image quality and other settings will be set in accordance with vendor advice.

A.2.2 Test sensitivity of performance to environment, population, usage

Some pre-trial tests will be carried out to determine environmental and other factors that may cause problems. This will be a limited investigation, mainly using the testing team. The aim is to determine:

- what potential problems exist,
- if these problems are controlled by the system,
- how significant the problems appear to be,
- whether we need to impose environmental or other controls to minimise the problem during the trials,
- what additional information we need to record to identify difficult subsets of volunteers during subsequent analyses.

Some of the potential sensitivities to test, and what may be done to analyse or control any problems are shown in the following table:

Technology	Effect to test	If effects seem significant
All	age, gender, template-ageing	Compare of error rates for different subsets of volunteers/attempts
All	lighting level & direction	Control lighting levels during trial
All	dirt/smears on sensor	Set policy for cleaning devices
All	movement during attempt	Provide appropriate instructions for volunteers
All	positioning	Provide appropriate instructions for volunteers
Fingerprint	Dry / cold / cracked / damp / wet fingers	Advise volunteers on improving fingerprint quality. Record temperature & humidity
Hand geometry	rings, plasters, etc.	Log attempts made with rings etc. Provide separate error rates for these cases
Iris, Face	Glasses	Record those who wear glasses/contact lenses Provide separate error rates for these cases

A.2.3 Set enrolment & transaction attempt policies

The enrolment policy will be set to deal with the problems identified, with the aim of achieving the greatest number of good enrolments.

The supervisors who will conduct enrolment will be trained and familiar with each system and its common problems.

A.2.4 Produce system information for volunteers.

For each system, a short description of how the system operates, and how it should be used will be prepared in consultation with the system vendor. This is to reduce the burden of describing full details of the systems at enrolment, and before later transaction attempts.

A.3 Volunteer crew

A call for volunteers will be issued. To encourage participation a small reward will be offered. If more than 200 people volunteer, participants will be selected at random from the volunteers.

Before enrolment participants will be informed of the purpose of the trials, what is required of them, and what information will be collected and stored. They will be asked to sign to give their consent to the collection of biometric images and information, and to confirm that they have not previously used any of the devices being tested. Age category and gender of participants will be recorded, together with any information found useful in identifying problem cases in the preliminary trials.

A.4 Enrolment

Each participant will attempt to enrol on each system under test. The order of enrolment on the devices being tested will be randomised. Only one set of equipment will be used for each system to avoid "channel" effects. Enrolment will be conducted using the enrolment functions of the supplied systems, and will supervised by a member of staff who had been trained for this purpose.

Enrolment images will be collected by the system. *(We use the word image to refer to the actual input signal; this may not strictly be an image in the case of non-optical devices. If the system is unable to record actual enrolment images, it may be possible to conduct the required analyses using the image templates.)*

Immediately after enrolment, several attempts will be made to check that the participant can be reliably verified. Advice to help users achieve successful verifications will be given if necessary. If they cannot be reliably verified this shall count as an enrolment failure.

If enrolment fails, one re-enrolment will generally be attempted. *(In some cases it may be clear that subsequent attempts must fail, for example if the volunteer does not have the required biometric feature. In such cases no re-enrolment attempt would be made. In other cases the enrolment failure may due to a clearly identifiable error which can easily be overcome, for example failures due to not following the proper enrolment process. In such cases more than two enrolment attempts might be made.)*

Some systems allow an "override" to register a poor quality image as an enrolment template in cases of difficulty; such features will not be used. Any problems with enrolment will be noted by the enrolment supervisor.

Cases where the enrolment template cannot be generated, or where all practice attempts fail, are

considered to be failed enrolments. In these cases, subsequent verification attempts are not required of the participant on the device in question. Data from failed enrolments will be removed from the enrolment database and will not be used in analysing false match or false non-match error rates.

A.5 Test data collection

Volunteers will make two sets of transactions, at approximately one and two months after enrolment. On each occasion they should make (at least) three attempts. This will allow direct calculation of "best of three attempt" rejection rates, and can also reveal whether some users are much more error prone than others.

Attempts will be largely unsupervised, but there will be a supervisor on hand to help in case of difficulty. Users may observe attempts made by others, but will not be allowed to make practice attempts (apart from those they made as part of enrolment). This is to ensure that only the genuine transactions are recorded. It is also the case that practice attempts could artificially lower the failure to acquire rate. Additional attempts (i.e. after the required 3 attempts) may be made. It is important to ensure that no attempt is made against the identity of another participant. If a volunteer is keen to see a rejection, it is permitted that they may make an attempt against a non-participating identity. Again, such attempts should not take place immediately prior to their "genuine" attempts.

The order of using the devices will be random across users, and not correlated with the order of use on other occasions. Users will be asked to try to make these attempts successful, and to refrain from making bogus attempts (e.g. using the wrong finger on fingerprint devices, or pulling faces on face recognition devices). As an incentive to obey these instructions, payment for participation is linked to making the required number of good attempts.

Attempt images will be collected by the system, and user details, date and time logged. To avoid data entry errors, user identity will be entered using a swipe card or smart card if possible.

The supervisor will note any problems that arise during the test data collection, so that non-genuine attempts are not included in the analyses. Details of such attempts should be reported.

A.6 Analysis & Reporting

A.6.1 Data collected

Collected by system

- event logs as collected automatically by each system
- images of all test attempts
- enrolment database
- enrolment images

Collected by supervisor:

- log of failed enrolments
- log of (non-genuine) attempts to be excluded
- user details, e.g. age, sex *(The relevant user information to collect will depend on the sensitivities identified in preliminary tests.)*

A.6.2 Failure to enrol rate

The proportion of volunteers failing to obtain an enrolment (of sufficient quality) will be reported along with the enrolment policy and any quality threshold settings.

A.6.3 Failure to acquire rate

The proportion of attempts resulting in a failure to acquire error, averaged across all enrolees, will be reported together with any quality settings.

A.6.4 Detection Error Trade-off plot

The following enrolments and attempts will be excluded when deriving false match and false non-match rates:

- enrolment templates associated with any failed enrolment,
- attempts made on the day of enrolment,
- attempts made by non-enrolees, non participants in the trials, or by participants not completing the trials,
- attempts noted as a non-genuine in the supervisor log book,
- attempts resulting in failure to acquire errors
- extra attempts (4th or later attempt) made by any user on any day. (This is to ensure there is no imbalance due to some users making many more attempts than others).

Distance scores for genuine transactions may have been generated "live" during data collection. Otherwise we use vendor provided software for generating these distance scores off-line from the collected images.

Some systems do not generate distance scores, but can operate at various security settings. In such cases the attempts will be analysed using off-line software at different security settings. In such cases we consider the distance measure to be the strictest security setting at which the attempt results in a match.

We use the supplied software to generate impostor attempt distance scores, by comparing each attempt against the templates for all other enrolees. In the case of non-independent templates it will be necessary to re-enrol all enrolees apart from the one who made the attempt.

The Detection Error Trade-off curve plots the proportion of genuine transaction scores exceeding the matching threshold *(we assume that low scores imply a good match and high scores a poor match)* against the proportion of impostor transaction scores below that threshold, as the threshold varies.

A.6.5 System false accept & false reject rates

In cases where the usual decision policy of the system is not based on a single attempt-template comparison, we give the false accept rate and false reject rate using the actual decision policy, at the system settings used.

A.6.6 Penetration rate & binning error rate.

If a binning algorithm is used, we need to know the "bin" for each template and each genuine attempt.

The penetration rate is the average proportion of the database that would need to be searched if the system were operating in identification mode, where the average is taken over all genuine attempts. This can be estimated if we know the number of attempts in each bin, and which bins are compared against each other. A bin error occurs when an attempt is placed in a bin which is not compared with the correct bin for the biometric entity used, and hence will fail to match.

A.6.7 User throughput & matching algorithm throughput.

User throughput measures the elapsed time of a single transaction. All attempts are to be timed at a consistent point during the transaction (e.g. the start time). The difference in times between the first and second, or second and third attempts, by an individual on one day approximates the total transaction time. This assumes that the 2nd and 3rd attempts immediately follow the first attempt.

We can time the off-line calculation of impostor distance scores and compute the number of template-attempt matches performed to obtain the matching algorithm throughput. As the time is hardware dependent, the system used should be specified with the resulting throughput rate.

A.6.8 Sensitivity to population & environment

Where there appear to be differences in performance due to population, environment or usage changes (see section A.2.2), in some cases we will be able to assess the affects on performance by analysing subsets of the attempts. For example we can compare the error rates for different age categories, for people with glasses against those without glasses etc. We can also compare the error rates for attempts one month after enrolment with those two months after enrolment (and with error rates immediately after enrolment) to see the effects of template ageing. Comparing the error rates for the first attempt with those for the second and third attempt made on any occasion may show possible improvement in performance due to habituation.

APPENDIX B. CONSENT FORM & ENROLLMENT DATA SHEET

Name

Laboratory

Phone

Email

TRIAL ID

□ Male □ Female

Age:

□ 18-24 □ 25-34 □ 35-44

□ 45-54 □ 55-64 □ 65+

Other

□ Glasses

□ Contact Lenses

I am happy to participate in these trials. I consent to my biometric data being collected during the trial and stored electronically.

I permit use of this data for the purposes of evaluating performance of biometric devices, by the National Physical Laboratory, the Government Biometrics Working Group, and by the manufacturers of the devices under test. *[Data made available outside NPL will consist of only the collected biometric data, and the personal details in the box above.]*

Signed:

System	Enrolled OK	Problems / Notes
Face		
Iris		
Vein		
Hand Geometry		
Voice		
Fingerprint Optical Reader		
Fingerprint Chip Reader		

Return for recognition attempts on:

APPENDIX C. VERIFICATION DATA SHEET

«FirstName» «LastName»

TRIAL ID **«PIN»**

Please make **3** attempts on each system

Try your best to be correctly recognised - Do **NOT** try and trick the systems

System & Brief Instructions		Comments
VEIN		
1. Place **RIGHT** hand on pad	☐	
2. Click button under your fingers to take image	☐	
3. Enter **«PIN»** on keypad, check on screen, then press *	☐	
FINGERPRINT – OPTICAL SENSOR		
Enter **«PIN»** in ID box – Check this before proceeding	☐	
1. Press VERIFY to make a verification	☐	
2. Use **RIGHT INDEX** finger	☐	
FACE		
Enter **«PIN»** and check your image displayed	☐	
1. Press START VERIFICATION	☐	
2. Stand on marked spot and face camera	☐	
IRIS		
1. If needed click START or 🔭 *to show ID entry box*	☐	
2. Enter **«PIN»** and click OK	☐	
3. Use **RIGHT** eye	☐	
FINGERPRINT – CHIP SENSOR		
Enter **«PIN»** in ID box – Check this before proceeding	☐	
1. Press START to commence verification	☐	
2. Use **RIGHT INDEX** finger	☐	
HAND GEOMETRY		
1. Enter **«PIN»** and press "#YES" key	☐	
2. Use **RIGHT** hand	☐	
	☐	
VOICE		
Dial 6901 and follow instructions	☐	
	☐	
	☐	
For impersonation attempts use ID **«PIN-impostor»**	☐	
	☐	
	☐	

Options for payment

☐ (NPLML Staff) Please make payment with my November salary
My staff number is:

☐ (non NPLML staff) Please send a cheque to:

☐ Please donate my payment to the NPL Sports Club Pavilion Rebuild Fund

☐ Please donate my payment to Save the Children

☐ I wish to waive payment

Signed:

APPENDIX D. SIGNIFICANCE OF USER & ATTEMPT VARIATIONS

55. Attempts can be categorised by:

a. Whether made at the enrolment visit or at the second or third visit by a volunteer;

b. The gender of the volunteer;

c. The age of the volunteer;

d. Whether the volunteer was wearing spectacles in the case of Face and Iris systems;

e. The length of the user's pass-phrase in the case of the Voice system.

Performance differences between these subsets have been analysed, and are reported for each system in Part II.

56. To determine the statistical significance of any observed differences (i.e. the probability of the difference being attributable to sampling error) a simple χ^2 test was used.

a. The number of correct and failed verifications at the default threshold were counted for each class. E.g.

Observed	Under 35	Over 34	Combined
FRR	3.9%	11.5%	8.3%
Rejected	29	116	145
Verified	710	893	1603
Total	739	1009	1748

b. If there were no difference between classes the combined error rate would apply to both classes.

Expected	Under 35	Over 34	Combined
FRR	8.3%	8.3%	8.3%
Rejected	61.3	83.7	145
Verified	677.7	925.3	1603
Total	739	1009	1748

Observed-Expected		
	-32.3	32.3
	32.3	-32.3

c. The test statistic used is

$$\sum \frac{(Obs.\ -\ Exp.)^2}{Exp.} = (32.3 - ½)^2 \left(\frac{1}{61.3} + \frac{1}{83.7} + \frac{1}{677.7} + \frac{1}{925.3}\right) = 31.17$$

(The subtraction of ½ represents the correction for continuity; and is used because the observed values can only take integer values.)

d. If all attempt results are statistically independent, the test statistic would follow a χ^2 distribution (with 1 degree of freedom). In the example case χ^2 exceeds 31.17 with probability less than 0.01%. However, this overstates the significance since there are dependencies between each attempt made by the same user.

e. If all N attempts by any user had the same result (the maximum correlation possible), while attempts by different users are independent, then the test statistic divided by N follows a χ^2 distribution (with 1 degree of freedom). In the example case, if there are 9 attempts per user, the probability of χ^2 exceeding $\frac{31.17}{9} = 3.46$ is 6.28%. This understates the significance, since user attempts are not correlated to such an extent.

f. Both results are shown, the true significance lies between these values.

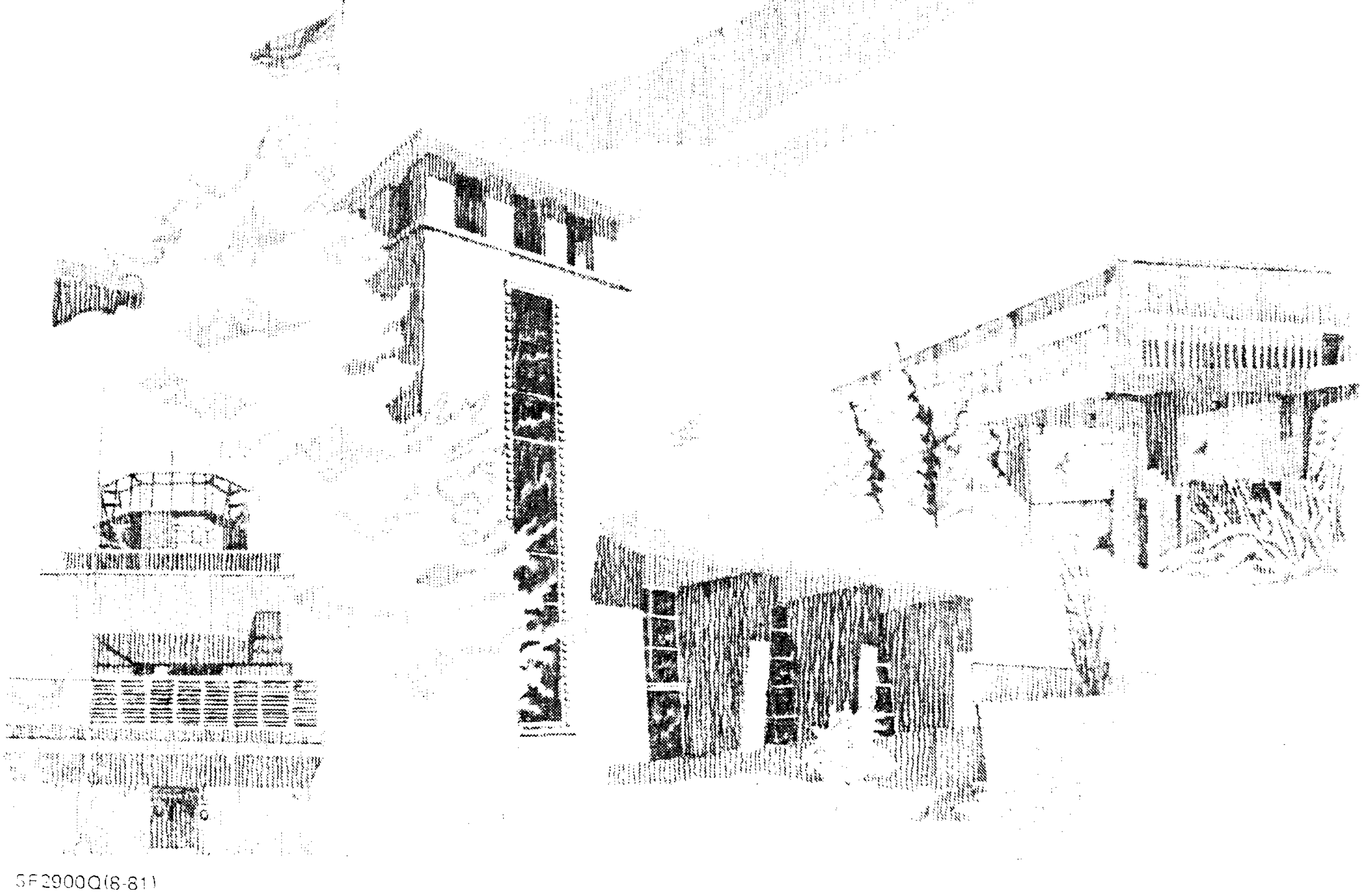
SANDIA REPORT

SAND91–0276 • UC–906
Unlimited Release
Printed June 1991

A Performance Evaluation of Biometric Identification Devices

James P. Holmes, Larry J. Wright, Russell L. Maxwell

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550
for the United States Department of Energy
under Contract DE-AC04-76DP00789



Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

Printed in the United States of America. This report has been reproduced directly from the best available copy.

Available to DOE and DOE contractors from
Office of Scientific and Technical Information
PO Box 62
Oak Ridge, TN 37831

Prices available from (615) 576-8401, FTS 626-8401

Available to the public from
National Technical Information Service
US Department of Commerce
5285 Port Royal Rd
Springfield, VA 22161

NTIS price codes
Printed copy: A03
Microfiche copy: A01

SAND91–0276
Unlimited Release
Printed June 1991

Distribution
Category UC–906

A Performance Evaluation of Biometric Identification Devices

James P. Holmes and Larry J. Wright
Facility Systems Engineering Division

Russell L. Maxwell
Systems Engineering Division
Sandia National Laboratories
Albuquerque, NM 87185

Abstract

When an individual requests access to a restricted area, his identity must be verified. This identity verification process has traditionally been performed manually by a person responsible for maintaining the security of the restricted area. In the last few years, biometric identification devices have been built that automatically perform this identity verification. A biometric identification device automatically verifies a person's identity from measuring a physical feature or repeatable action of the individual. A reference measurement of the biometric is obtained when the individual is enrolled on the device. Subsequent verifications are made by comparing the submitted biometric feature against the reference sample. Sandia National Laboratories has been evaluating the relative performance of several biometric identification devices by using volunteer test subjects. Sandia testing methods and results are discussed.

Contents

Figures

A Performance Evaluation of Biometric Identification Devices

Introduction

In many applications, the current generation of biometric identification devices offers cost and performance advantages over manual security procedures. Some of these applications are: physical access control at portals, computer access control at terminals, and telephone access control at central switching locations. An installation may have a single, standalone verifier which controls a single access point, or it may have a large networked system which consists of many verifiers, monitored and controlled by one or more central security sites.

Establishing how well a biometric identification device operates should be an important consideration in any security application. Performance data, however, is neither easy to obtain nor to interpret. Because there are no test standards yet to test against, test methods must be well documented. To measure its theoretical performance limit, a verifier could be tested in an ideal environment with robotic simulation of biometric data. The results of such a test would probably differ greatly from its real-world performance. The human element greatly affects the performance of any identity verifier. Environmental factors such as noise, light, electromagnetic radiation, moisture, dust, and temperature could also affect the verifier's performance.

Sandia began its latest verifier test series in November, 1989. Nearly 100 volunteers attempted many verifications on each machine. Environmental conditions were nominal, as the tests were all performed in a laboratory room for the convenience of the test volunteers. The biometric features used by the suppliers of the latest generation of verifiers in the Sandia tests include:

1. Fingerprint by Identix, Inc.[1]
2. Hand geometry by Recognition Systems, Inc.[2]
3. Signature dynamics by Capital Security Systems, Inc. Sign/On Operations.[3] (Formerly Autosig Systems, Inc.)
4. Retinal vascular pattern by EyeDentify, Inc.[4]
5. Voice by Alpha Microsystems, Inc.[5]
6. Voice by International Electronics, Inc.[6] (Formerly ECCO, Inc.)

General Test Description

Statistics have been compiled on false-rejection error rates and false-acceptance error rates for each verifier. The error rates are described as a percentage of occurrence per verification attempt. "Attempt" is used in this report to describe one cycle of an individual using a verifier as proof of being a validly enrolled user (enrollee). Most verifiers allow more than one try per attempt. "Try" describes a single presentation of an individual's biometric sample to the verifier for measurement. "False-rejection" is the rejection of an enrollee who makes an honest attempt to be verified. A false-rejection error is also called a Type I error. "False-acceptance" is the acceptance of an imposter as an enrollee. A false-acceptance error is also called a Type II error. False-acceptance attempts are passive; these are cases where the imposter submits his own natural biometric, rather than a simulated or reproduced biometric of the enrollee whose identity is claimed. To sum up:

false-rejection error = Type I error = rejection of an enrollee
false-acceptance error = Type II error = acceptance of an imposter.

Each verifier in the test is a commercially available unit. Because of the differences in these units and because we needed an equitable basis of comparison, we attempted to modify some of the units. One goal was to have each verifier report a final decision score for every verification try. Although the manufacturers were generally cooperative, it was not possible to achieve all our goals within the time and budget constraints of the testing. The Identix fingerprint verifier did not generate score data at all. The Capital Security signature verifier scores were not directly related to the accept or reject decision because of some additional decision making after the scores were generated. If a biometric testing standard ever becomes a reality, it should include a section on score data generation and reporting.

Software and/or firmware modifications were made by the manufacturer on some units to allow Sandia to collect the desired test data. All verifiers and specified modifications were purchased by Sandia. Where possible, each verifier was set up in accordance with the manufacturer's recommendations. In most cases, a representative from each manufacturer visited the testing laboratory to verify that his device was properly set up. Where problems were pointed out, attempts were made to rectify them. Some attempts were more successful than others within the limits of our test facility resources.

Testing and Training

The verifier tests at Sandia were conducted in an office-like environment; volunteers were Sandia employees and contractors. A single laboratory room contained all of the verifiers. Each volunteer user was enrolled and trained on all verifiers. There were both male and female volunteers and the efforts of both were valuable to this study. However, for the purpose of simplifying the text, we will use the term "his" rather than "his/her."

There is a learning curve for the proper use of a biometric identification device. As a user becomes more familiar with a verifier, his false-rejection rate decreases. This curve differs for individual users and verifiers. This learning effect was minimized for the Sandia testing by training the individuals before the test, by monitoring their performance, and by eliminating the first few weeks of test data in the results. A number of users were reenrolled on verifiers where there was indication of below-average performance. The transactions prior to the reenrollment were not included in the test results. Some manufacturers recommend that the users be reenrolled as many times as necessary to produce the best enrollment scores. We tended to limit reenrollments to known problem cases due to the relatively short duration of our test, and also to give the verifiers more nearly equal treatment. Verifiers on which it is more difficult to enroll would therefore tend to give somewhat less than optimum performance in our test. This effect is less significant for verifiers which modify the stored reference template by averaging in the biometric samples from successful verification attempts. The EyeDentify and the Identix units are the two tested verifiers that do not modify the reference template.

Other known errors were identified for removal by instructing the users to note on a real-time hardcopy printout any transaction where he made a mistake, or was "experimenting" and did not feel that the verification attempt was valid. A similar method was used to identify invalid transactions on the false-acceptance test. Many hours were devoted to identifying and removing invalid transactions from the data files. There is no doubt, however, that a small number of unrecognized errors remain in the data.

The problem of selecting a representative test user group is most vexing when testing biometric identification devices. While the differences in physiological and behavioral properties of humans are the bases for the devices, these same differences can bias test results between test user groups. The best solution to this problem seems to be to use many users and to make numerous attempts. The larger the numbers, the more likely the results will represent true performance values. Relative performance must be measured against absolute performance. A verifier's relative performance within a user group is generally easier to defend than is the absolute performance.

No extraordinary incentives were offered the volunteer users who performed the tests. Treats in the test room were used to tempt users to remain active. A drawing for a free lunch was offered to the regular users. About 80 of the 100 enrolled users remained fairly active in the tests. Work and travel schedules accounted for the loss of some users. Others simply became disinterested.

First Test Series: False-Rejection Testing

- users attempted verification on each machine many times
- test period was three months long
- users were allowed up to three tries per verification attempt.

Second Test Series:
Passive False-Acceptance Testing

- user submitted the personal identification number (PIN) of other users
- user then submitted his own natural biometric
- users were allowed up to three tries per verification attempt.

Data Processing

The first step in the data processing was to remove the invalid transactions that were noted on the printed data logs generated at each verifier. The data files were then processed to remove incomplete records and to convert the data to a common format. The data was sorted into individual user groups. Records from users making less than six transactions were deleted. User data obtained prior to user group reenrollment on a verifier was also deleted.

A verifier can usually be configured to accept up to three "tries" on a verification attempt. A "try" is one cycle of the user presenting his biometric to the verifier for measurement. To simulate verifier performance on one-, two-, and three-try attempt configurations, our users were instructed to try a third time if verification was not successful on the first or second try. Recorded time- of-day information allowed each score to be identified as either a first, second, or third try.

Up to three tries in a five-minute time interval were considered one verification attempt. Additional tries within this interval were ignored. Tries beyond the five-minute interval were considered another verification attempt. At any given threshold value, a score will produce either an accept or a reject. An accept on the first try is counted as an accept for one-, two-, and three-try configurations. An accept on the second try is counted as a reject on a one-try configuration and an accept on a two and three-try configuration. An accept on the third try is counted as a reject on a one and two-try configuration and an accept on a three-try configuration. Three rejects are counted as a reject on all three configurations. To sum up:

	Configuration Test Result		
Verification Action	one-try	two-try	three-try
Accept on first try	accept	accept	accept
Accept on second try	reject	accept	accept
Accept on third try	reject	reject	accept
No accepts with three tries	reject	reject	reject
No accepts with less than three tries	only actual rejects counted		

The false-reject error rate is the ratio of false-rejects to total attempts at verification. A false reject will be represented as "FR" and is reported in this document as a percentage value. Where transaction score data was available, the FR was calculated for each user for one-try, two-try, and three-try verifier configurations over a range of possible thresholds. The scores were used to find the number of errors that would have occurred had the verifier test threshold been set at each of the possible thresholds.

The false-accept error-rate is the ratio of false-acceptances to total imposter attempts. It will be represented as "FA" and was calculated for each user over the range of possible thresholds and presented as a percentage value.

The FR and FA for each verifier was calculated by averaging the user-percent error rates at each threshold value selected. The FA and FR error-rate curves are shown in the next section, entitled "Results of the Testing." Where possible, error-rate curves are shown for one-try, two-try, and three-try verification attempts. These curves exhibit two general characteristics. One characteristic is the non-zero value of the crossover point of the FA and FR curves. A second characteristic is the trend toward a lower rejection rate as the number of tries at verification increases. Both these characteristics force some tradeoffs in using these verifiers.

The non-zero error value at the crossover point means that there is no threshold setting where both the FA and FR error-rates are zero. The user must choose a threshold setting to fit the application. As the threshold is moved toward tighter security (higher rejection error rates), both imposters and valid users face higher rejection rates. Both are rejected less often when the threshold is moved toward lower security. The point at which the FA and FR curves cross over is referred to as the equal-error setting. This single-value error rate has been accepted as a convenient value to describe the performance of a verifier in the Federal Information Processing Standards Publication (FIPS PUB) 83. This and other single-value criteria have been used to characterize verifier performance, but no single value can provide much insight into the true performance capability of any verifier. The FA and FR error-rate curves provide much more insight into performance and should be examined for suitability in any security application.

Multiple-try attempts at verification can improve the performance of some biometric verifiers. The rejection rate for valid users generally decreases faster than the rejection rate for imposters, as more verification tries are allowed. Valid users are generally rejected because of inconsistent presentations of their biometric input. Additional tries allow the valid user to correct the inconsistencies and to generate an acceptable input that matches the reference template. Imposters are generally rejected because their biometric is not close enough to the reference to be accepted. Additional tries increase the chances of imposter acceptance if the biometric differences are small enough to be masked by the inconsistent user inputs and by tolerant threshold settings.

The Identix fingerprint verifier we tested did not have a customer adjustable system threshold. While individual thresholds could be adjusted, we did not get any test data at other than the factory-set threshold. The other verifiers tested did provide test score data, but the Capital Security signature verifier scores could not be used to generate error-rate curves because of a second calculation that it uses to make the accept or reject decision.

Our transaction time results were obtained by timing the users from when they touched the verifier until the verification attempt verdict was given. The users were not told that they were being timed. We feel that the results reflect verification times that would be typical in an actual installation. These times are substantially longer than the minimum times of a skilled user in a hurry.

Results of the Testing

Alpha Microsystems Results

Alpha Microsystems of Santa Ana, California bought out Voxtron and is now selling an updated system called Ver-A-Tel. This voice verification system makes use of a personal computer (PC), which contains the speech board hardware and the software programs. User terminals are touch-tone telephones. The Ver-A-Tel system is offered in two similar versions: the telephone intercept system (TIS) and the remote-access system (RACS). We tested the public TIS version, but not the direct-line RACS version.

The software supplied with the system provides the necessary management functions to enroll and delete users, to configure the system parameters, to display activities and alarms and to generate reports. Because this password-protected software is menu driven, it allows the security manager to select options from the screen and to fill in the blanks to configure the system. A supplied user's guide provides any additional information that might be needed.

Users were enrolled on the same touch-tone telephone that was later used to access the system. Prior

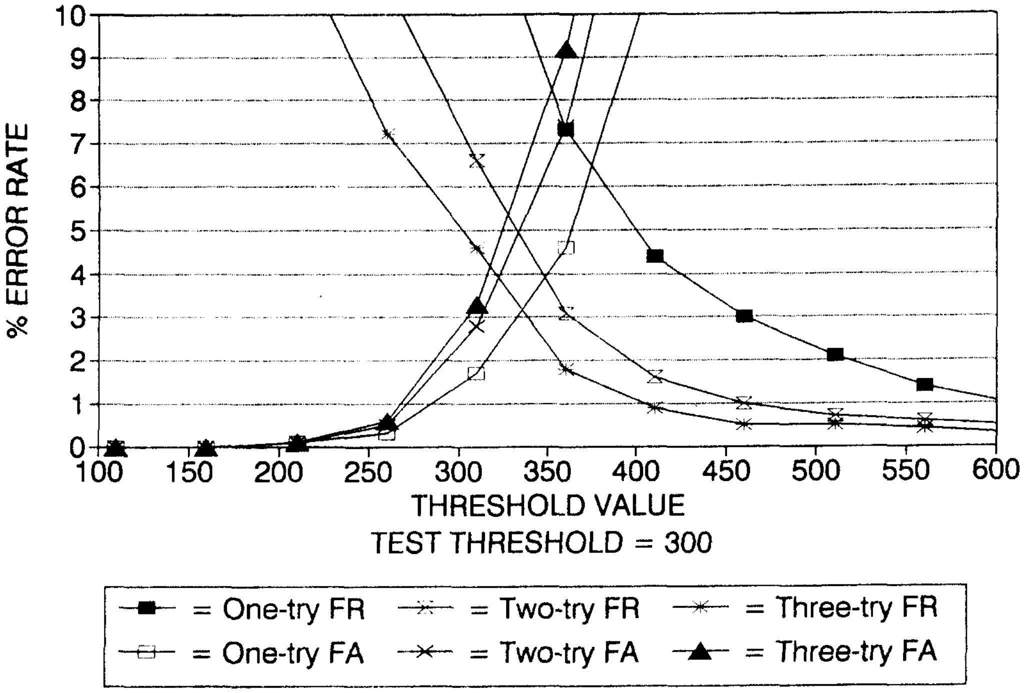


Figure 1. Alpha Microsystems Voice Verifer

Capital Security Systems, Inc. Results

Capital Security Systems, Inc. of Columbia, MD purchased the signature dynamics verifier line from Autosig Systems, Inc. This verifier consists of a user interface tablet and a controller which is designed to integrate into a host-computer access control system. The Capital security system offers products for both physical entry control and data access control. The user interface is similar for both applications. A variety of hardware and software options allow the system to function in applications from stand-alone protection of a single entrance to networked, host-based systems.

The user interface is a desk top tablet (~9 3/8 by 11 inches) that incorporates a digitizer tablet, a magnetic stripe card reader, and a tethered pen. The digitizer tablet (~2 1/2 by 5 inches) is the area where the user actually signs his name with the tethered pen. The system measures the dynamics of the user's signature to form the biometric template for enrollment and verification.

The controller can function as a stand-alone device with the user interface and door interface hardware, but must be connected to a computer for programming and user enrollment. An IBM PC or a higher class, compatible computer with a serial port and a floppy disk drive can be used. The computer class must match the controller interface requirement.

Software is provided to allow the security manager to configure the system and to enroll users. A menu-driven program provides the manager with the necessary options. Before a user can be enrolled, a user data record must be generated in the user data file. The manager selects the options and fills in the blanks to generate the record. For the model tested, a magnetic stripe card was required for ID entry. It was coded with the user's PIN and provided to the user for verifiers in this test series.

To enroll, the user must follow the illuminated prompts on the interface tablet. First the user PIN is entered with a swipe of his magnetic stripe card through the card reader. Next, the user is prompted to alternately sign on and wait while the system generates a template. Finally, the user is prompted when the sequence is complete. It normally takes two signatures and one verification signature to enroll. The signature must be within the marked digitizer pad area, using the tethered pen. The system can be used with a regular ball-point pen tip and a stick-on paper sheet over the pad, or with an inert, inkless pen tip system directly on the digitizer pad.

Verification is similar to enrollment. The user PIN is entered with the magnetic card and the user signs his name on the digitizer pad with the tethered

to enrollment, the security manager created a record for each user and each was assigned a unique PIN. An optional secret enrollment passcode, to prevent an imposter from enrolling in place of the authorized user, was not tested.

A phrase is required for enrollment and subsequent verification. The security manager can select from a number of standard phrases on the menu display; from this selection, he can allow the user to make up his own phrase. There are some restrictions on user-selected phrases, such as the minimum and maximum length and the optimum number of syllables. These options are discusssed in the User's Guide which is supplied with the system.

Voice verifier manufacturers are quick to point out that security is enhanced if each user has a secret phrase. These manufacturers, however, do not address the problem of how to keep a phrase secret that must be uttered into a microphone. On the other hand, it is certainly less likely that an imposter would be accepted if he does not know the proper phrase. It is even plausible that a valid user could have a lower false-reject error rate with a chosen phrase that was more natural or familiar to him. The objective of our test was to measure the ability of the system to verify users based solely on their biometric properties. Thus, we assigned the same phrase to all users.

To enroll, a user calls the verifier telephone number. The system answers and instructs the user to enter his PIN on the touch-tone keypad. If the system finds that the PIN belongs to someone who is not yet enrolled, it tells the user what he must do to enroll. This may include an instruction to enter the proper enrollment passcode on the keypad. The user is instructed to say the verification phrase a number of times. The system performs checks on each response and may prompt the user to be more consistent and to repeat the phrase again. When the system parameters for a successful enrollment are met, the system so informs the user. A user template is generated from the enrollment data and is stored for future verification of the user's identity. The system may tell the user that the enrollment was better than most. This indicates that the enrollment phrases were very consistent. It is also possible for the user to fail. In this case, the user is told to practice and try again. The security manager can also check the enrollment scores to get a measure of the enrollment performance. Individual accept or reject thresholds can be set by the security manager to compensate for differences in user performance. This adjustment is made (plus or minus) to the system threshold setting.

On verification attempts, an enrolled user's PIN is recognized by the system and is used to retrieve the proper template from the enrollment database for verification. The user is then prompted to say the phrase for verification. Optionally, the new phrase data may be averaged into the stored template to update the template each time the verification is successful. In time, if the user becomes more consistent and the verification scores improve, the security manager may opt to adjust the user threshold value to a more secure value. Experienced users generally skip the voice prompts because a preceding tone signals the user that he can go ahead without further delay if he does not need the voice instruction.

The time information given for the Alpha Microsystems voice verifier is different from other verifiers because it includes dialing a 5-digit telephone number and waiting for the verifier to answer. We included this scenario because the telephone access method was also used in our test verifier. Other access methods may result in different transaction times. The minimum time of ~13 seconds was necessary to perform the following steps:

- lift the phone and dial a 5-digit extension
- wait for the voice system to answer and generate the tone prompts (without waiting for the subsequent voice prompts)
- enter a 4-digit PIN on the phone keypad
- say "yankee doodle dandy"
- be verified.

The average user in our test took ~19.5 seconds for a complete verification. This average includes multiple-try attempts when this was required by the system.

The crossover point where the one-try false-reject and the one-try false-accept curves are equal has an error rate of 6.5% at a threshold value of ~375. At the test threshold setting of 300, the three-try, false-reject error rate was 5.1% and the three-try, false-accept error rate was 2.8%.

There were 5434 transactions in the false-reject test and 2990 transactions in the false-accept test. The results of these tests are shown in Figure 1.

pen. A prompt then tells the user whether the verification was successful or if another signature try is necessary. Two tries are usually allowed. Each successful verification is averaged into the reference template to allow the system to accommodate long-term changes in the user signature. This averaging can be inhibited by the security manager.

Imposter testing consisted of each imposter entering PINs by using the magnetic stripe badges of all other users. The imposter knew the real user's name from the badge, but did not have a sample of the user's signature. The imposter was free to try to sign the actual user's name. As a matter of interest, we attempted some verifications by tracing over valid signatures. The scores were generally much worse than other imposter attempts because of the importance of the signature dynamics in verification. None of the tracing attempts were included in our test results.

The time to perform a verification depends in part on how long a user takes to sign his name. Our users averaged ~15 seconds to verify on the Capital Security system; this time includes PIN entry via a swipe card reader and some multiple-try attempts as required by the system. The minimum time observed was ~12 seconds.

Error-rate curves are not shown because the Capital Security accept or reject decision process is more than just a function of the transaction score. A second decision calculation is performed on all tries that produce a score between 16,000 and the verifier threshold setting. The threshold was set at 21,000 for our test.

All false-accept and false-reject error rates obtained were from a count of the errors at the operational threshold:

False-Reject Error Rate	Percentage
three-try	2.06%
two-try	2.10%
one-try	9.10%

False-Accept Error Rate	Percentage
three-try	0.70%
two-try	0.58%
one-try	0.43%

The Capital Security is usually set up for two tries.

There were 3106 transactions in the false-reject test and 6727 transactions in the false-accept test. The Capital Security system error-rates are shown in Figure 2.

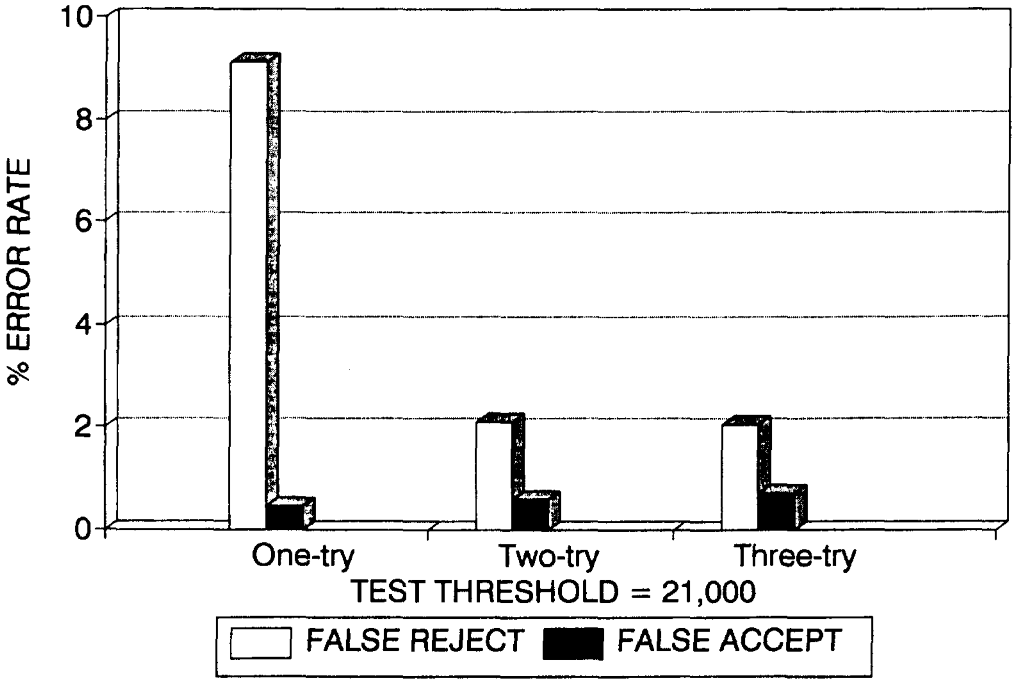


Figure 2. Capital Security Signature Dynamics

International Electronics (ECCO VoiceKey) Results

International Electronics, Inc. of Needham Heights, MA purchased ECCO Industries, Inc. of Danvers, MA and now markets the ECCO VoiceKey. The VoiceKey is a self-contained, wall-mounted user interface that communicates with a controller over a copper wire cable. The user interface contains an alphanumeric display, keypad, a microphone, an audible beeper, and indicator lights. Keys, displays, etc. allow all necessary functions to be performed at the user interface. Some of these functions are user enrollment and system management.

The user interface and controller can operate in a stand-alone mode to provide security at a single entry point, or can be networked through a network controller to other units in a security system. A VoiceKey network has a master voice reader and slave voice readers. The master voice reader is normally used for all enrollments and programming, which are then downloaded to the slave readers. Enrollment and programming can be performed at any slave, but it cannot be downloaded to any other reader. A printing capability allows audit information to be output to a printer connected to the controller of the master reader.

User enrollment is normally performed at the master voice reader by a security manager who is authorized to enter the programming mode. This authorization must be verified by voice before the programming mode can be entered. Programming is accomplished by keypad key inputs. Message displays and lights provide feedback to the programmer as the program steps are entered. A supplied programming manual provides complete information on the programming procedures. A user program allows new users to be added. This option requires the security manager to enter a unique PIN to access zone data and to enter the user authorization level for the new user. The reader then displays a series of message and colored-light prompts for the new user to initiate the sequence and to say his password several times. A red/green light display at the end of the enrollment sequence informs the new user of failure/success in enrolling. (This frustrates color-blind users who cannot distinguish between the red and green colors.) If successful, the new user can practice using his password as desired. Each successful verification causes the user's template to be modified by the new input.

Verification can be accomplished in ~5 seconds. Users averaged ~6.6 seconds per one-try attempt; in this time, they were able to enter a 4-digit PIN on the keypad and to utter the single password.

The crossover point where the one-try, false-reject curve and the one-try, false-accept curve are equal has an error-rate of 8.2% at a threshold value of 100. Only one-try, false-accept data was obtained for the VoiceKey verifier. There are three user thresholds available for the VoiceKey verifier. Security level 1 is a threshold of 75, level 2 is a threshold of 65 and level 3 is a threshold of 55. At the test threshold setting of 75, the three-try, false-reject error rate is ~4.3%, and the one-try false-accept error-rate is ~0.9%.

Voice verifier manufacturers are quick to point out that security is enhanced if each user has a secret phrase. These manufacturers, however, do not address the problem of how to keep a phrase secret that must be uttered into a microphone. On the other hand, it is certainly less likely that an imposter would be accepted if he does not know the proper phrase. It is even plausible that a valid user could have a lower false-reject error rate with a chosen phrase that was more natural or familiar to him. The objective of our test was to measure the ability of the system to verify users based solely on their biometric properties. Thus, we assigned the same phrase to all users.

We experienced high, false-rejection error rates with the assigned password. The manufacturer's representative suggested that each user be allowed to choose a password familiar or comfortable to him. We gave additional training and reenrolled ~15% of the users that were experiencing the most trouble with verification. On reenrollment, the users could choose from several suggested words. Some were allowed to select a word of their choice. This effort did produce better verification scores for many of the individuals after they were reenrolled. We were unable to correlate the effect of reenrollment on the long-term, false-rejection error rates. Several variables remain in the verification process. As the user becomes more familiar with a password, he would be expected to get more consistent in its use. The user's reference template is also modified for each successful verification, and thus should improve the verification scores of consistent users. An analysis of entire user group performance before and after reenrollment, however, did not show a significant improvement over time.

There were 4871 transactions in the false-reject test and 3270 transactions in the false-accept test. The graphical results of these tests are shown in Figure 3.

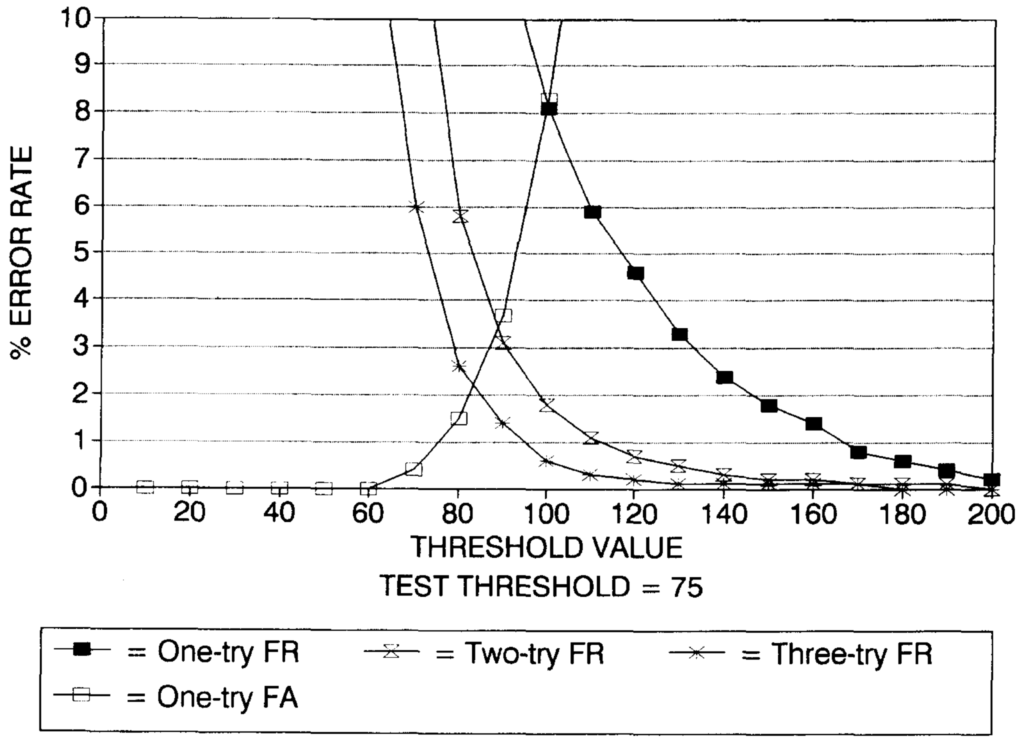


Figure 3. International Electronics Voice Verifier

EyeDentify Verify Mode Results

The retinal pattern verifier in this test series was Model 8.5, manufactured by EyeDentify, Inc. of Portland, Oregon. The verifier includes a reader and a controller. The reader contains an aperture where the user looks to align his eye with an optical target, which appears as a series of circles. As the user moves his eye around, the circles become more or less concentric. Proper alignment is achieved when the circles appear concentric and the user is looking at the center of the circles. The reader also contains a display, a keypad, and an insertion reader for magnetic stripe cards. A copper cable connects the reader to a controller box that contains processing and interface electronics.

The controller can function as a stand-alone device with the user interface and door interface hardware, but must be connected to a computer for programming and user enrollment.

Two readers were tested. Reader 1 was set up to operate in the verify mode using a PIN entered via an insertion card. Reader 2 was set up to operate in the "hands-free" recognize mode. The results for Reader 1 are discussed in this section, and the results for Reader 2 are discussed in the following section entitled: "EyeDentify Recognize Mode Results."

The software allows the security manager to configure the system and to enroll users. A menu-driven program provides the manager with necessary options. Before a user can be enrolled, a user data record must be generated in the user data file. The manager selects the options and fills in the blanks to generate the record. Once the record generation in the enrollment sequence is completed, a message instructs the user to enroll. The new user then aligns the optical target in the viewing aperture and presses the "ENTER" key on the keypad to initiate the eye-scan sequence. Each subsequent scan generates a score on the computer display and allows the security manager to accept or reject it. The user template is generated from an average of the accepted scans on enrollment. This template is not modified by subsequent verifications, so it is important to take some care during enrollment and not to accept scores below the mid 70s. It is not difficult for most properly instructed users to score above 80.

The user's PIN must be entered for verification. The EyeDentify 8.5 allows either manual entry on the keypad or automatic entry by using the card reader. Our tests used the card entry option. The average time for our users to perform the verification process was ∼7 seconds. This time included some multiple-try attempts and the removal of glasses by some users after inserting their card. The quickest times were around 4.5 seconds.

The false-reject error rates for EyeDentify Model 8.5 in this test are significantly less than for the Model 7.5 we tested in 1987. There are two differences between the models we tested that could account for the decrease in these errors:

1. Improved data acquisition software for Model 8.5 now tests for eye fixation before accepting a scan. This feature reduces the chance of a rejection due to eye movement.
2. The Model 7.5 we tested used only keypad PIN entry, while the Model 8.5 we tested used magnetic card PIN entry.

The verify mode crossover point, where the one-try, false-reject error rate and one-try, false-accept error rate are equal, was ∼1.5% at a threshold of ∼45 for Model 8.5. At the test threshold setting of 70, the three-try, false-reject error rate was 0.4%. No false-accepts were recorded at this threshold value. There were 5134 transactions in the false-reject test and 4196 transactions in the imposter test. The test results for Reader 1 are shown in Figure 4.

EyeDentify Recognize Mode Results

A unique option of the Model 8.5 verifier is the "hands-free" mode of operation. While the verifier is operating in this mode, the user merely peers into the viewing aperture and aligns an optical target by positioning his head. The verifier senses the user's presence, takes a scan, and decides whether or not the scan data is from an eye. If a digital pattern is generated from an eye, the verifier searches the template data base for a match. If a match is found, the verifier recognizes the user as valid. Otherwise, the user is requested to "REPEAT" up to two more tries until a valid match is found. The user is rejected if a match is not found in three tries.

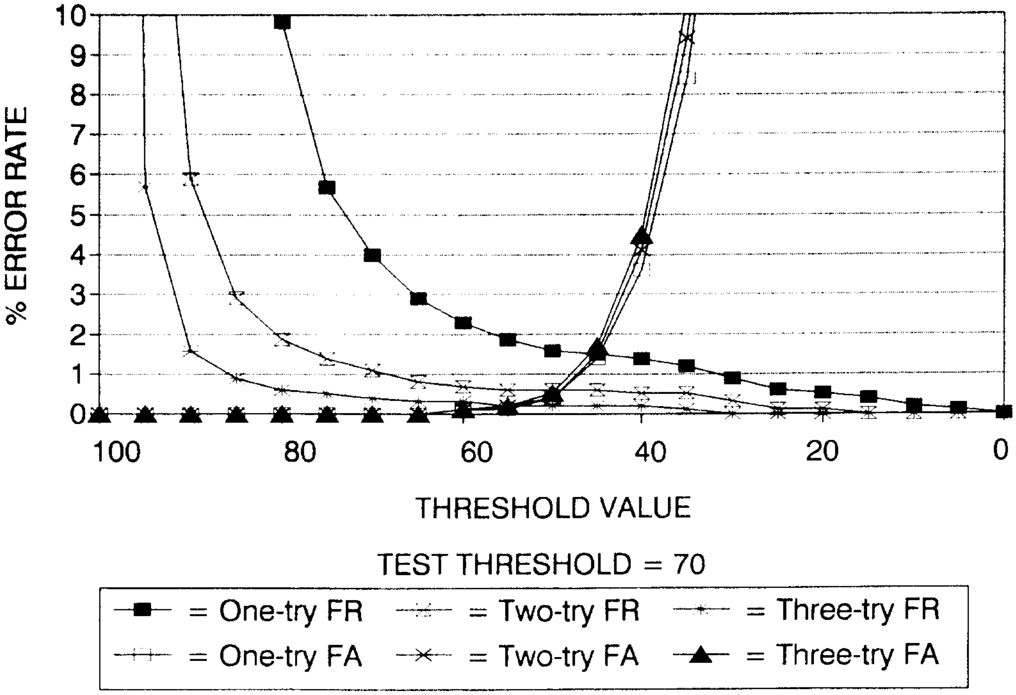


Figure 4. EyeDentify Eye Retinal Pattern

No timing information was taken for the recognize-mode operation because there is no precise point that can be observed when the user initiates the sequence. The user peers into the aperture, aligns the target, and waits for the target to turn off at the end of the scan. The auto-scan feature eliminates the need to insert the magnetic card and press the START button, cutting ~2 to 3 seconds from the verify-mode transaction time. We had a user database of ~100 users that had to be searched to find a matching template for each transaction. This searching did not add a noticeable time delay to the transaction. Larger databases will add more search time to each transaction.

The threshold was set to 75 for the recognize mode of operation. This means that any scan that produces a score of 75 or less is rejected as not being a member of the enrolled user base. A score of greater than 75 causes an accept, and the name of the identified user is displayed on the reader.

There were 5072 transactions recorded on the recognize-mode reader. A transaction is defined as any scan the machine decides meets the minimum criteria to be an eye. None of these scans resulted in a false accept. This result is especially significant because the 100 user database multiplies the possible matches to over half a million!

False-reject information cannot be reported on the "hands-free" recognize reader because there is no PIN associated with a reject that can tie it to a user. No doubt the false-reject rate is significantly higher in the recognize mode because the user does not control the start of the scan. In many attempts, the scan started before the user had the target properly aligned. With practice, most users learned to use the recognize mode to their satisfaction. EyeDentify has now modified their acquisition software to allow users more time to align the target. This change should lower the false-reject error rate.

Identix Results

The fingerprint verifier evaluated in this test was the TouchLock, manufactured by Identix, Inc. in Sunnyvale, California.

The user interface to the Identix system is a sensor module that contains the finger platen/scanner hardware, a display, a keypad and communications electronics. This module is ~8.2 inches wide, 4.4 inches tall, and 3.9 inches deep. The sensor module communicates with a remote processor module over a copper wire cable. The remote module contains the processor, memory, input/output hardware, and communications hardware to support stand-alone operation at a single entry point or in a network environment. Our test verifier was connected to a host computer with the Identix TouchNet software support system. It also was connected to a magnetic-stripe, swipe-card reader via its built-in card reader interface. The card reader was used to enter user PIN information for verification attempts.

The Identix supplied software is a password-protected, menu-driven program for IBM PC and compatibles. It provides the capability to configure the system, to set up user records, and to generate reports.

User enrollment is performed at the sensor module. A security manager must first be verified by a fingerprint scan before the enrollment mode can be entered. Messages on the sensor module display provide user prompts and status information. A unique PIN must be entered for the new user, followed by a number of finger scans that allow the system to generate a template. If the enrollment is successful, a quality rating is displayed. The manager can accept or reject the enrollment at this point. The manufacturer recommends that only "A" or "B" quality ratings be accepted. A "C" rating is the least desirable. If the enrollment is unsuccessful, the system informs the user, who is invited to try again. The templates are not modified by subsequent verifications, so if problems appear, the user should be enrolled again.

We accepted some "C" enrollments for our test. We retrained and reenrolled users that experienced the most problems with verification. The reenrollment did not always result in a higher quality rating. A number of our users appear to have poor quality fingerprints that would not produce good results, even when other fingers were tried. Another problem was caused by low humidity during our test period. User's skin would dry out to the point where the system could not verify the user. Lotion or skin moisturizer often solved the dryness problem.

Our users all had the factory-default verification threshold of 125. The host system software allows the security manager to change individual threshold values, but we did not exercise this option. Our test results do not include the error-rate curves because this verifier did not generate verification score information. Only the percentages of false-reject errors and the false-accept errors at the factory-default threshold can be reported.

The lack of score data hampered our attempts to quantify the Identix verifier. Enrollment quality ratings were generated from groups of finger scans. Individual scan quality was not available. Some clues were available from prompts to position the finger further up or down on the platen, but we could not correlate the finger positioning to scan quality. Our

false-rejection error rates were significantly worse than the estimated error rates published in the Identix TouchNet User's Guide, supplied by Identix with the TouchNet system. Identix indicates an estimated single-try, false-rejection error rate of ~3% for an enrollment threshold setting of 125. We experienced over 9% false-rejections for three-try attempts with the 125 threshold setting. The cold, dry weather effect on skin conditions in Albuquerque could account for some of this difference. Individual score data might have given us more insight into the problem.

Our users averaged ~6.6 seconds for a card PIN entry verification, including multiple-try attempts. The fastest users verified in under 5 seconds.

Two identical readers were used in this test. The two readers tested were set up for a maximum three-try attempt and only reported a single accept or reject transaction result for each attempt. If a user was accepted on either the first, second, or third verification try, the attempt was recorded as an accept. If a user was rejected on all three tries, the attempt was recorded as a reject. Individual-try data was not available from the monitoring program.

Reader 1 logged 2248 verification attempts with a false-reject error rate of 9.4% and no false accepts. Reader 2 logged 2316 attempts with a false-reject error rate of 9.5% and no false accepts. The number of false-accept attempts was 3424. The false-reject error rate equals the percentage of the three-try false-rejects that occurred in the verification attempts.

Recognition Systems, Inc. Results

The Model ID3D-U hand-profile verifier manufactured by Recognition Systems, Inc. (RSI) of San Jose, California was evaluated in this test. The verifier houses the hand geometry reader and all the electronics in one enclosure. Both the wall mount or the desk top models are available. The reader has a platen with guide pins to aid in proper hand placement; an optical imaging system acquires the hand geometry data. Displayed messages prompt the user and provide status information. A keypad and an insertion magnetic-stripe card reader record user data input. This verifier can be configured for stand-alone operation or for use with a host processor. Our test verifiers were configured for use with a host processor. The host management software we used included some custom features not required for normal system operation.

User enrollment takes place at the verifier reader. In actual security system applications, each user is assigned an authority level and, if required, a password for entering the security management command mode. A new user can only be enrolled by a security manager with the proper authority level and password to enter the enrollment sequence. The manager must first be verified on the hand geometry reader, and then he must enter the proper password within a time limit to initiate the enrollment sequence. Our test software did not require a password or manager verification for user enrollment. It provided the necessary functions with a menu-driven program that allowed the test conductors to fill in the blanks and to initiate the enrollment sequence.

User Enrollment Sequence

1. A valid PIN is entered by the new user.
2. A ** PLACE HAND ** message then appears on the reader display.
3. The user must then place his hand on the platen and against the guide pins.
4. When the imaging system determines that the hand is properly positioned within the time limit, the hand geometry data is acquired and a ** REMOVE HAND ** message is displayed.
5. The message display prompts are repeated at least two more times, and the user reference template is then generated from an average of the three inputs.

User Verification Sequence

1. Enter the user PIN by keypad or card reader.
2. Follow the ** PLACE HAND ** and ** REMOVE HAND ** instructions on the display.

The average verification time for our users was ~5 seconds, with card PIN entry. (Times as low as ~2.9 seconds were observed.)

The false-reject error rates for Model ID3D-U in this test were less than the rates were in 1987 when we tested the Model ID3D-ST. PIN entry by magnetic card rather than by keypad is the most likely reason for the lower error rates.

The crossover point, where the one-try, false-reject error rate and the one-try, false-accept error rate are equal, was ~0.2% at a threshold of ~100 for Model ID3D-U. At the test threshold value of 75, the three-try, false-reject error rate was less than 0.1% and the one-try, false-accept error rate was ~0.1%. Three-try, false-accept error rate data was not obtained in this test. The test results were very similar on both readers; thus, only Reader 0 results are plotted.

Reader 0 logged 5303 transactions in the false-reject test and 5248 transactions in the imposter test. Reader 1 logged 5285 transactions in the false-reject test and 3839 transactions in the imposter test. The results of this test are shown in Figure 5.

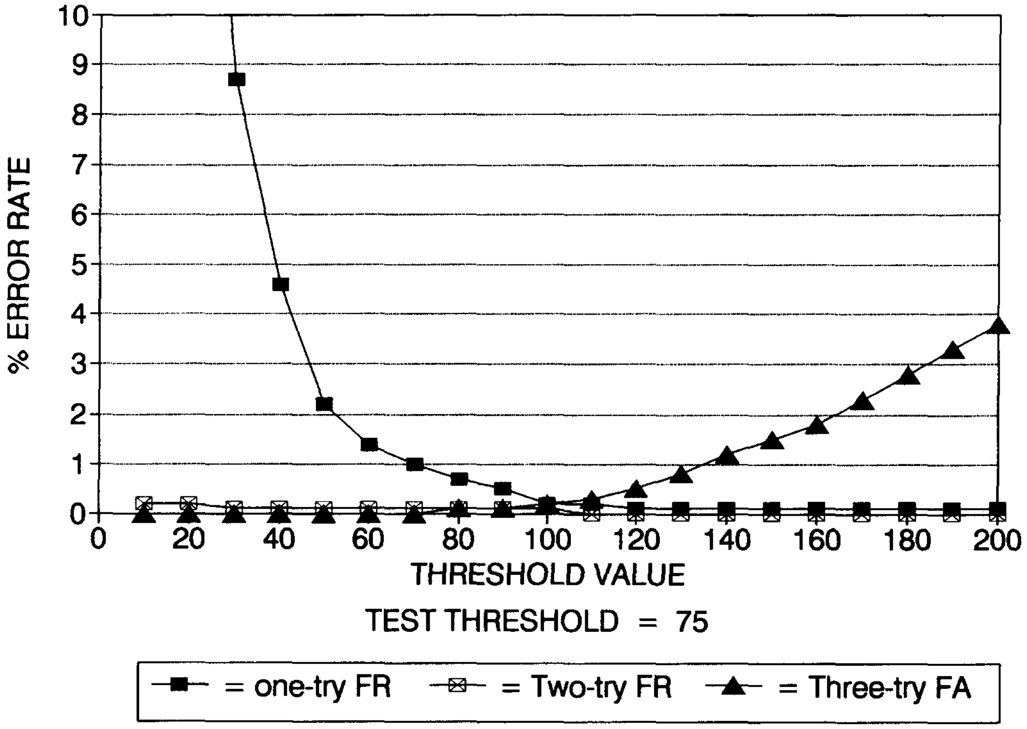


Figure 5. Recognition Systems Hand Geometry

Summary

The relative performance of the tested verifiers can be deduced from the test results. These results include the user variables in the operation of the machines and are therefore representative of the performance that can be expected with average users; at the same time, they are not a true measure of the machines absolute performance limits. The degree to which our results differ from the performance limits is an indication of the complexity of the user interface. As an interface becomes more complex, more user variables are introduced that could shift the test results away from the performance limit.

From a test viewpoint, it is desirable to have a final score value reported for each verification try. This report is not possible, however, because some verifiers do not provide the score data necessary for us to calculate error-rate curves. Verifier results in this case are given only for the one threshold value tested. It would have been possible to repeat the performance tests at a number of different threshold values to obtain points on the error-rate curves, but we did not have the resources for such an extensive test. This is only one of several roadblocks for developing biometric verifier testing standards.

A user survey was taken late in the test. The summary results are given in the appendix. Users generally preferred the verifiers that produced the fewest false-rejects and which took the least time to use. User frustration grew rapidly with high, false-rejection rates; these rates proved to be a bigger problem for them than did the slow transaction times. The RSI hand geometry was overall the user favorite.

The verification timegraph (see Figure 6) shows the average transaction times for:

- entering the PIN
- presenting the biometric feature
- verification or rejection.

The Alpha Microsystems time also includes the time necessary:

- to dial a five-digit number on a touch-tone telephone
- wait for an answer from the system.

This data was obtained by timing the users without their knowledge. These times are representative of actual-use transactions; they are not intended to indicate the minimum times possible.

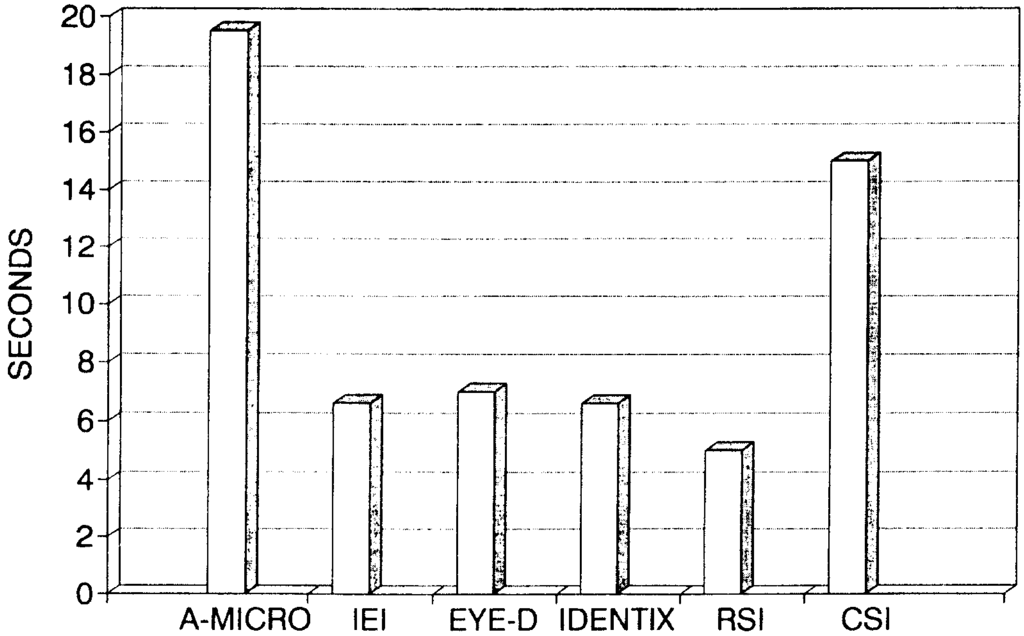


Figure 6. Average Verification Time in Seconds

Conclusions

Performance is a very important issue, but it is not the only factor in choosing a biometric identification device. The device must also be suitable for the facility in which it is installed. The present generation of biometric identification devices provides reliable and cost-effective protection of assets. Available computer interfaces and software provide effective security management with real-time control, transaction logging, and audit-tracking capabilities. The current need in the biometric identification field is to have the market make greater use of what already exists. While new biometric devices are still emerging, it is unlikely that any of them will turn the market around with a price or performance breakthrough.

The error-rate curves contain much more information about the performance of the verifiers than was included in our individual discussions. Manufacturers can provide additional information about how to apply their devices to specific requirements. Finally, it is important to keep the error rates in perspective to the real world. A 3% false accept means that there is a 97% probability that an imposter will be detected.

References

[1]Identix, Inc., 510 N. Pastoria Ave., Sunnyvale, CA 94086, (408) 739-2000

[2]Recognition Systems, Inc., 1589 Provencetown Drive, San Jose, CA 95129, (408) 257-2477

[3]Capital Securities Systems, Inc., Capital Security Operations, 9050 Red Branch Road, Columbia, MD 21045, (301) 730-8250

[4]EyeDentify, Inc., PO Box 3827, Portland, OR 97208, (503) 645-6666

[5]Alpha Microsystems, 3501 Sunflower, Santa Ana, CA 92704, (714) 957-8500

[6]International Electronics, Inc., (ECCO) VoiceKey, 32 Wexford St., PO Box 584, Needham Heights, MA 02194, (617) 449-6646.

APPENDIX

User Survey Results

Which machine do you feel:	ALPHA		EYEDENTIFY			RECOGNITION	AUTOSIG	
	MICRO	ECCO	VERIFY	RECOGNIZE	IDENTIX	SYSTEMS	SIGNON	NONE
1. is the easiest to use?	0	4	2	22	15	35	1	0
2. is the fastest?	1	4	1	28	8	35	0	0
3. is the slowest?	38	5	1	2	9	0	24	1
4. rejects you most often?	11	36	2	5	17	1	6	0
5. rejects you least often?	11	6	10	11	12	42	9	0
6. requires most concentration?	10	25	12	23	6	1	4	0
7. requires most proficiency?	11	23	9	15	11	1	9	4
8. requires least proficiency?	5	6	4	9	12	38	6	1
9. is most frustrating to use?	10	34	2	12	12	0	5	3
10. is most friendly/fun?	5	2	6	17	13	31	6	1
11. gives health/safety concerns?	1	0	23	21	1	5	0	47
12. gives invasion of privacy concerns?	0	1	2	2	3	1	16	56
13. was most difficult to enroll on?	17	21	1	1	15	2	3	18
14. was most intimidating to use?	5	16	4	6	4	0	2	41
15. best to secure a computer terminal?	7	4	12	10	22	18	7	9
16. best for door security?	3	7	18	19	13	27	3	4
17. best for bank/POS use?	1	0	13	8	21	11	23	6
18. best for large population?	2	2	5	14	16	38	3	8
19. Did you like card or pin best?	Card: 56		Pin: 17	None: 3				

NOTES:
1. Number of respondents: 76
2. Respondents were allowed to make multiple responses to each question.

DISTRIBUTION:

1 Edward J. McCallum, Director
Office of Safeguards and Security
US DOE
SA-10
Washington, DC 20545

1 William L. Barker, Acting
Dep. Asst. Secy. for Security Affairs
US DOE
SA-1
Washington, DC 20545

1 David A. Jones, Acting Director
Policy, Standards and Analysis Division
Office of Safeguards and Security
US DOE
SA-12
Washington, DC 20545

1 William J. Desmond, Chief
Physical Security Branch
Office of Safeguards and Security
US DOE
SA-121
Washington, DC 20545

1 Larry D. Wilcher, Chief
Technical and Operations Security Branch
Office of Safeguards and Security
US DOE
SA-123
Washington, DC 20545

1 Jerry C. Howell, Deputy Director
Field Operations Division
Office of Safeguards and Security
US DOE
SA-13
Washington, DC 20545

1 Donald C. Tubbs
Assessment and Integration Branch
Office of Safeguards and Security
US DOE
SA-131
Washington, DC 20545

1 Ernest E. Wagner, Chief
Weapons Safeguards and Security Operations
Branch
Office of Safeguards and Security
US DOE
SA-132
Washington, DC 20545

1 A. J. Heysel, Chief
Production/Energy Safeguards/
Security Operations Branch
Office of Safeguards and Security
US DOE
SA-133
Washington, DC 20545

1 G Dan Smith, Chief
Planning and Technology Development Branch
Office of Safeguards and Security
US DOE
SA-134
Washington, DC 20545

1 Carl A. Pocratsky
US DOE
SA-134
Washington, DC 20545

1 Marshall O. Combs, Deputy Director
Headquarters Operations Division
Office of Safeguards and Security
US DOE
SA-14
Washington, DC 20545

1 David A. Gurule, Acting Director
Security and Nuclear Safeguards Division
US DOE/AL
PO Box 5400
Albuquerque, NM 87115

1 Donald J. Cook, Director
Attn: Stan Laktosic, Tom Golder
Central Training Academy
US DOE/AL
PO Box 5400
Albuquerque, NM 87115

DISTRIBUTION (Continued):

1 Donald Jewell, Assistant Director
Central Training Academy
US DOE/AL
PO Box 5400
Albuquerque, NM 87115

1 Ronald Perry
Argonne National Laboratory
Bldg. 222 Electronics
Argonne National Laboratory
9700 South Cass Avenue
Argonne, IL 60439

1 Roger L. Black
W. Patrick Keeney
Argonne National Laboratory
Bldg. 752/MS 6000
PO Box 2528
Idaho Falls, ID 83403

1 Larry Runge and George Schoener
Safeguards and Security Division
Bldg. 50
2400 Upton Road
Upton, NY 11973

1 Kris Dahms
Safeguards and Security Division
Bldg. 703
2400 Upton Road
Upton, NY 11973

1 Robert L. Windus, Security Officer
US DOE/BP
PO Box 3621
Portland, OR 87208

1 Harold W. Kelley, Director
Safeguards and Security Division
US DOE/CH
9800 South Cass Avenue
Argonne, IL 60439

1 Rudy Dorner
Fermi National Accelerator Laboratory
MS 102
Batavia, IL 60150

1 H. R. Martin, Acting Director
Safeguards and Security Division
US DOE/ID
785 DOE Place
Idaho, Falls, ID 83402

1 Timothy L. Mitchell, L 024
Lawrence Livermore National Laboratory
PO Box 808
Livermore, CA 94550

1 Darryl B. Smith
James W. Tape
N-DO/MS E550
Los Alamos National Laboratory
PO Box 1663
Los Alamos, NM 87545

1 Jack England, Division Leader
OS-DO, MS G729
Los Alamos National Laboratory
PO Box 1663
Los Alamos, NM 87545

1 E. Wayne Adams, Director
Safeguards and Security Division
US DOE/NV
PO Box 98518
Las Vegas, NV 89193-8518

1 William G. Phelps, Director
Safeguards and Security Division
US DOE/OR
PO Box 2001
Oak Ridge, TN 37831-8570

1 J. A. Bullian, Director
Safeguards and Security Division
US DOE/PNR
PO Box 109
West Mifflin, PA 15122

2 Joseph W. Wiley, Director
Safeguards and Security Div
US DOE/RL
PO Box 550
Richland, WA 99352

DISTRIBUTION (Continued):

1 Michael Hooper, Acting Director
Safeguards and Security Division
US DOE/SF
Lawrence Livermore Laboratories
L-556
PO Box 808
Livermore, CA 94550

1 Gerorge G. Stefani, Jr., Director
Security and Safeguards Division
Schenectady Naval Reactors Office
US DOE
PO Box 1069
Schenectady, NY 12301

1 Donald J. Ornick, Director
Security Division
US DOE/OR
900 Commerce Road East
New Orleans, LA 70123

1 H. B. Gnann, Chief
Safeguards Engineering and Projects Branch
US DOE/SR
PO Box A
Aiken, SC 29808

1 Joan Christopher, Security Officer
Western Area Power Administration
US DOE
PO Box 3402
Golden, CO 80401

1 Larry Cameron
Allied Signal, Inc., Kansas City Division
2000 E. 95th Street
Kansas City, KS 64131-3095

1 Edward C. McGurren, Manager
Security Operations
Allied Signal, Inc., Kansas City Division
2000 E. 95th Street
Kansas City, KS 64131-3095

1 Harley Toy, Manager
Nuclear Services
Battelle Memorial Institute
505 King Avenue
Columbus, OH 43201

1 Boeing Petroleum Services
Attn: Security Department
850 South Clearview
New Orleans, LA 70123

1 John W. Jones, Manager
Safeguards and Security
EG&G Idaho
1955 Fremont
Idaho Falls, ID 83402-3126

1 Daniel Baker, Manager
Security
EG&G Mound
Bldg. 99
PO Box 3000
Miamisburg, OH 45432

1 K. N. Gardner
Technical Security
Bldg. 99
EG&G Mound
PO Box 3000
Miamisburg, OH 45432

1 Ron Mahan, Manager
Security Administration
EG&G Mound
Bldg. 99
PO Box 3000
Miamisburg, OH 45432

1 Vince Hanson, Manager
Protective Force
Bldg. 47
EG&G Mound
PO Box 3000
Miamisburg, OH 45342

1 Curtis L. Fellers
Technologies Department
Bldg. OSE-211
EG&G Mound
PO Box 3000
Miamisburg, OH 45342

DISTRIBUTION (Continued):

1 Roy E. Gmitter, Manager
Plant Security
General Electric Neutron Division
PO Box 2908
Largo, FL 34649

1 Holmes and Narver, Inc.
Attn: Electronics Department
PO Box 93838
Las Vegas, NV 89193-3838

1 Clifford A. Druit, Manager
Y-12 Safeguards and Security
Martin Marietta Energy Systems
Bldg. 9706-1, MS 8213
PO Box 2009
Oak Ridge, TN 37831-8213

1 James Hallihan
Mason and Hanger-Silas Mason, Co., Inc.
Pantex Plant
PO Box 30020
Amarillo, TX 79177

1 James Long
Protection Technologies of Idaho
785 DOE Place
Idaho Falls, ID 83402

1 Jeffrey Jay, Team Manager
Inspection and Technical Assessment Branch
Science Applications International Company
c/o DOE/Savannah River Operations Office
PO Box A
Aiken, SC 29802

1 Wackenhut Services, Inc.
800 West Commerce Rd., Suite 100
New Orleans, Louisiana 70123

1 Walk, Haydel, and Associates
600 Carondelet
New Orleans, LA 70130

1 Edward R. Saxon, Chief
Hanford Patrol
Westinghouse Hanford Company
SO-46
PO Box 1970
Richland, WA 99352

1 E. L. Goldman
Westinghouse Idaho Nuclear Company, Inc.
PO Box 4000
Idaho Falls, ID 83403

1 Ronald D. Klingler, Manager
Safeguards and Security
Westinghouser Idaho Nuclear Co., Inc.
MS 5102
PO Box 4000
Idaho Falls, ID 83403

1 Larry Schenk, Manager
Technical Security
Westinghouse Idaho Nuclear Company, Inc.
PO Box 4000
MS 5102
Idaho Falls, ID 83403

1 James M. Miller, Manager
Safeguards and Security
Westinghouse Materials Company of Ohio
PO Box 398704
Cincinnati, OH 45239

1 W. W. Arra
Westinghouse Savannah River Co., WSRS
703-57A, Rm. 7
PO Box 616
Aiken, SC 29802

1 M. Brinton
Westinghouse Savannah River Co., WSRS
703-45A, Rm. 110
PO Box 616
Aiken, SC 29802

1 C. J. O. Cox
Westinghouse Savannah River Co., WSRS
703-45A, Rm. 150
PO Box 616
Aiken, SC 29802

1 J. W. Maloney, Manager
Safeguards and Security
Westinghouse Savannah River Co., WSRS
PO Box 616
Aiken, SC 29802

DISTRIBUTION (Concluded):

1 S. C. Nashatker
Westinghouse Savannah River Co., WSRS
703-45A, Rm. 151
PO Box 616
Aiken, SC 29802

1 W. W. Rajczar
Westinghouse Savannah River Co., WSRS
703-42A, Rm. 115
PO Box 616
Aiken, SC 29802

1 John M. Samuels, Managers
Safeguards and Security Department
Westinghouse Savannah River Co., WSRS
PO Box 616
Aiken, SC 29802

1	3430	R. P. Kelly
1	3431	J. A. Kaiser
1	3432	D. E. Kerome
1	3433	R. M. Workhoven
1	3437	R. G. Baca
1	5200	J. Jacobs
1	5210	C. C. Hartwigsen
1	5211	S. H. Scott
1	5219	R. W. Moya
1	5220	J. W. Kane
1	5230	H. M. Witek
1	5231	D. J. Gangel
1	5233	D. C. Hanson
1	5234	J. C. Mitchell
1	5238	R. F. Davis
1	5240	D. S. Miyoshi
10	5240A	M. W. Green
1	5245	I. G. Waddoups
20	5245	J. P. Holmes
1	5245	L. S. Wright
1	5248	R. P. Syler
5	5248	R. L. Maxwell
1	5249	B. J. Steele
1	5260	J. R. Kelsey
1	5268	S. J. Weissman
1	8530	M. A. Pound
1	8531	D. R. Charlesworth
1	8536	C. L. Knapp
1	8523	R. C. Christman
5	3141	S. A. Landenberger
8	3145	Document Processing For DOE/OSTI
3	3151	G. C. Claycomb

SCHLAGE

ALLEGION

3rd Party PoE Adapter Use: F-Series & G-Series

This document stands to act as a procedural guide for when using a 3rd party PoE adapter with the HandReaders, both F-Series & G-Series[1]. Schlage has performed testing to confirm that when using a PoE adapter[2], the HandReader will operate normally; so long as the minimum power requirements are met. Please use the following instructions as a guideline for initial set up of the Wi-Fi adapter.

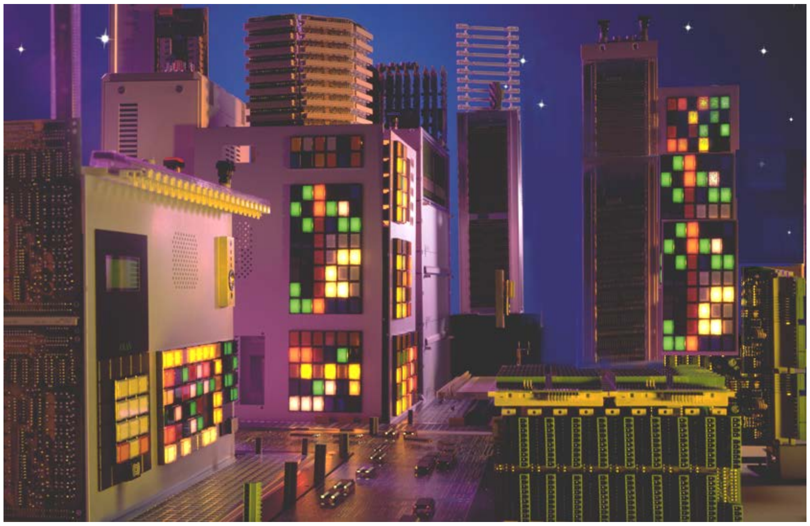
Setup Summary of the PoE Injector and PoE Splitter (One-on-One)

Host --> Switch --> PoE Injector --> PoE Splitter --> HandReader

1. Connect from a host PC to a network switch via an Ethernet cable
2. Connect another Ethernet cable from the network switch to "LAN IN" on the PoE Injector
3. Connect between "Power/Data Out" of PoE Injector and "Power/Data In" of PoE Splitter by using Ethernet cable
    a. It is important to note the distance between the PoE Injector and PoE Splitter. PoE supported distances may vary depending on the manufacturer[3].
        i. Power degradation could occur if lengths are exceeded, which could have undesirable effects in the performance of the HandReader.
4. Connect power cable to the PoE Injector
5. Connect "LAN OUT" from PoE Splitter to HandReader Ethernet port
6. Connect "DC OUT" from PoE Splitter to HandReader power port
    a. It is important to ensure that the outputting power is at least 12V at 1A.
    b. It is important to ensure that the power (barrel) connector is compatible with HandReader.
        i. Power degradation could occur when inadequate power is outputted from the splitter, which could have

[1] F-Series models include: all HandPunch & HandKey models that have Ethernet enables. G-Series includes the GT-400.
[2] PoE Device Detail: Model Name & Number; TP-LINK PoE Adapter Kit: TL-POE200
[3] The TL-POE 200 maximum transfer length is 100 meters (330 ft)

Application Notes Biometric Templates on Contactless Smart Cards



HP3000 / HKII – IOLAN XXW

Version 5.0

Contents

Versions

Release	Date	Status	Description
1.0	6/3/2002	Concept	Application notes on the integrated solution of the HP3000 / HKII with the IOLAN XXW MIFARE reader.
1.1	10/07/2002	First Release	Added Upload Keys From Project Card based on pincode
1.2	10/08/2002		Upload Keys From Project Card based on MIFARE keys
2	06/20/05		Added Notes on Card management
3	07/08/09	Special Release	Added Support for two card configurations, card type 1 uses Sector 2 and 3, card type 2 uses Sector 13 and 14
4	06/04/11	Special realease	Added Support for two card configurations, One type card uses sector 2&3, second type uses sector 11&12
5	02/27/12	Combined release	Merges different types of documentations into one, extra information on project cards

References

#	Title	Version	Authors	Date
1	RSI IOLAN ISI Hand Punch 4000	1.4	ISI	04/08/01
2	SmartEncoder Manual	8	ISI	06/01/10

Biometric Templates on Contactless Smartcards

Instead of storing user templates in centralized databases, the contactless smart card technology allows users to store templates directly on the user card, thus preventing complicated template management over several locations. This new approach allows a direct check on ownership of the card at the access points where the card is presented. Stolen cards will be left unusable to others.

Recognition Systems and Iolan Systems Inc. have developed a turn-key integrated solution of Smart card reader / writer and the RSI products. The combination of HandReader and smart card reader manages templates on the user card. No centralized storage of the templates is required. Performance and distribution problems are solved in this integrated solution. The contactless smart card reader is built into the unit, thus reaching an optimal integration and user friendliness level.

Integration HP3000 / HKII / XXW

User interface and networking aspects are handled by the HP3000 / HKII; the XXW reader is responsible for reading from and writing to the MIFARE Cards. This setting allows the HP3000 a uniform interface where no project specific items like keys and card location have to be programmed; the XXW reader is prepared for easy adaptation to these project specific settings and can be programmed to project specific needs.
Also, from a security point of view this setup is a good one; no MIFARE keys will be transported from the HP3000 to the XXW; thus allowing no interception of this type of information on the communication line.

Functionality

After enrolling users on their own user card, using a project specific procedure the operation of the system is very user friendly:

- The user card IS presented to the smart card reader
- ID information and template are read from the card
- The user places their hand on the HandReader
- The HandReader checks the actual hand image against the template on the card
- If the user is verified, the door open contact is activated or Wiegand output is created
- When necessary, an updated template is written back to the card

Since the smart card reader uses a dedicated port of the HandReader, the normal communication options stay intact, thus allowing easy upgrades of existing projects without changing the technical infra-structure.

Only 2 out of 16 sectors (1K card) are used to store the Template and ID information for this application and the rest of the card is freely available to other applications. The information on the card is securely stored behind project specific MIFARE keys so only cards created for a specific project can be read by the integrated combination.

Project Cards

The function of the project card that is shipped with every reader is to upload the MIFARE keys to the HandReader. This allows companies to bring the MIFARE keys that they use to secure sector 2 and 3 of the badges (user cards) they have in use to the HandReader reader. For any MIFARE reader to work with user cards, there will need to be a match between MIFARE keys in the card and reader. When you receive the HandReader from the factory, the public keys set A0A1A2A3A4A5, B0B1B2B3B4B5 are pre-loaded in the project card and already brought to the HandReader for test purposes.

There are two kinds of projects: Demo projects that come with a demo project card and Production projects. Production Projects are installations that are used for secure access control.

Demo projects

HandReaders belonging to a demo project are used in demo situations like on site sales demo, test situations and for readers used in shows. Basically these readers use the same type of project card; any demo project card will work with any demo reader. Security is not an issue here so it is convenient that any project card will work with all the readers on site.

Production projects

Every production project has its own project card, and it is important that a project card created for company A does not work on the site of company B. Otherwise, it would be possible that company A could change reader keys in company B readers. The combination of reader / project card is embedded in the reader software and can only be changed by reprogramming the reader.

Uploading user card keys to the HandReader

The user cards that are used by the employees to get access to a building are protected by secret MIFARE keys. When default MIFARE cards are purchased, they are unprotected and block 3 for all sectors will contain a public keyset, depending on the chip manufacturer either A0A1A2A3A4A5, B0B1B2B3B4B5 or FFFFFFFFFFFF, FFFFFFFFFFFF.

Before going into production the public keys need to be replaced by a new set of secret keys, and this can be done with the SmartEncoder software.

The next step is to get the HandReaders to work with the new secret keys. The project card will take care of transporting the secret MIFARE keysets to the HandReader.

Uploading MIFARE keys to project card

There are a couple of options to get the company specific secret MIFARE keys in the project card:

1.) ISI can upload the keys and send them with the readers. For this to work we will need the secret keys in Austin under a NDA

Companies can use the SmartEncoder software and upload the secret keys on site.

User cards

MIFARE is a remote coupling smart card system for multi-applications. It was tailored especially for automatic fare collection (AFC) and similar applications. A plastic card the size of a credit card is passed over a reader target within a distance of up to 10 centimeters, or 4 inches. Reading information from the card and writing information back to the card takes only a few milliseconds. Thus, for example, passengers boarding a bus or subway train can simply walk through gates while the transaction takes place.

When moving the card over the reader target, passengers can leave the card in their wallet, even if it contains coins. The world largest installation of contactless smartcards services the 12 million inhabitants of Seoul, where MIFARE cards are used for payment in the public transport system, and related applications. This project has proven the maturity and reliability of MIFARE.

The MIFARE Cards can handle multiple applications. Every sector can carry information for a different application. On the 1K MIFARE cards each sector is divided into 4 blocks of information; each block can contain 16 bytes of data; block 3 of each sector is used for key storage and access conditions for that particular sector.

0	Block 0 16 bytes	Block 1 16 bytes	Block 2 16 bytes	Sector Keys and AC
1	Block 0 16 bytes	Block 1 16 bytes	Block 1 16 bytes	Sector Keys and AC
2	Block 0 16 bytes	Block 1 16 bytes	Block 1 16 bytes	Sector Keys and AC
3	Block 0 16 bytes	Block 1 16 bytes	Block 1 16 bytes	Sector Keys and AC
4	Block 0 16 bytes	Block 1 16 bytes	Block 1 16 bytes	Sector Keys and AC
5	Block 0 16 bytes	Block 1 16 bytes	Block 1 16 bytes	Sector Keys and AC
6	Block 0 16 bytes	Block 1 16 bytes	Block 1 16 bytes	Sector Keys and AC
7	Block 0 16 bytes	Block 1 16 bytes	Block 1 16 bytes	Sector Keys and AC
8	Block 0 16 bytes	Block 1 16 bytes	Block 1 16 bytes	Sector Keys and AC
9	Block 0 16 bytes	Block 1 16 bytes	Block 1 16 bytes	Sector Keys and AC
10	Block 0 16 bytes	Block 1 16 bytes	Block 1 16 bytes	Sector Keys and AC
11	Block 0 16 bytes	Block 1 16 bytes	Block 1 16 bytes	Sector Keys and AC
12	Block 0 16 bytes	Block 1 16 bytes	Block 1 16 bytes	Sector Keys and AC
13	Block 0 16 bytes	Block 1 16 bytes	Block 1 16 bytes	Sector Keys and AC
14	Block 0 16 bytes	Block 1 16 bytes	Block 1 16 bytes	Sector Keys and AC
15	Block 0 16 bytes	Block 1 16 bytes	Block 1 16 bytes	Sector Keys and AC

More information on MIFARE cards can be found at: www.MIFARE.net

User Cards: Application Sectors

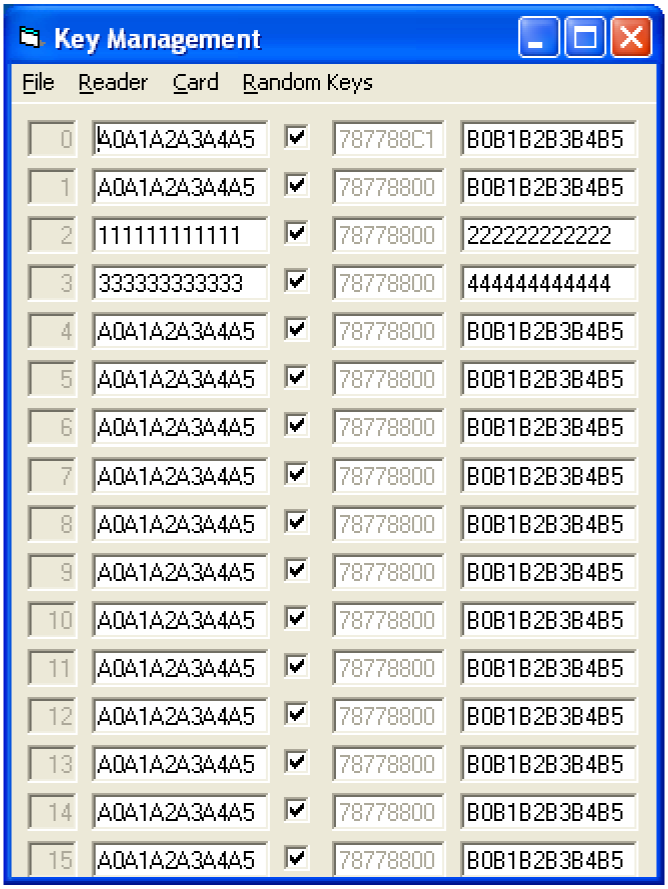
For the HP3000, application sector 2 and 3 are used to store the information. It is possible to use different sector pairs if 2 and 3 are already in use in your project. When a different set of sectors needs to be used we need to have this information when ordering the readers.

It is even possible to use a mix of sectors on user cards. For example, one set of cards uses sector 2 and 3 and another set of cards uses sector 12 and 13. This can be necessary after mergers of companies where one set of user cards already uses sector 2 and 3 for other applications.

User Cards: Initialization

Preparing the MIFARE cards for operation in a project requires the following aspects:

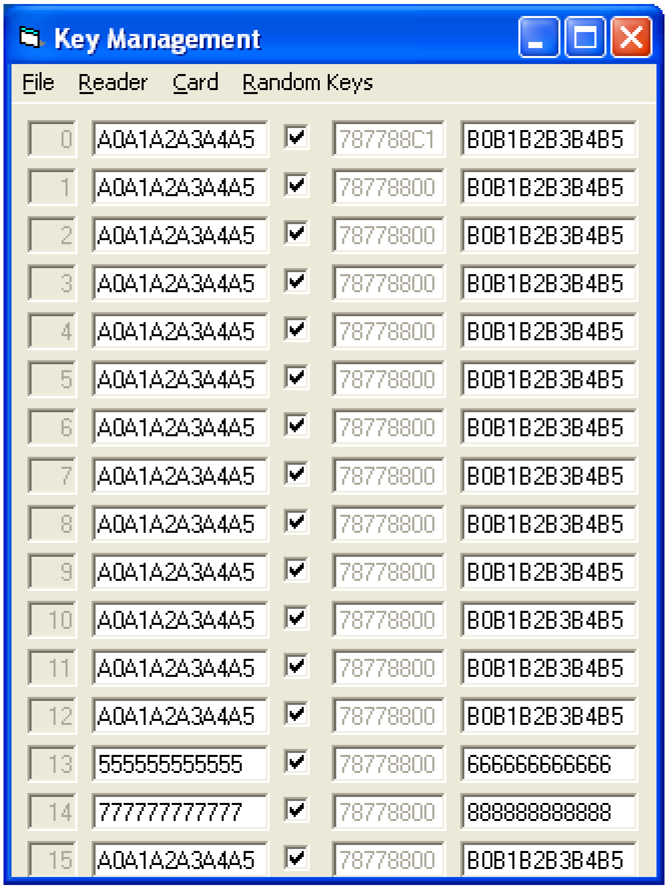
- Defining a card layout (where on the card will the applications store and retrieve their data?)
- Defining key sets for the user cards
- Initializing the cards (put the keys on the card trailers). Take note, that sector 2 and 3 have read access with Key A and write access with key B.
- Initializing the cards for the different applications (put startup information on the card)



0	A0A1A2A3A4A5	☑	787788C1	B0B1B2B3B4B5
1	A0A1A2A3A4A5	☑	78778800	B0B1B2B3B4B5
2	111111111111	☑	78778800	222222222222
3	333333333333	☑	78778800	444444444444
4	A0A1A2A3A4A5	☑	78778800	B0B1B2B3B4B5
5	A0A1A2A3A4A5	☑	78778800	B0B1B2B3B4B5
6	A0A1A2A3A4A5	☑	78778800	B0B1B2B3B4B5
7	A0A1A2A3A4A5	☑	78778800	B0B1B2B3B4B5
8	A0A1A2A3A4A5	☑	78778800	B0B1B2B3B4B5
9	A0A1A2A3A4A5	☑	78778800	B0B1B2B3B4B5
10	A0A1A2A3A4A5	☑	78778800	B0B1B2B3B4B5
11	A0A1A2A3A4A5	☑	78778800	B0B1B2B3B4B5
12	A0A1A2A3A4A5	☑	78778800	B0B1B2B3B4B5
13	A0A1A2A3A4A5	☑	78778800	B0B1B2B3B4B5
14	A0A1A2A3A4A5	☑	78778800	B0B1B2B3B4B5
15	A0A1A2A3A4A5	☑	78778800	B0B1B2B3B4B5

Keyset for type 1 cards, public keys need to be replaced by keys relevant to your project. (right)

Keyset for type 2 cards, public keys need to be replaced by keys relevant to your project. (right)



0	A0A1A2A3A4A5	☑	787788C1	B0B1B2B3B4B5
1	A0A1A2A3A4A5	☑	78778800	B0B1B2B3B4B5
2	A0A1A2A3A4A5	☑	78778800	B0B1B2B3B4B5
3	A0A1A2A3A4A5	☑	78778800	B0B1B2B3B4B5
4	A0A1A2A3A4A5	☑	78778800	B0B1B2B3B4B5
5	A0A1A2A3A4A5	☑	78778800	B0B1B2B3B4B5
6	A0A1A2A3A4A5	☑	78778800	B0B1B2B3B4B5
7	A0A1A2A3A4A5	☑	78778800	B0B1B2B3B4B5
8	A0A1A2A3A4A5	☑	78778800	B0B1B2B3B4B5
9	A0A1A2A3A4A5	☑	78778800	B0B1B2B3B4B5
10	A0A1A2A3A4A5	☑	78778800	B0B1B2B3B4B5
11	A0A1A2A3A4A5	☑	78778800	B0B1B2B3B4B5
12	A0A1A2A3A4A5	☑	78778800	B0B1B2B3B4B5
13	555555555555	☑	78778800	666666666666
14	777777777777	☑	78778800	888888888888
15	A0A1A2A3A4A5	☑	78778800	B0B1B2B3B4B5

User Cards: Existing projects

When user cards are already in use in your project, they are probably already initialized. However, it should be checked that sector 2 and 3 are secured with for this project unique MIFARE keys. Also, check if there is read access with Key A and write access with key B.

User Cards: New Projects

When user cards are being bought off the factory, they need to be initialized. From the factory, the cards are unprotected and they have public keys that are known to everyone that works with MIFARE cards. Before handing out the cards to the users, all sectors will need to be protected with secret project keys. This initialization process can be done with the SmartEncoder software and reader or any other software from different manufacturers. More information on how to initialize cards can be found in the SmartEncoder manual.

Optional SmartEncoder Software

Software

Defining key sets and writing them to project cards can be done on site, through the use of the software package: “Smart Encoder”. In the software, MIFARE keys will have to be defined to be used for the sectors **2** and **3.** The Standard Key management screen can be used to define keys A and B for sectors 2 and 3 the key set has to be saved to the Project Card, presenting the card to the smartcard readers in the project will upload the new user card keys to the reader.

Step I

To start, you need to have a working combination of Smart Encoder 8 software on a PC with the desktop MIFARE reader powered up and connected to the RS232 port.

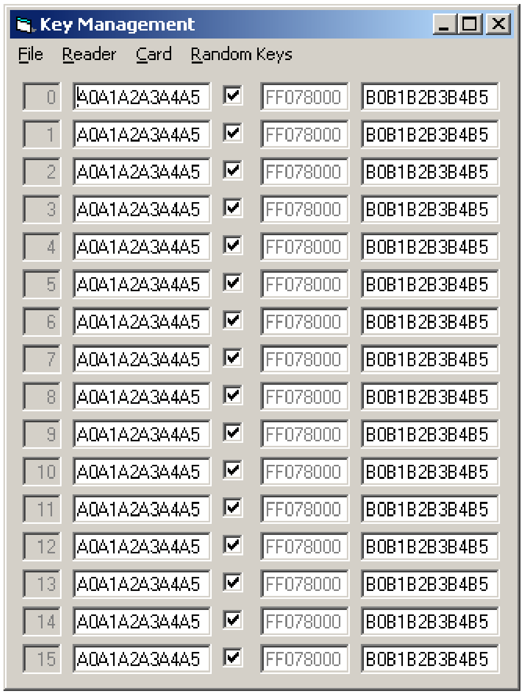
At start-up of the software, the message “Detected ISI Reader” should be shown in the startup screen of the software. When the reader is detected by the software, the green LED will light up.

Step II

The first step is to define keys A and B for the sectors 2 and 3 (these are the sectors the HandReader uses for storing and retrieving information).

Choose **File**, **Key Management** from the main menu, the next screen on the right should show:

Standard the public key set I is shown in this screen. With File open other key sets can be edited and saved.



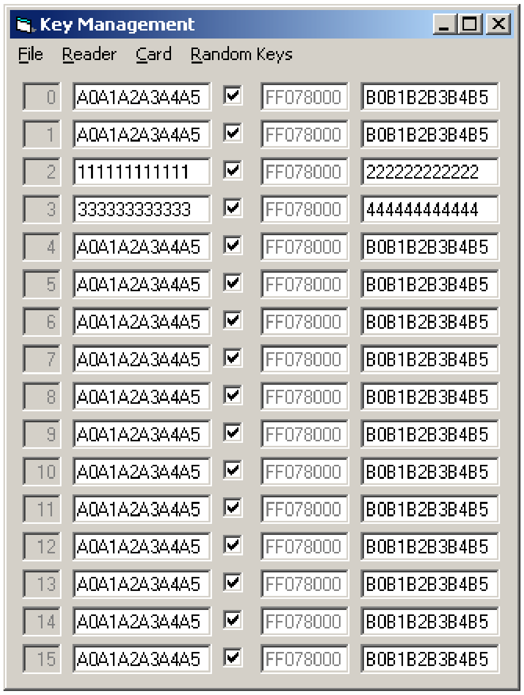
0	A0A1A2A3A4A5	☑	FF078000	B0B1B2B3B4B5
1	A0A1A2A3A4A5	☑	FF078000	B0B1B2B3B4B5
2	A0A1A2A3A4A5	☑	FF078000	B0B1B2B3B4B5
3	A0A1A2A3A4A5	☑	FF078000	B0B1B2B3B4B5
4	A0A1A2A3A4A5	☑	FF078000	B0B1B2B3B4B5
5	A0A1A2A3A4A5	☑	FF078000	B0B1B2B3B4B5
6	A0A1A2A3A4A5	☑	FF078000	B0B1B2B3B4B5
7	A0A1A2A3A4A5	☑	FF078000	B0B1B2B3B4B5
8	A0A1A2A3A4A5	☑	FF078000	B0B1B2B3B4B5
9	A0A1A2A3A4A5	☑	FF078000	B0B1B2B3B4B5
10	A0A1A2A3A4A5	☑	FF078000	B0B1B2B3B4B5
11	A0A1A2A3A4A5	☑	FF078000	B0B1B2B3B4B5
12	A0A1A2A3A4A5	☑	FF078000	B0B1B2B3B4B5
13	A0A1A2A3A4A5	☑	FF078000	B0B1B2B3B4B5
14	A0A1A2A3A4A5	☑	FF078000	B0B1B2B3B4B5
15	A0A1A2A3A4A5	☑	FF078000	B0B1B2B3B4B5

The relevant keys should be typed in HEX format (0 – 9, A – F) on position 2 and 3. The first key is the “A” key for reading information the second the “B” key for writing information to the card. The field in the middle is the access conditions for the sector. For our purpose: Key Upload they are not relevant.

As an example the keys “111111111111” are typed as key A for sector 2 and “222222222222” as key B for sector 2.

“333333333333” key A to sector 3 and “444444444444” as key B for sector 3.

When the keys are defined, the new key set can be stored on a floppy disk with **File**, **Save As**. Store the keys in a secure place!



0	A0A1A2A3A4A5	☑	FF078000	B0B1B2B3B4B5
1	A0A1A2A3A4A5	☑	FF078000	B0B1B2B3B4B5
2	111111111111	☑	FF078000	222222222222
3	333333333333	☑	FF078000	444444444444
4	A0A1A2A3A4A5	☑	FF078000	B0B1B2B3B4B5
5	A0A1A2A3A4A5	☑	FF078000	B0B1B2B3B4B5
6	A0A1A2A3A4A5	☑	FF078000	B0B1B2B3B4B5
7	A0A1A2A3A4A5	☑	FF078000	B0B1B2B3B4B5
8	A0A1A2A3A4A5	☑	FF078000	B0B1B2B3B4B5
9	A0A1A2A3A4A5	☑	FF078000	B0B1B2B3B4B5
10	A0A1A2A3A4A5	☑	FF078000	B0B1B2B3B4B5
11	A0A1A2A3A4A5	☑	FF078000	B0B1B2B3B4B5
12	A0A1A2A3A4A5	☑	FF078000	B0B1B2B3B4B5
13	A0A1A2A3A4A5	☑	FF078000	B0B1B2B3B4B5
14	A0A1A2A3A4A5	☑	FF078000	B0B1B2B3B4B5
15	A0A1A2A3A4A5	☑	FF078000	B0B1B2B3B4B5

Step III

The Key Set with the relevant keys for sector 2 and 3 need to be transported to the HandReader, this is done by means of the project specific Project Card. Put the Project Card on the IOLAN Desktop Reader. and choose option **Card**, **Save To Card** the key background will light up green and the key set is stored.

Step IV

Present the Project Card to the powered up HandReader, the card will be recognized by the IOLAN reader and the keys will be uploaded to the MIFARE module. A beep and Yellow LED can be heard and seen after a successful upload.

The key upload process can be repeated indefinitely with different keys.

Step V

The user cards for the project should have the right keys for this project on sectors 2 and 3. The access conditions for sector 2 and 3 should allow **read with key A** and **write with key B**. See the Smart Encoder manual for instructions. For example the settings “78778800” will work with this application.

70200-0041

BR-100

Installation Instructions

This installation guide consists of 3 sections:

- How to connect the BR-100 to an F3 HandReader
  - Bell Output - page1
  - Lock Output - page 2

F3 HandReader Models
HP-1000E, HP-1000-F3, HP-2000-F3, HP-3000-F3, HP-3000E-F3,
HP-4000-F3, HP-4000-S-F3, HK-2-F3, HK-2-CR-F3, HP-1000E-XL,
HP-1000-XL, HP-2000-XL, HP-3000-XL, HP-3000E-XL

- How to connect the BR-100 to an F1 HandReader
  - Bell Output - page 2
  - Lock Output - page 3

F1 HandReader Models
HP-50E, HP-1000, HP-2000, HP-3000, HP-3000E,
HP-4000, HP-4000-S, HK-2, HK-CR

- How to connect the BR-100 to an E Series HandReader
  - Bell Output - page 3
  - Lock Output - page 4

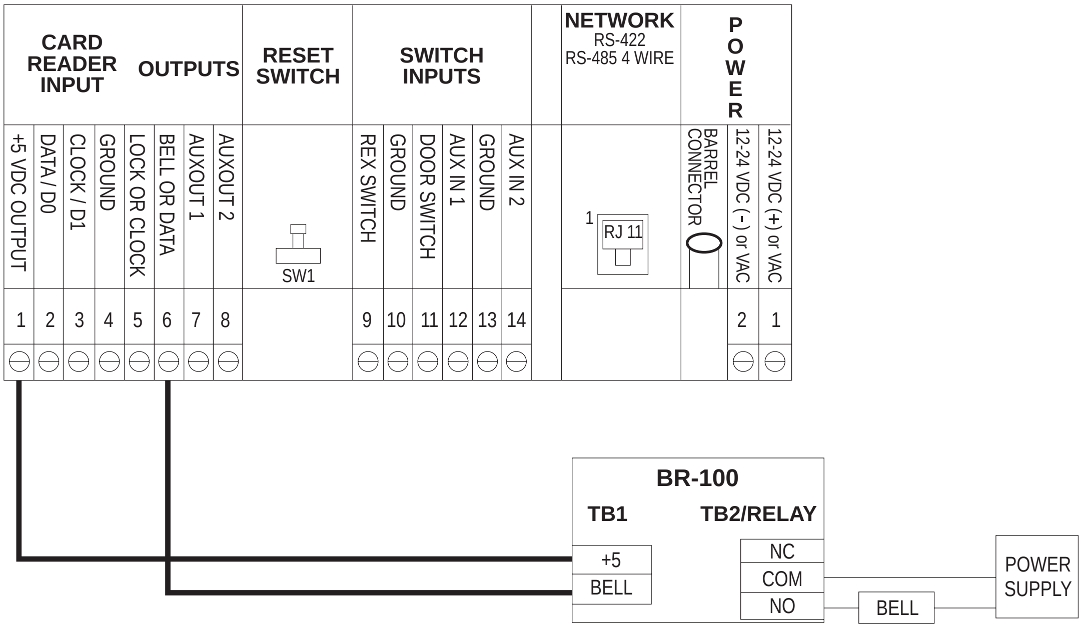
E Series HandReader Models
ID3D-R, ID3D-RW, LH-100, LH-100-RW

⚠ **CAUTION: Please choose your model carefully as the reader can be damaged by incorrectly wiring the relay.**

➔ *See page 4 for examples on wiring the BR-100 relay to a lock.*

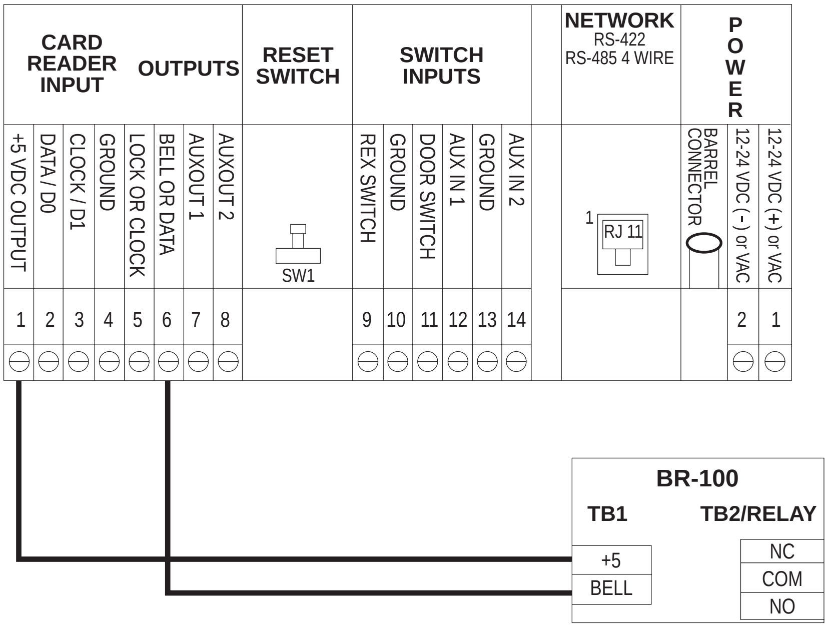
How to connect the BR-100 to an **F3 HandReader** for…

Bell Output



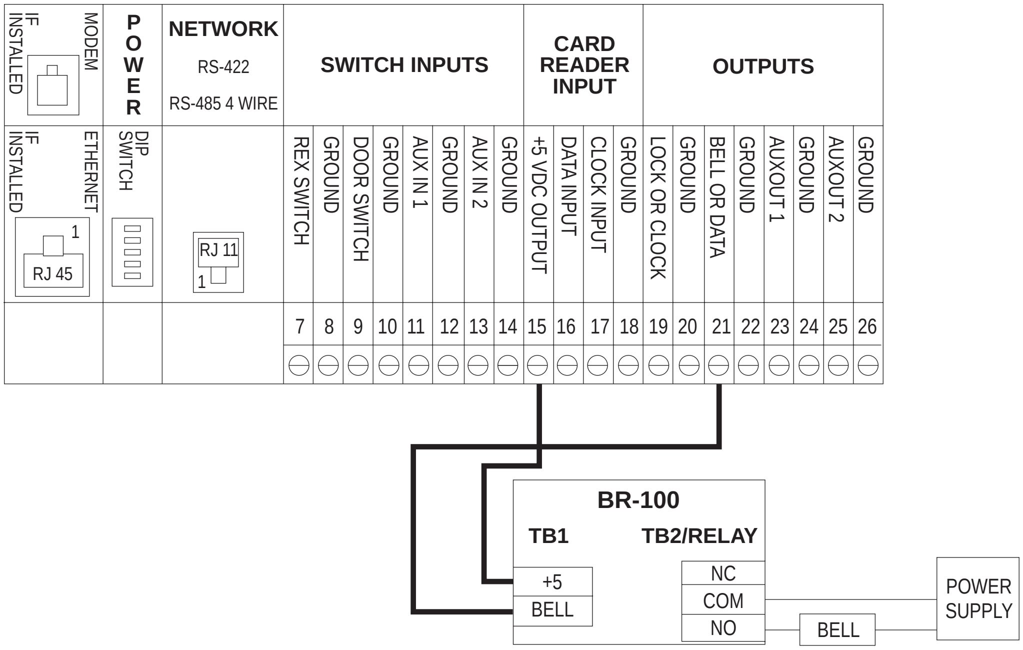
How to connect the BR-100 to an **F3 HandReader** for…

Lock Output



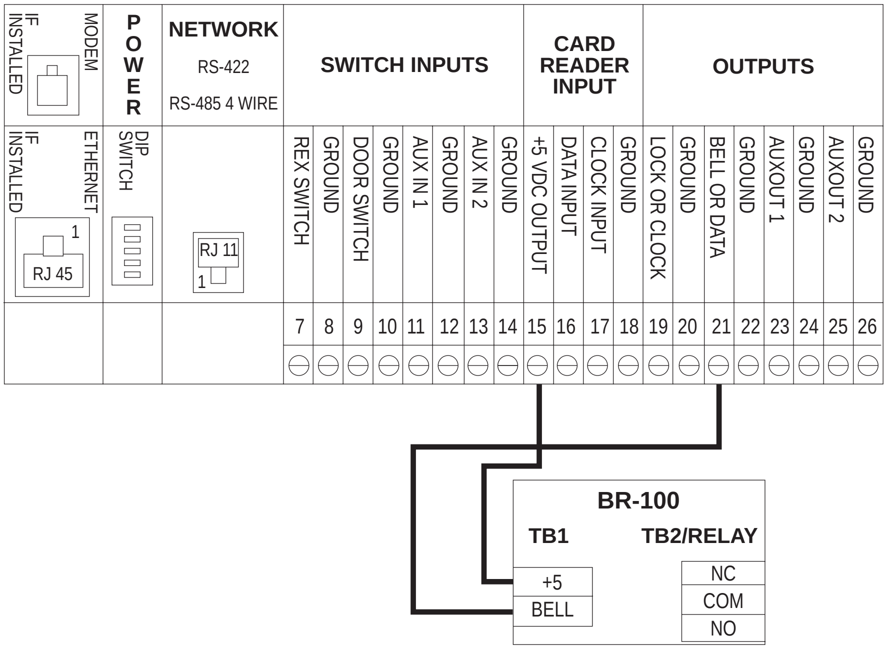
How to connect the BR-100 to an **F1 HandReader** for…

Bell Output



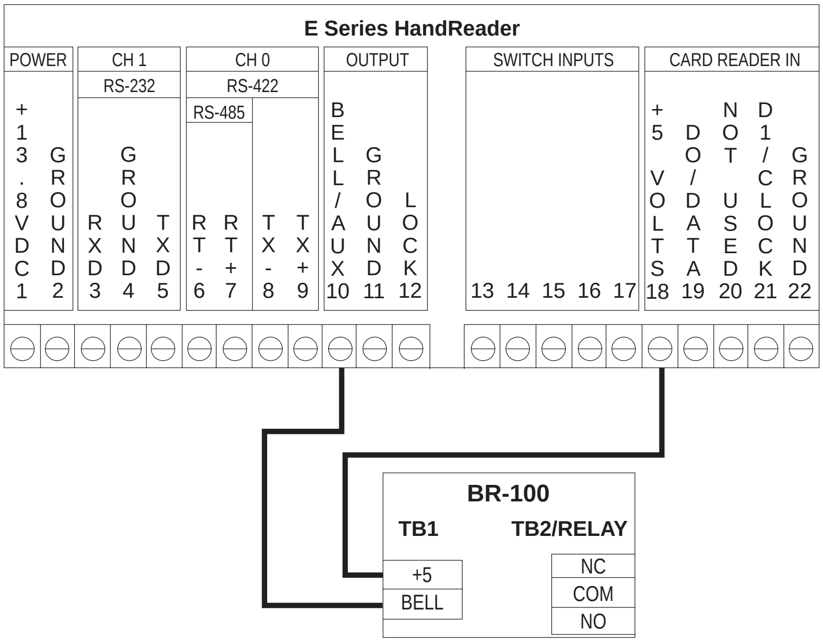
How to connect the BR-100 to an **F1 HandReader** for…

Lock Output



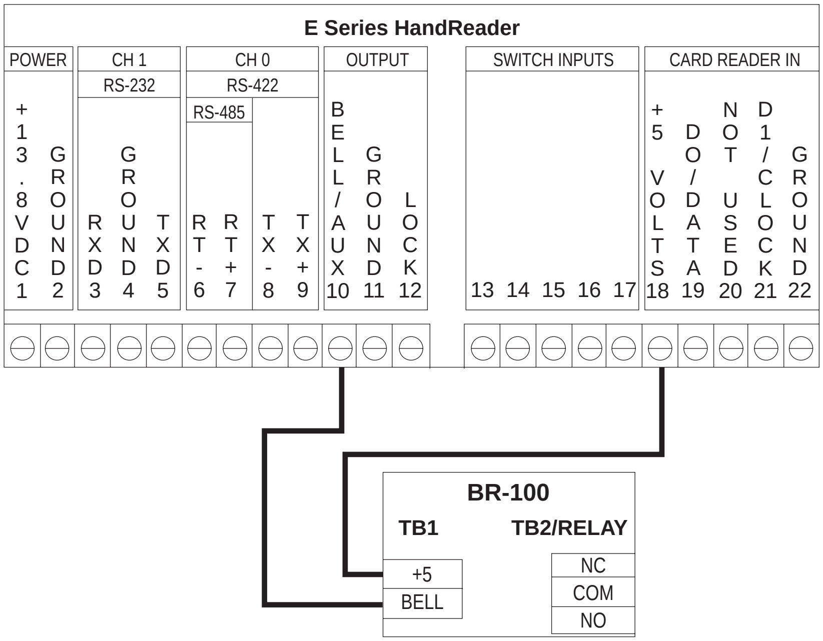
How to connect the BR-100 to an **E Series HandReader** for…

Bell Output



How to connect the BR-100 to an **E Series HandReader** for…

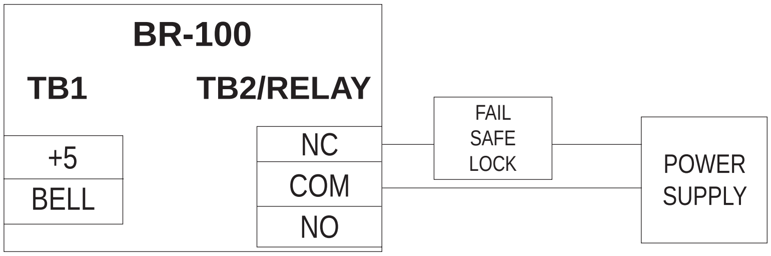
Lock Output



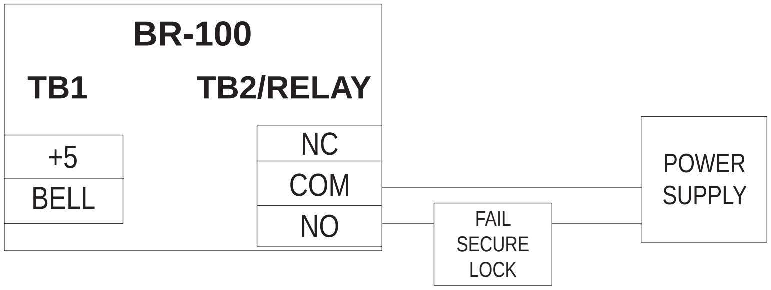
Wiring Examples

⚠ **WARNING: These are generic examples. Please follow the wiring guidelines provided by the manufacturer of the lock.**

Fail Safe Lock: The fail-safe lock guarantees access if power fails. The lock requires power to stay locked; during a power failure, access is granted.



Fail Secure Lock: The fail-secure lock guarantees security if power fails. The lock requires power to unlock; during a power failure, access is denied.

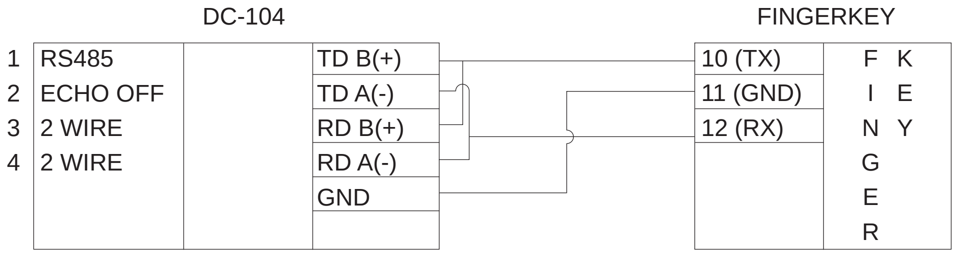


Ingersoll Rand
Security Technologies
(877) 671-7011
Printed in Country
70200-0041 Rev. 8/11-c

70200-0063

DC-104

Installation Instructions



DIP switches on the DC-104 need to be set as follows:

1. RS485
2. Echo off
3. 2 wire
4. 2 wire

SW1 DIP Switch on the FingerKey needs to be set as follows:

1. ON
2. ON
3. OFF
4. OFF

- Jumper needs to be installed between the TD B(+) and RD B(+)= TD/RD(+)
- Jumper needs to be installed between the TD A(-) and RD A(-)= TD/RD(-)
- The TD/RD(+) on the DC-104 connects to terminal #10(TX) of the FingerKey.
- The TD/RD(-) on the DC-104 connects to terminal #12(-) of the FingerKey.
- The GND on the DC-104 connects to terminal #11(Ground) of the FingerKey.

(877) 671-7011
Printed in Country
70200-0063 Rev. 8/11-b

70200-0014

F Series Ethernet Upgrade

Installation Instructions

Ethernet Requirements

- A TCP/IP network
- CAT 5 cable or better
- 10baseT
- Static IP address, gateway and subnet addresses (if needed)
- Port 3001 must be opened

Power Up

A reader with an Ethernet adapter installed and the network cable plugged in will automatically detect the presence of the Ethernet adapter upon power up. If the network cable is not plugged in prior to power being applied, the Ethernet adapter will not see the network and the reader will ask if the cable is plugged in. Plug in the network cable and power cycle the reader. When the reader boots up and detects the network, the LCD will display an IP address and then proceed to either the "Enter ID" or "Ready" prompt.

Address Requirements

The EN-100/200 does not support DHCP; therefore a static IP address is required and must be programmed into the reader before the adapter will communicate with the network.

Obtain all addresses that are required for the network from the system administrator of the site. If there is no need for a gateway address, set it to all zeros (i.e. 000.000.000.000). If the reader is required to communicate over a WAN, the subnet mask needs to be converted to a host bit number. If a subnet mask is not needed, set the host bit to 0. Have the system administrator set Port 3001 to allow access on all switches and routers between the EN-100/200 and host program.

To configure the Ethernet adapter, follow these steps:

1. The reader's IP address resides in the SET SERIAL command of the SETUP menu, which is by default in the menu 2 of the reader.
2. Press # when the LCD display shows.

```
SET SERIAL
* NO  YES #
```

3. Enter the 12 digit IP address using leading zeros and press #.
4. Enter the 12 digit gateway using leading zeros or enter all zeros if no gateway is required then press #.
5. Enter the host bits if the reader will be communicating over a WAN, or leave the host bits set to 0 if not needed and then press #.
6. Press CLEAR twice to exit menu.

Subnet to Host Bits Conversions

The readers will only accept a host bit, so the subnet mask needs to be converted. The only legal subnet masks and host bits are listed below:

SUBNET MASK	HOST BITS
255.255.255.255	0
255.255.255.254	1
255.255.255.252	2
255.255.255.248	3
255.255.255.240	4
255.255.255.224	5
255.255.255.192	6
255.255.255.128	7
255.255.255.0	8
255.255.254.0	9
255.255.252.0	10
255.255.248.0	11
255.255.240.0	12
255.255.224.0	13
255.255.192.0	14
255.255.128.0	15
255.255.0.0	16
255.254.0.0	17
255.252.0.0	18
255.248.0.0	19
255.240.0.0	20
255.224.0.0	21
255.192.0.0	22
255.128.0.0	23
255.0.0.0	24

Installing the EN-200 Ethernet Adapter

➔ *The EN-100 Ethernet adapter is not field installable. Call the factory for installation.*

⚠ **CAUTION: This procedure requires a cold boot. Back up all data with the host program before proceeding.**

⚠ **CAUTION: If the reader is equipped with an optional battery backup, remove the J7 jumper before proceeding. Failure to do so could lead to risk of shock and/or main board damage, if the ground strap were to touch the main board. See figure 9.**

⚠ **CAUTION: Before removing the back plate of reader, wear a grounding wrist strap to help aid in protecting the circuit board from any ESD damage that might occur from improper handling.**

1. Unlock the reader and rotate.
2. Disconnect the power supply from the board.
3. Remove and tag all external connections to make correct re-attachment.
4. Remove HandReader from wall by sliding it to the right, away from the wall mount. See figure 1 below.

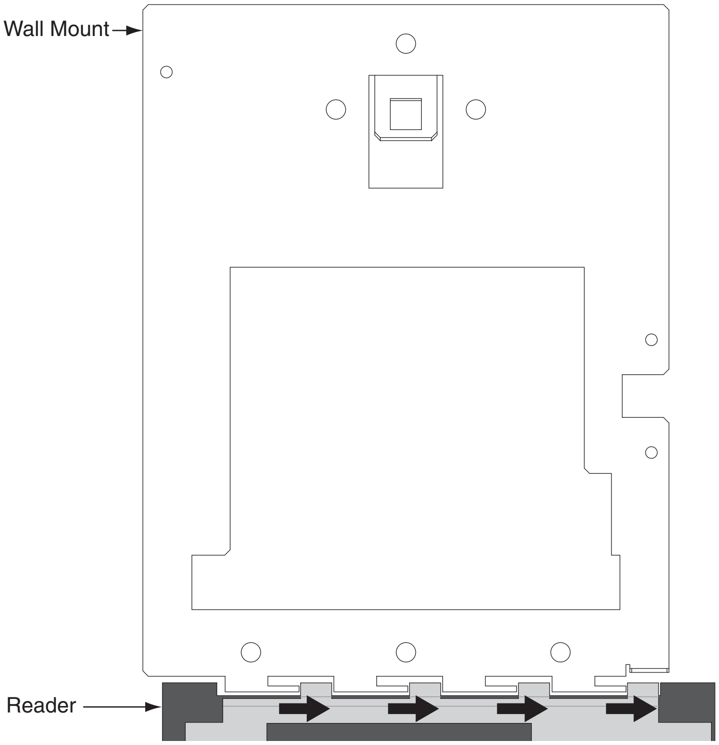


Figure 1

5. Set the reader on a firm surface such as a table. Remove the four screws that secure the back plate to the reader. Remove the grounding screw and/or ground lug (if present). See figure 2 below.

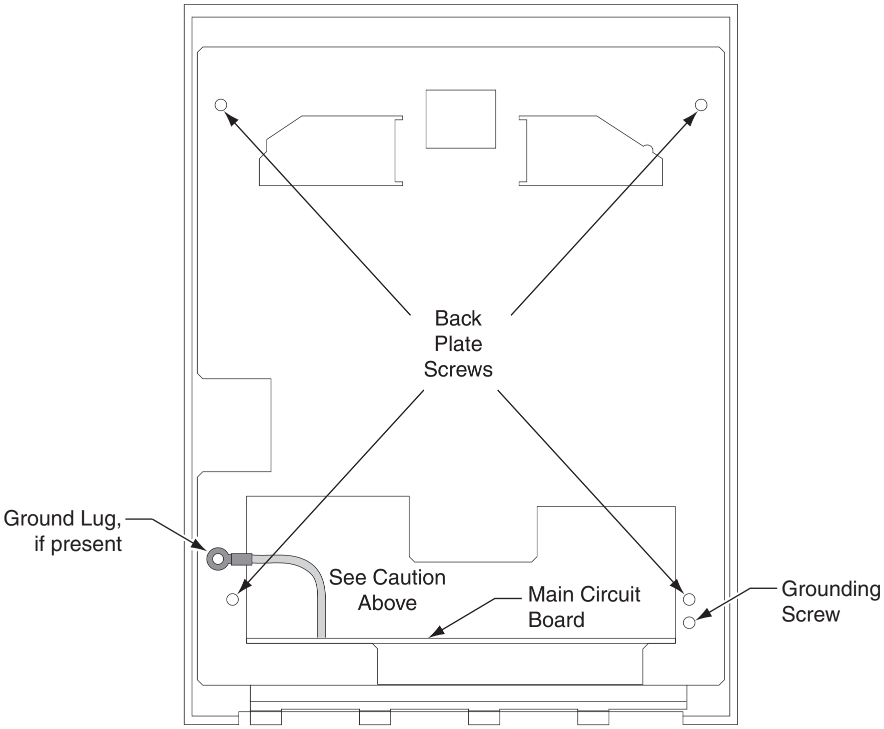


Figure 2

6. Carefully remove the back plate.

7. Locate the cable on the left side of the reader that runs from the top panel circuit board to the main circuit board. Disconnect this cable from J9 on the main circuit board. See “1” on figure 3. To remove the J9 connector from the main circuit board, depress the retaining clip on the connector and pull upwards. Take care to pull on the connector and to not pull on the cable. See figure 4 below.

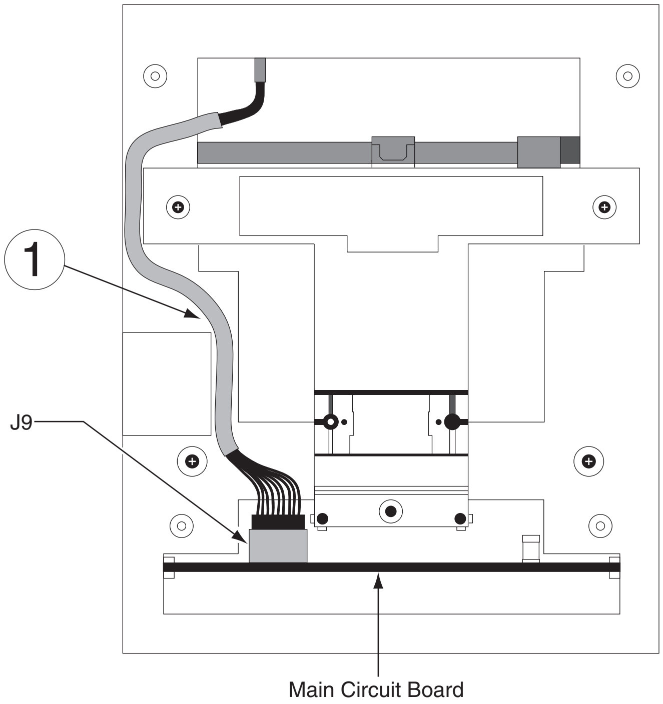


Figure 3

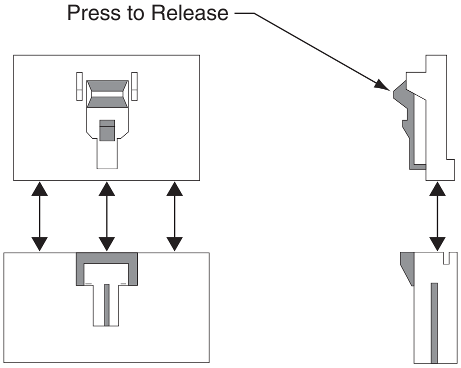


Figure 4

8. Carefully slide the main circuit board out until the ribbon cable between the camera assembly and J2 on the main circuit board is accessible. First, disconnect the J5 connector from the main board. To remove, depress the retaining clip on the J5 connector and pull upwards. See "2" on figure 5 below. Next, remove the ribbon cable from J2 by gently pulling up on this cable, being careful not to pull down as damage may occur to the camera assembly. See "3" on figure 5 below.

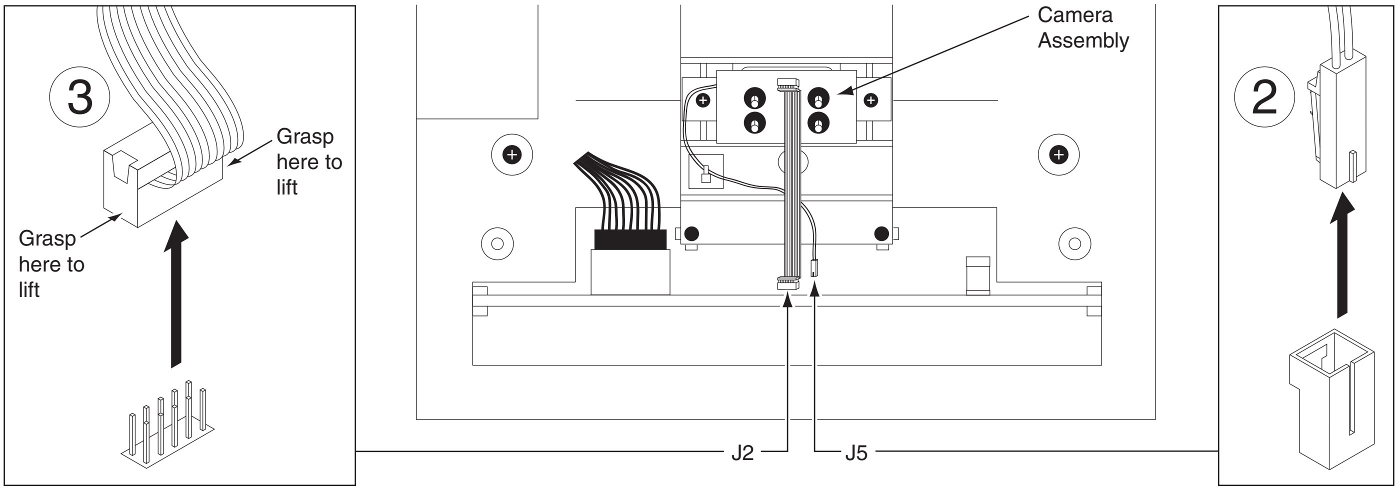


Figure 5

9. Carefully remove the main circuit board by sliding it free from the chassis.

10. Align the Ethernet adapter and carefully press the Ethernet card into place. Install the washers and nuts to secure the adapter. See figure 6 below.

⚠ **CAUTION: Torque the 4-40 nuts to 4.5 – 5.5 in. lbs. (.51 - .62 Nm). Excessive torque may damage the circuit boards. After installing the Ethernet card, inspect for warped Ethernet or main PCBs.**

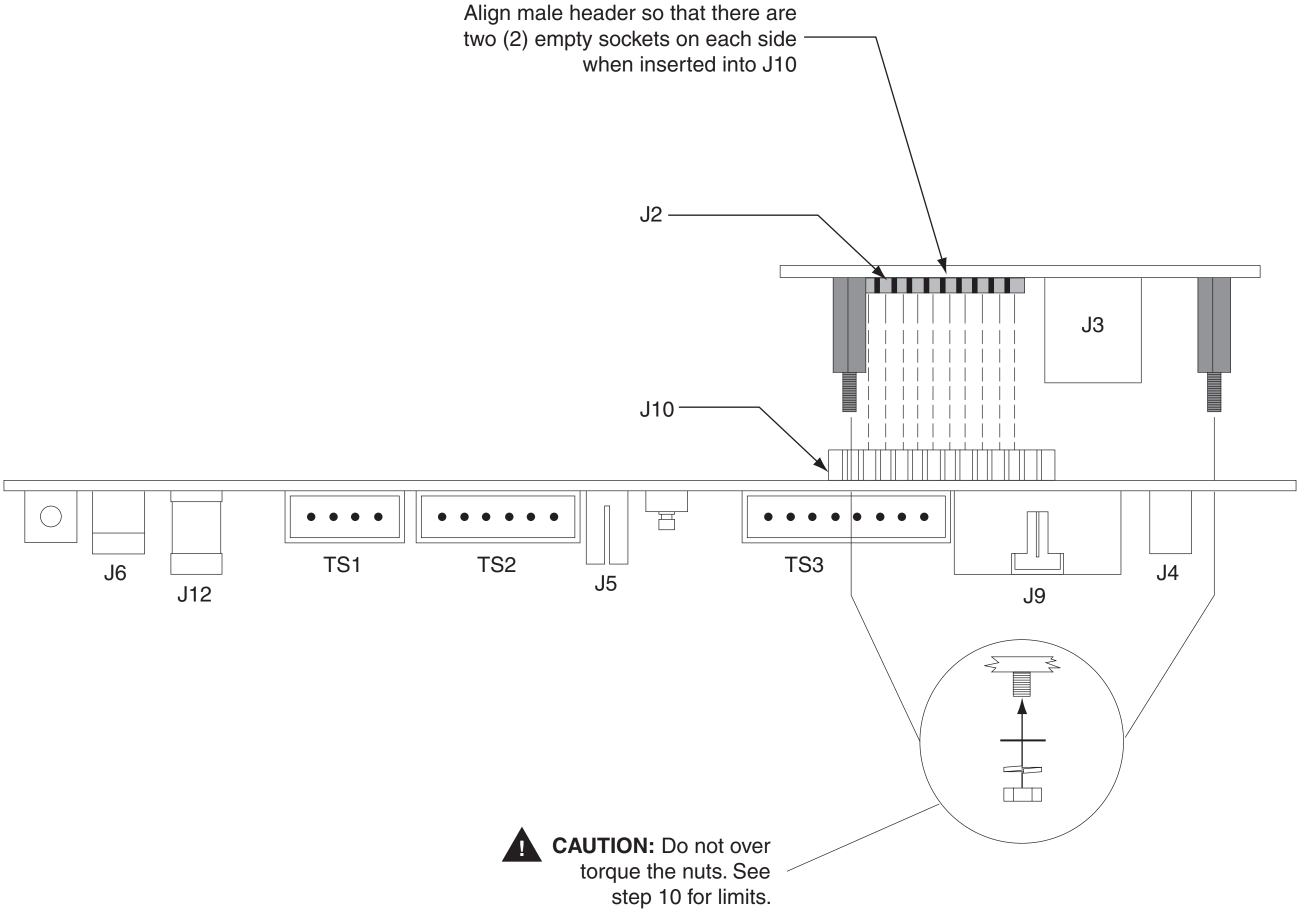

Align male header so that there are two (2) empty sockets on each side when inserted into J10
J2
J3
J10
J6
J12
TS1
TS2
J5
TS3
J9
J4
⚠ **CAUTION:** Do not over torque the nuts. See step 10 for limits.

Figure 6

11. Carefully slide the main circuit board back into the chassis using the guides to align the board correctly. Leave the main circuit board out about 1".

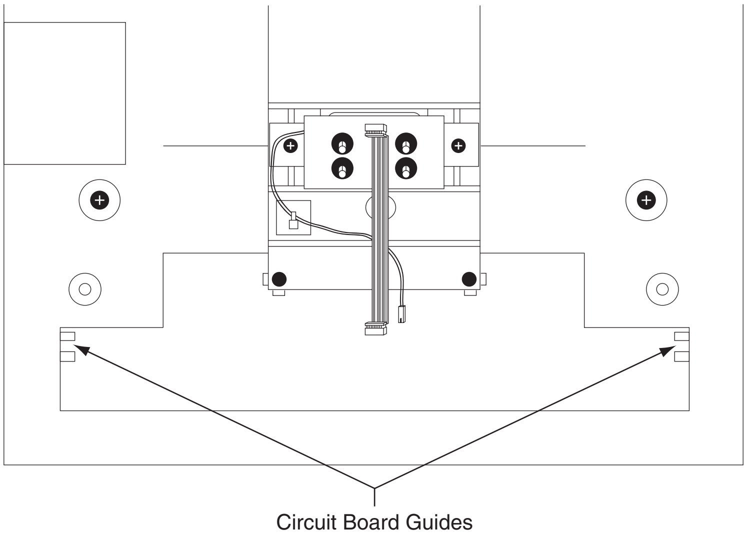


Figure 7

12. Attach the camera cable to J2 on the main circuit board. Take care to align the connector to the pins on the main circuit board and do not twist the cable, as this will damage the camera.

13. Plug in the J5 connector.

14. Locate the cable that runs from the top panel circuit board to the main circuit board. Connect this cable to J9 on the main circuit board. See figure 8 for cable routing.

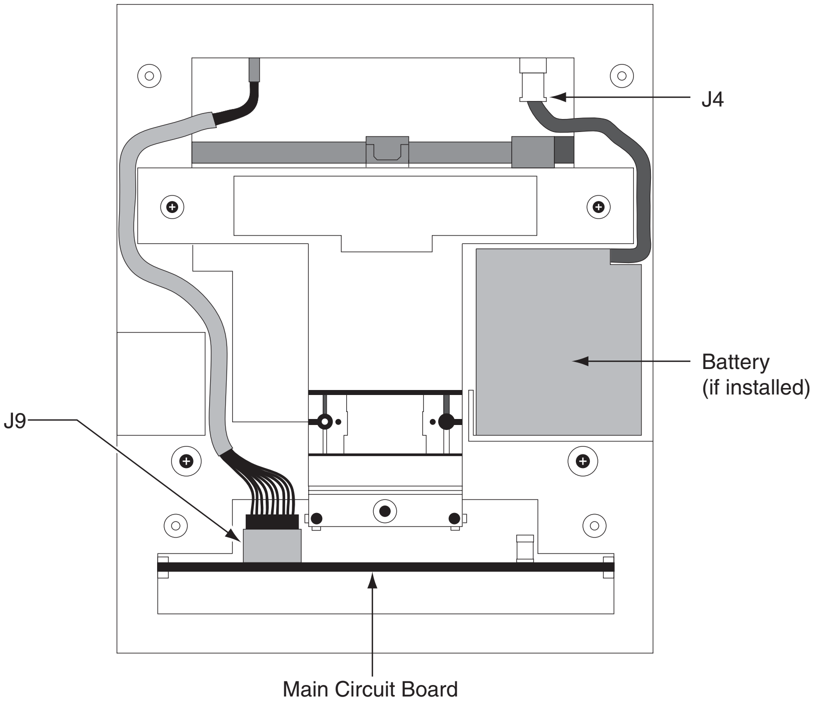


Figure 8

15. Slide the main circuit board in the rest of the way.

16. Replace the back plate. Attach the grounding screw to the main circuit board using the lower right hole on the back plate. If a ground lug is present, do not allow it to come into contact with J7. Secure the back plate with the four screws removed in step 5.

17. Line up the slots at the bottom of the reader's back with the four hinge pins at the bottom of the wall mount. Slide the reader to the left so the pins go in the slots. This fastens the reader to the wall and wall mount and forms a hinge.

18. Reconnect all external connections removed in step 3.

19. Hold down reset button and apply power. Once the reader has booted up, release the reset button.

20. Press "9" on the keypad to complete the reset when prompted.

21. Reconnect the J7 jumper (if applicable).

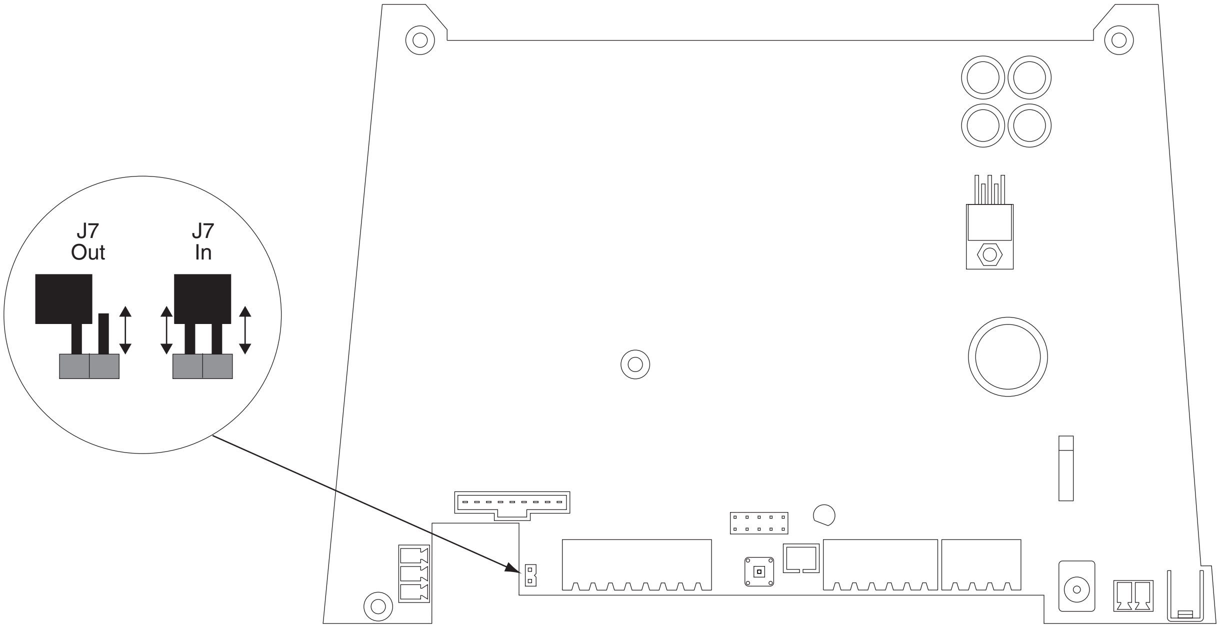


Figure 9

22. Secure the unit to wall mount with key. Upgrade is completed.

What do the LEDs on the Ethernet adapter mean?

1. Steady red or yellow LED:
   - This means the Ethernet adapter has finished booting up but has not tried to detect a network cable plugged in.
2. Red or yellow flashing:
   - This means the Ethernet cable is not plugged in or no network is detected.
3. Red or yellow and green LEDs are both flashing:
   - This means the Ethernet cable has been detected but IP address entered at the reader has not been sent to the Ethernet adapter yet. This status is normally not seen as this process happens quickly.
4. Steady green:
   - This means communication with the network has been established but the host program has not contacted the Ethernet adapter yet.
5. Green flashing:
   - This means everything is ready and messaging can occur when initiated by the host program.

(877) 671-7011
Printed in Country

70200-0013

F Series HandPunch Modem

Installation Instructions

Periodically, enhancements to the HandKey or HandPunch are introduced that offer added functionality and performance. Should it be necessary to incorporate the enhancements into the F Series circuit board (HP-2000, HP-3000, HP-4000, HK-2 and HK-CR), use the following procedures.

⚠ **CAUTION: This procedure requires erasing the existing hand templates. Save the existing hand templates before proceeding.**

1. Unlock the reader and rotate.
2. Disconnect the power supply from the board.
3. Remove and tag all external connections to make correct re-attachment.

⚠ **CAUTION: If the unit is equipped with an optional battery backup, remove the J7 jumper before proceeding. See figure 9.**

4. Remove HandReader from wall by sliding it to the right, away from the wall mount. See figure 1 below.

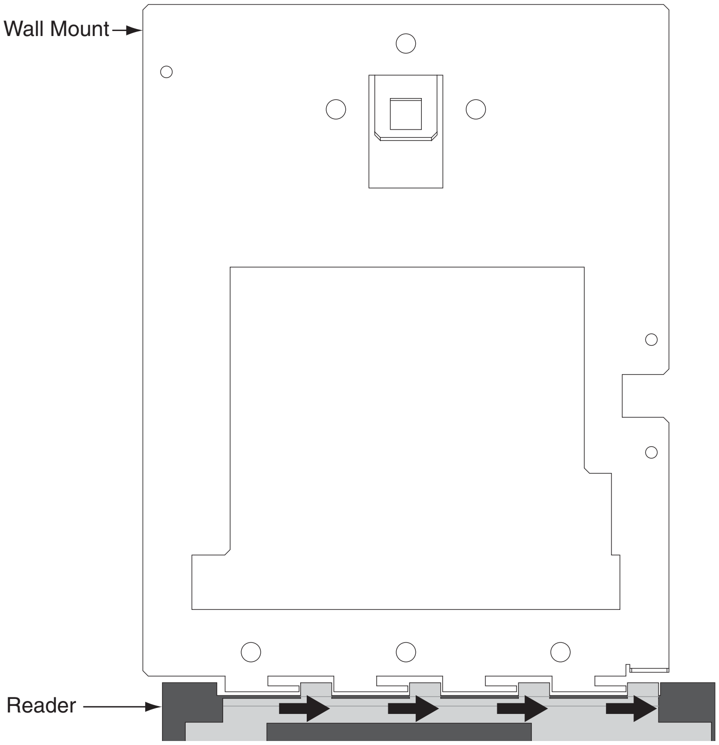


Figure 1

5. Set the reader on a firm surface such as a table. Remove the four screws that secure the back plate to the HandReader. Remove the grounding screw and/or ground lug (if present). See figure 2 below.

⚠ CAUTION: Before removing back plate of reader, wear a grounding wrist strap to help aid in protecting the circuit board from any ESD damage that might occur from improper handling.

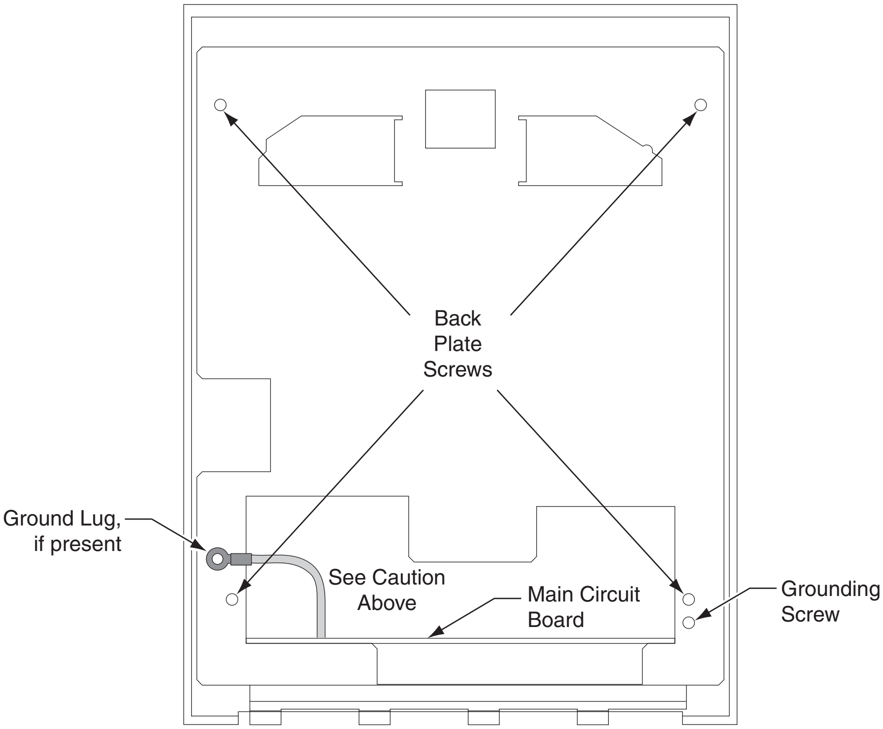


Figure 2

6. Remove the back plate.

7. Locate the cable that runs from the top panel circuit board to the main circuit board. Disconnect this cable from J9 on the main circuit board. See "1" on figure 3. To remove the J9 connector on the main circuit board (lower board), depress the retaining clip on the connector and pull upwards. See figure 4 below.

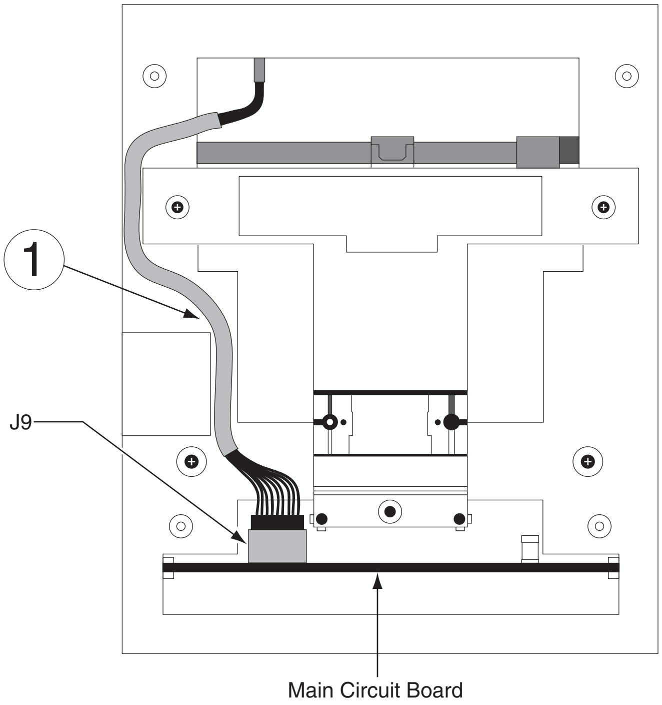


Figure 3

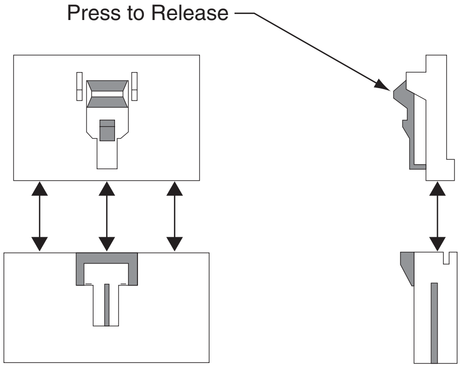


Figure 4

8. Carefully slide the main circuit board out until the ribbon cable between the camera assembly and J2 on the main circuit board is accessible. First, disconnect the J5 connector from the main board. To remove, depress the retaining clip on the J5 connector and pull upwards. See “2” on figure 5 below. Next, remove the ribbon cable from J2 by gently pulling up on this cable, being careful not to pull down as damage may occur to the camera assembly. See “3” on figure 5 below.

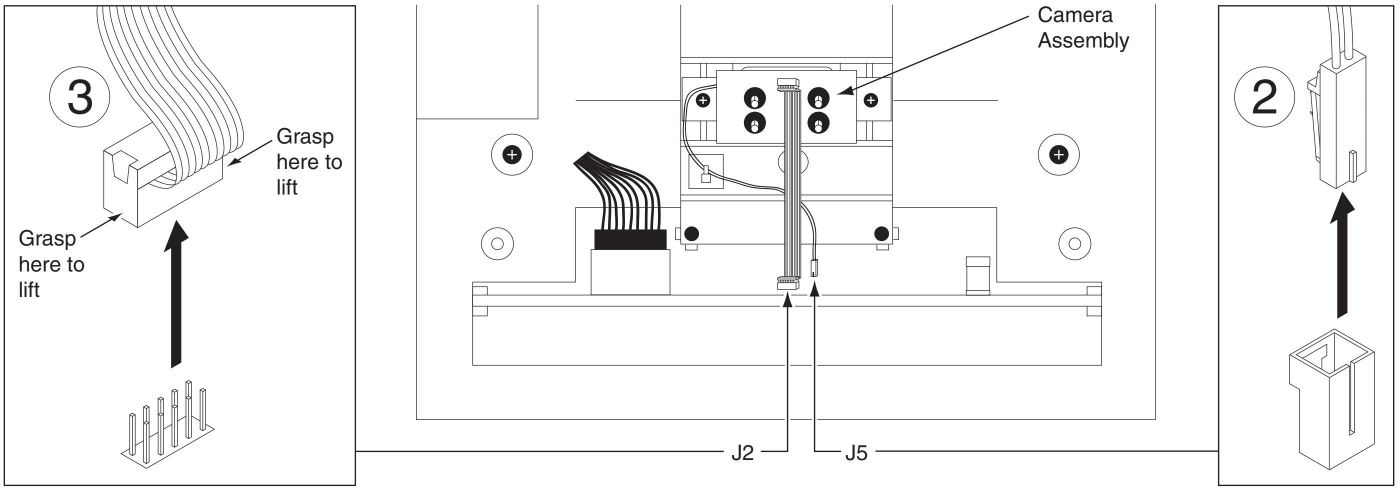


Figure 5

9. Carefully remove the main circuit board by sliding it free from the chassis.

10. Install the modem PCB onto the main PCB. See figures 6 and 7 below.
    a. Align P1 on the modem PCB with J10 on the underside of the main PCB.
    b. Insert the P1 pins into the J10 socket. If done correctly, the two standoffs on the modem PCB should insert through the mounting holes in the main PCB.
    c. Turn the PCB's over so that the main circuit board is on top of the modem PCB. Secure the modem PCB to the main PCB by adding the provided flat washers, split washers, and nuts onto the standoff(s). Tighten the nuts using a $^3/_{16}$" nut driver.

⚠ **CAUTION: Torque the 4-40 nuts to 4.5 – 5.5 in. lbs. (.51 -.62 Nm). Excessive torque may damage the circuit boards. After installing the modem, inspect for warped modem PCB or main PCB.**

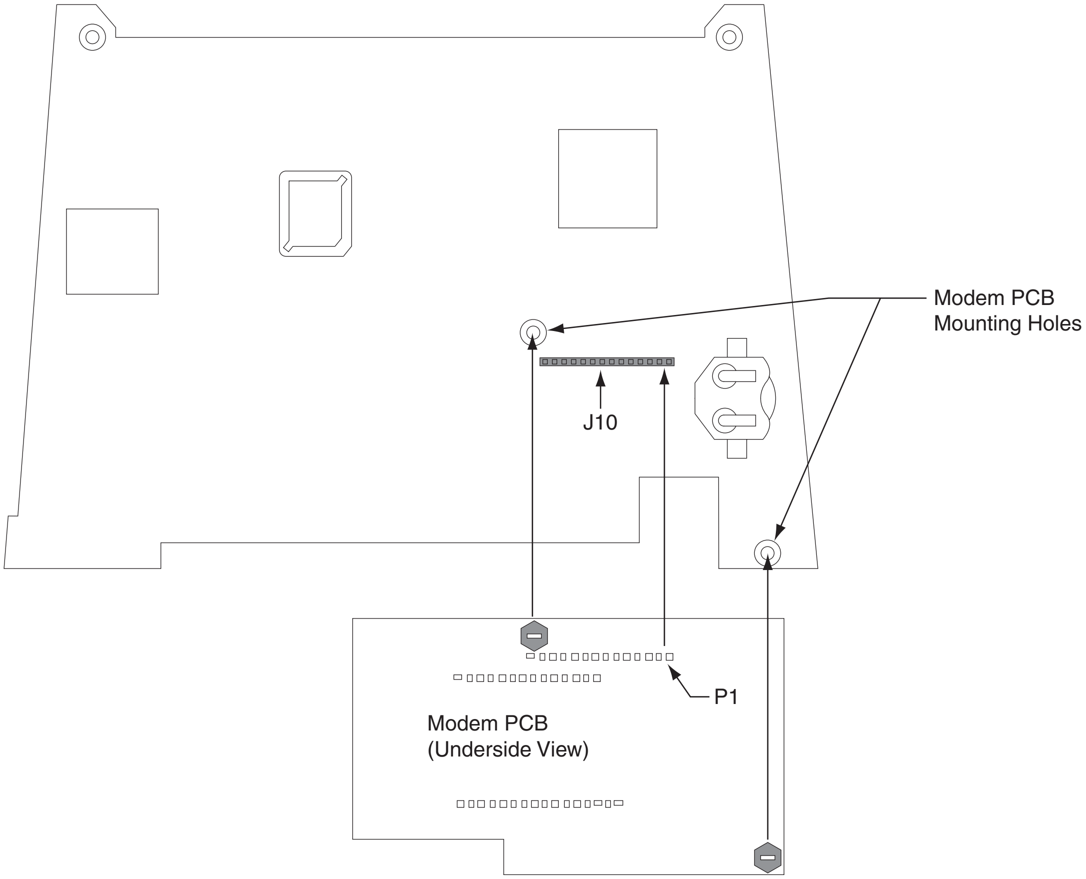
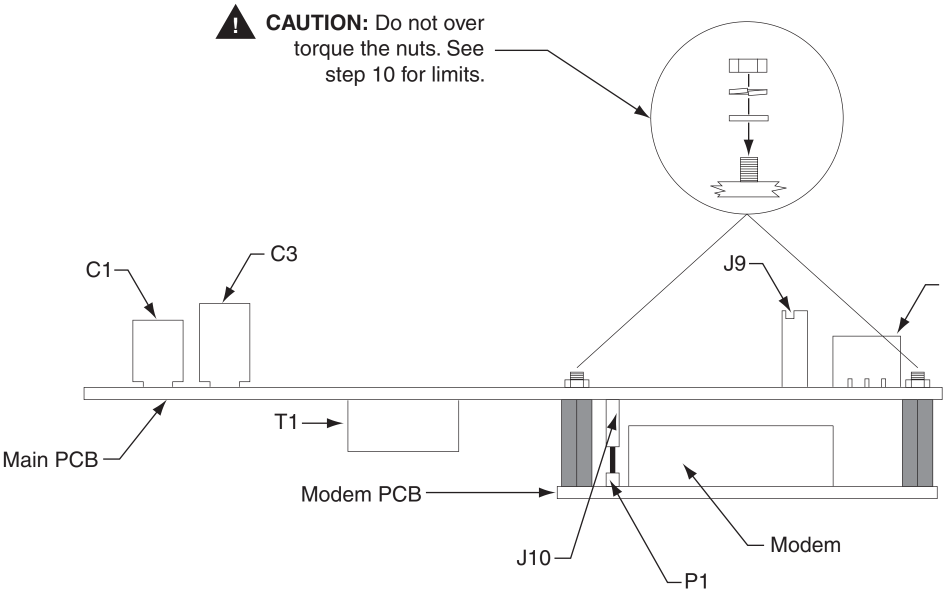


Figure 6



⚠ **CAUTION:** Do not over torque the nuts. See step 10 for limits.

Side View

Figure 7

11. Carefully slide circuit board back into the chassis using the circuit board guides to locate the circuit board correctly. See figure 8 below.

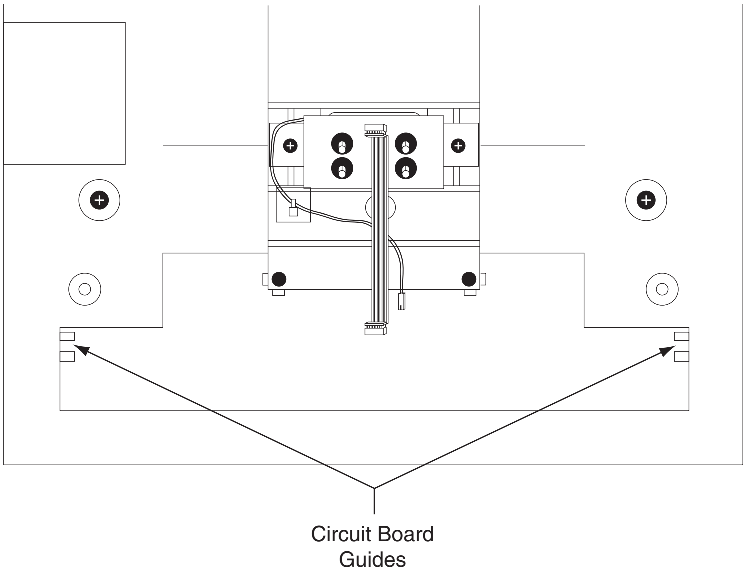


Figure 8

12. Being careful to align all pins, attach the camera cable to J2 on the main circuit board.
13. Plug in the J5 connector.

14. Locate the cable that runs from the top panel circuit board to the main circuit board. Connect this cable to J9 on the main circuit board. See figure 10 for cable routing.

15. If not already removed, remove the J7 jumper from the main PCB. See figure 9 below.

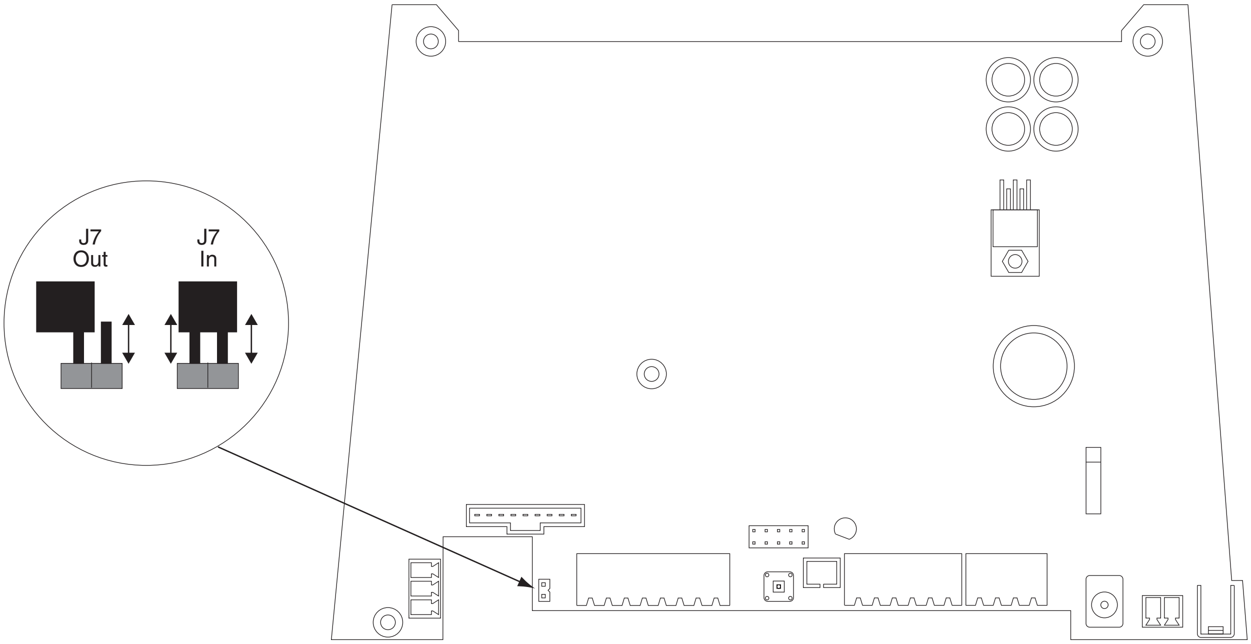


Figure 9

⚠ CAUTION: If there is a ground strap on the main board, do not allow the ground strap to touch the J7 jumper. Failure to do so will cause permanent damage to the main circuit board and will not be considered a warranty repair.

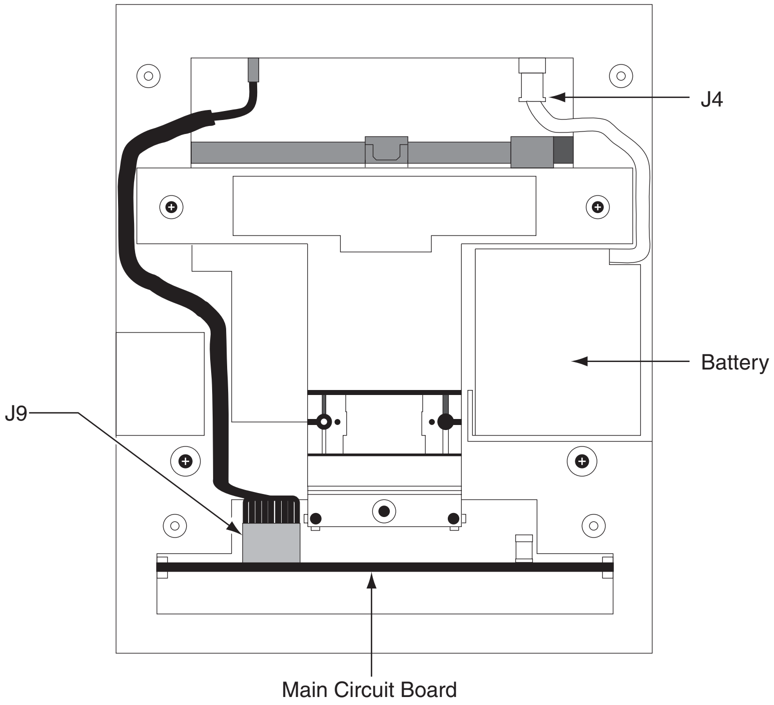


Figure 10

16. Reinstall the back plate onto the chassis. Reinstall grounding screw and/or ground lug. If a ground lug is present, do not allow it to come into contact with J7.
17. Secure the back plate with the four screws removed in step 5.
18. Line up the slots at the bottom of the reader's back with the four hinge pins at the bottom of the wall mount. Slide the reader to the left so the pins go in the slots. This fastens the reader to the wall and wall mount and forms a hinge.
19. Reconnect all external connections removed in step 3.
20. Power up the unit and reinstall the J7 jumper (if applicable).
21. Secure unit to wall mount with key. Upgrade is completed.

Ingersoll Rand
Security Technologies
(877) 671-7011
Printed in Country

70100-6101

Outdoor Reader

Installation Instructions

TABLE OF CONTENTS

OUTDOOR READER INSTALLATION

About the Outdoor Reader

The outdoor reader unit has two separate components:

- The case (called the *weather shield*) protects the reader from bad weather.
- The *HandReader* is able to function in much colder weather than regular readers when ordered with an internal heater (INT-HTR).

How the HandReader and internal heater work

In cold weather, when one places a hand on the HandReader, a mist forms around the hand. This distorts the image so the reader doesn't recognize the hand. To prevent this problem, the HandReader can be ordered with an internal heater. To accommodate the heater in the platen, the HandReader uses a 24 VDC, 2 amp power supply; this is different from the power supply for indoor readers.

UL Disclaimer

The reader is UL approved for indoor use only.

INSTALLATION INSTRUCTIONS

Before you start the installation

Before you start installing the reader and weather shield, pick an appropriate location for the reader. (See the reader manual for more information about where to locate the reader in relation to the door.)

Also make sure that you are familiar with local building codes that affect this installation and that you have the appropriate tools and fasteners.

Tools you will need for the installation

a. To install the reader, you need:

- A level
- A measuring tape
- A Phillips screwdriver
- A drill with ¼ and ½ inch bits

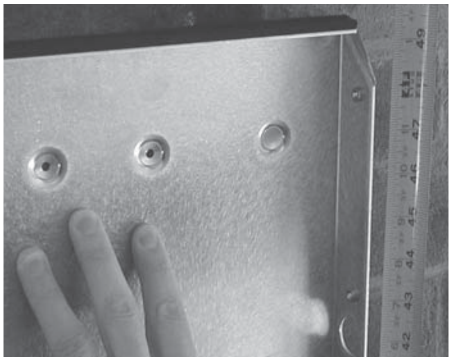
b. Materials you must provide

- wiring raceways approved by local code
- the appropriate fasteners to secure the reader to the wall

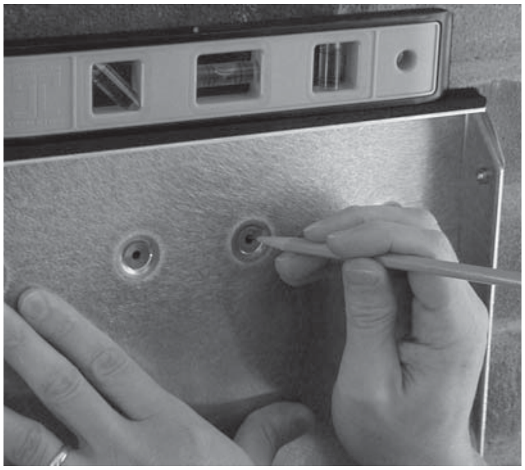
Installing the weather shield's back panel and wall mount

1. Hold the weather shield's back panel against the wall so the top of it is 49.5 inches (126 cm) from the floor or ground.

   When the installation is done, this will put the reader platen 40 inches (roughly 102 cm) from the ground.



2. Make sure the top of the back panel is level.
3. Mark the location of the five screw holes (two on the top and three on the bottom). Also mark the location of the wiring hole if you plan to run the wiring straight through the wall.

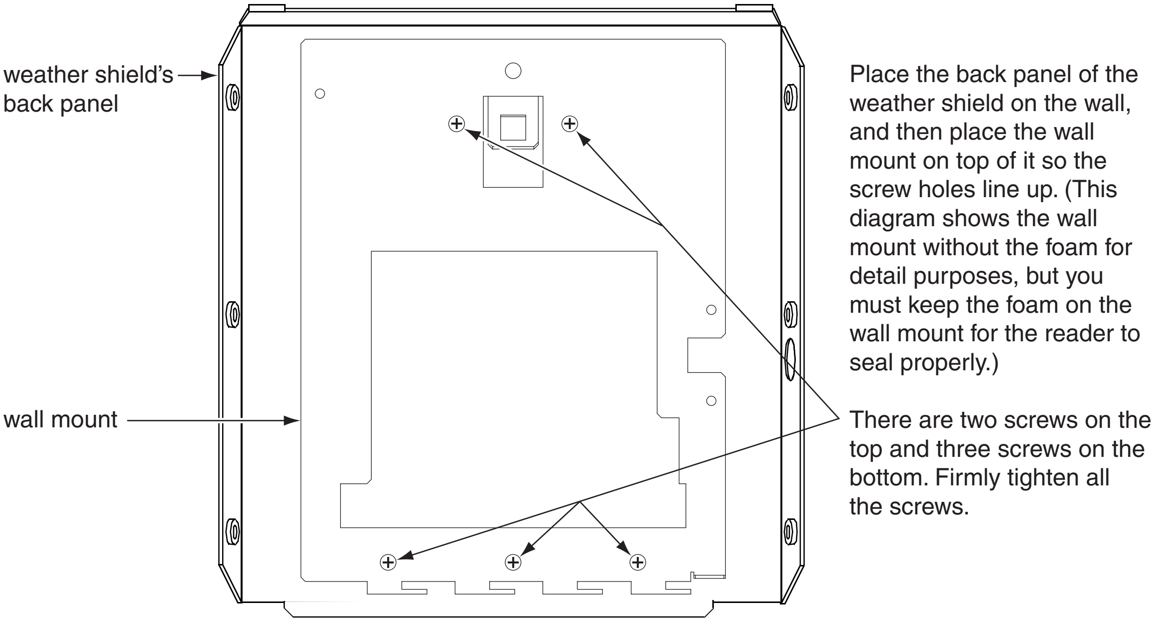


4. If needed, drill holes for each of the holes that you marked.

The size of the holes and the method you use to fasten the weather shield's back panel and wall mount to the wall depends on the type of wall, on the fasteners you have, and on any local building code requirements.

- **For wooden walls:** You may need to drill pilot holes for your screws so you don't split the wood.
- **For hollow walls:** You will probably want to use toggle bolts or some similar type of fastener designed for hollow walls. The size of the holes you need depends on the fastener.
- **For a solid wall (e.g., brick or masonry):** It's most common to use ¼ inch expansion anchors. Drill ¼ inch diameter holes that are ¼ inch deeper than the anchors.

5. Screw the weather shield's back panel and the wall mount to the wall.



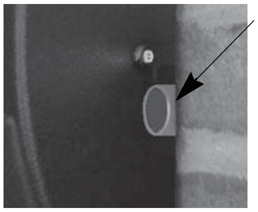
Place the back panel of the weather shield on the wall, and then place the wall mount on top of it so the screw holes line up. (This diagram shows the wall mount without the foam for detail purposes, but you must keep the foam on the wall mount for the reader to seal properly.)

There are two screws on the top and three screws on the bottom. Firmly tighten all the screws.

6. If you will use surface conduit to bring the wiring to the reader, notch the side of the weather shield and reader at the appropriate places. (Skip this step if your wiring will come straight through the wall.)

   To find the location for the hole in the weather shield, put the case on the back panel and mark the location of the conduit hole on the right side of the weather shield's back panel.

   The location for the hole is already marked on the reader (on the left side if you are looking at it from the back).



Make a notch in the side of the case so it lines up with the hole for the conduit in the side of the weather shield's back panel.

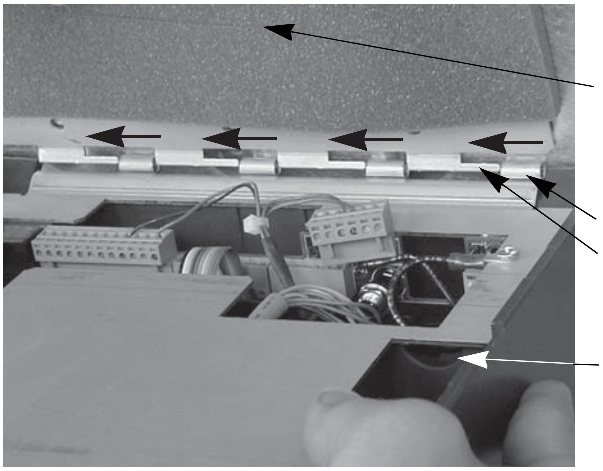
Running the wiring

7. Run the wiring for the reader, but don't connect the wires to the green terminal connectors yet.

- Make sure that you follow all local electrical codes in bringing the wiring to the reader.
- See the reader manual for wiring instructions.
- See step 9 before you connect the green terminal connectors.
- Make sure that you use an appropriate power supply. The HandReader with heated platen uses a 24 VDC, 2 amp power supply rather than the 12± volt power supply that regular readers use.

Mounting the reader

8. Line up the slots at the bottom of the reader's back with the four hinge pins at the bottom of the wall mount. Slide the reader to the left so the pins go in the slots. This fastens the reader to the wall and wall mount and forms a hinge.



Wiring that comes through the wall passes through this slit.

These slots slide over these pins, fastening the reader to the wall mount and forming a hinge.

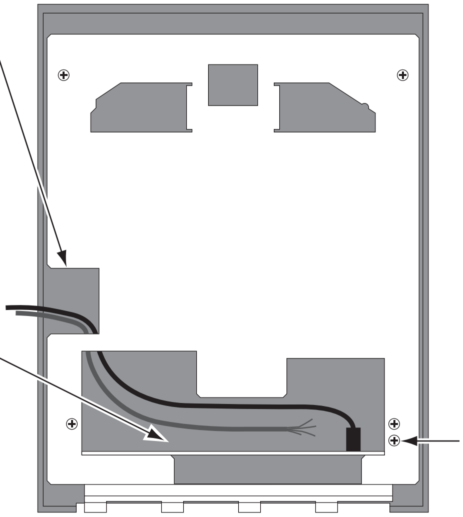
If using surface conduit, all wiring must pass through this hole (see step 9).

9. Connect the wiring and power to the reader.

   If you are using surface conduit: *Make sure all the wires pass through this hole in the reader before you connect the wires to the green terminal connectors. The green terminal connectors won't fit through this hole, and the wires must pass through this hole so they don't get pinched when you close the case.*

   If the wiring will come through the back of the reader: *The wires enter directly into the wiring area through the slit in the black foam. This is the easiest way to do the wiring.*

   See the reader manual for instructions on which wires must connect to which terminal pins.



Grounding Screw

10. Put the key in the lock on the side of the reader, turn the key clockwise, close the reader, and then turn the key counterclockwise to lock the reader.

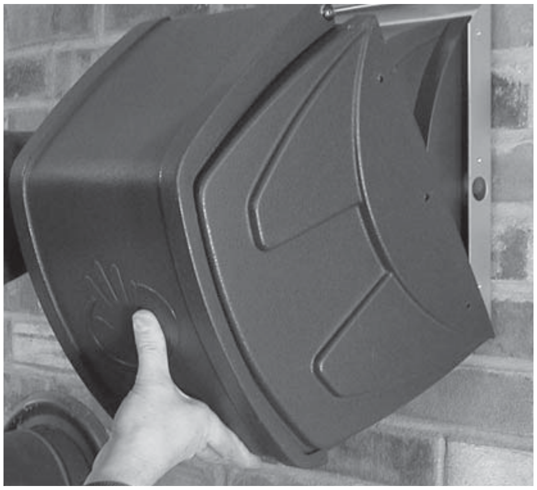
    Don't try to shut the reader without using the key; this will bend the locking mechanism.

11. Test the reader to make sure it is wired and communicating correctly.

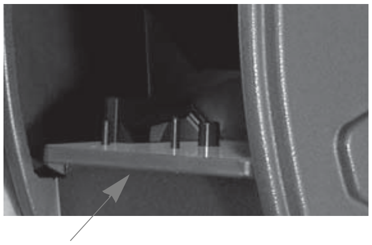
    Do this prior to installing the weather shield; you can't open the reader back up to adjust wiring or connections with the weather shield in place.

Mounting the weather shield over the reader

12. Place the weather shield over the reader. You must place the bottom of the case on first and then push in the top.

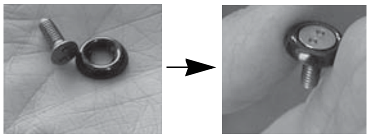


The bottom of the case must go on first so the lip at the bottom of the opening slips under the platen rather than sliding in front of it.



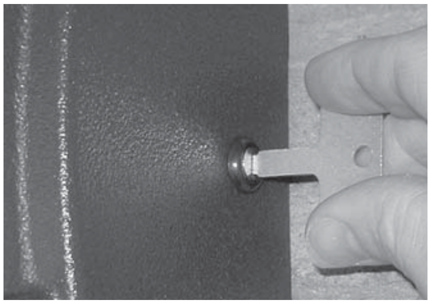
Make sure the lip at the bottom of the opening in the weather shield slips under the platen.

13. Put a washer on each of the six screws.



14. Use the tool with two small prongs on the end to insert the screws that hold the weather shield onto the weather shield’s back plate.

    This tool provided with the reader may be slightly different than the key shown in this picture.



15. If needed, use the RTV sealant we provided to seal any places on the top or sides where water might get behind the weather shield.

    The black pad on the back side of the weather shield’s back panel adequately seals the back on a flat wall, but on brick, clapboards, or other surfaces that aren’t flat, use the sealant to fill any gaps.

    Do NOT caulk the bottom of the case! In cool damp weather, moisture can condense inside the weather shield. Leaving the bottom uncaulked lets any water droplets that form run out instead of collecting inside the case.

Technical Note

Product	HandNet for Windows
Date	May 22, 2014
Subject	Microsoft Windows Compatibility

HandNet for Windows, Microsoft Windows Compatibility

Hand Net for Windows has been tested with the following operating systems:

- Windows XP Professional Service Pack 2
- Windows XP Professional Service Pack 3
- Windows Vista Business Service Pack 1
- Windows 7 Pro Compatible 32 Bit
- Windows 7 Pro Compatible 64 Bit

All basic functionality was tested and performs as expected.

The only exceptions that users may experience when running on one of the mentioned operating systems are noted below.

Windows Vista

1) The Activity Report may fail to generate and or display an error to the effect of “This function is already being run.” Specifically this may occur immediately after install. The recommended course of action is to reboot the machine, and the activity report should be generated correctly without error.
Windows XP

1) An error may occur when there are multiple user accounts on the PC. A user may encounter a HandNet for Windows error stating, “Cannot open SQL Server.” This may happen when HandNet for Windows was installed under User #1’s login on the PC, and then User #2 logs into the same PC and runs HandNet for Windows, logs in, and tries to generate a report. It is possible that this may be attributed to User #2 not having full administrative rights to the folder that HandNet for Windows is installed in. In order to prevent the error, the user should verify that he/she has full administrative rights on the machine and or should have HandNet for Windows installed under his account.

If more errors are encountered, we will make addendums or additions to this technical note.

For additional information, please contact Customer Care at 877-671-7011.

70200-0028

F Series HandPunch Top Panel Assembly Replacement

Installation Instructions

The following instructions apply to all F Series HandReader versions.

⚠ CAUTION: **The circuit boards within the HandReader are ESD sensitive. Observe proper ESD precautions when handling the unit.**

⚠ CAUTION: **This procedure requires erasing the existing hand templates. Save the existing hand templates before proceeding.**

1. Unlock the HandReader and rotate. See figure 6 on the last page of this instruction.

⚠ CAUTION: **If the unit is equipped with the optional battery backup, remove the J7 jumper before proceeding. See figure 2 on the next page for location of J7.**

2. Disconnect the power supply from the board.
3. Remove and tag all external connections to make correct re-attachment.

4. Remove HandReader from wall by sliding it to the right, away from the wall mount. See figure 1 below.

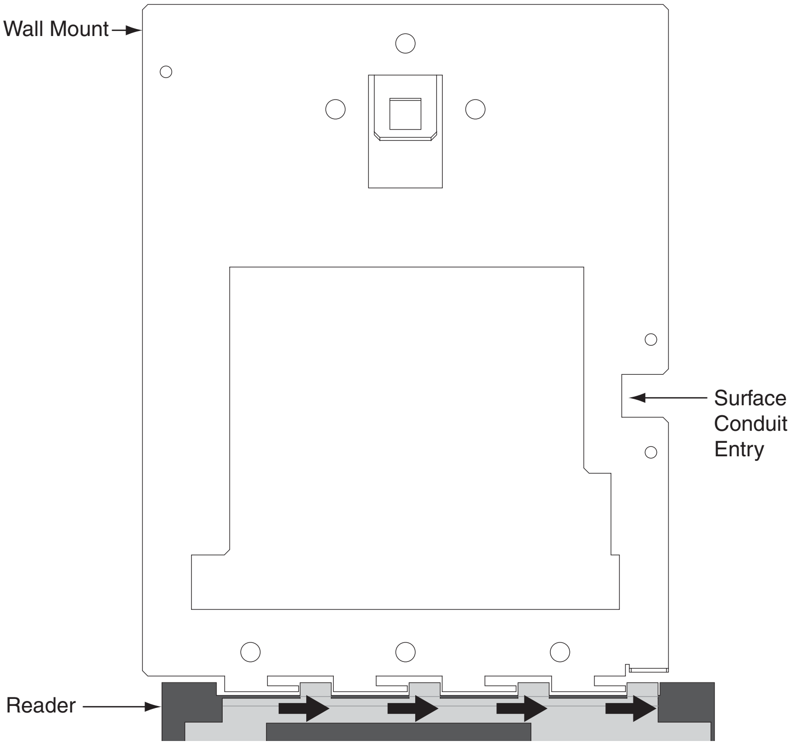


Figure 1

⚠ CAUTION: Before removing back plate of reader, wear a grounding wrist strap to help aid in protecting the circuit board from any ESD damage that might occur from improper handling.

5. Set the reader on a firm surface such as a table. Remove the four screws that secure the back plate to the HandReader. Remove the grounding screw and/or ground lug (if present). See figure 2 below.

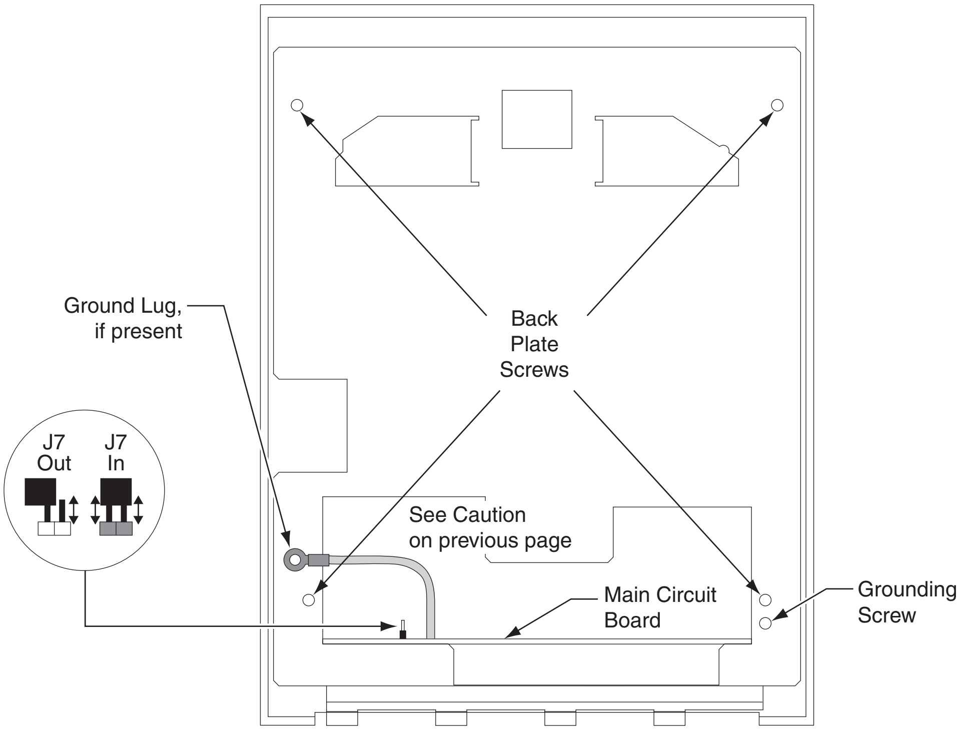


Figure 2

6. Locate the cable that runs from the top panel PCB to the main circuit board. Disconnect this cable from J3 on the top panel PCB. To remove the J3 connector on the top panel PCB, depress the retaining clip on the connector and pull downwards. If the optional battery backup is installed, disconnect the battery cable from J4 on the top panel PCB. See figures 3 and 4 below.

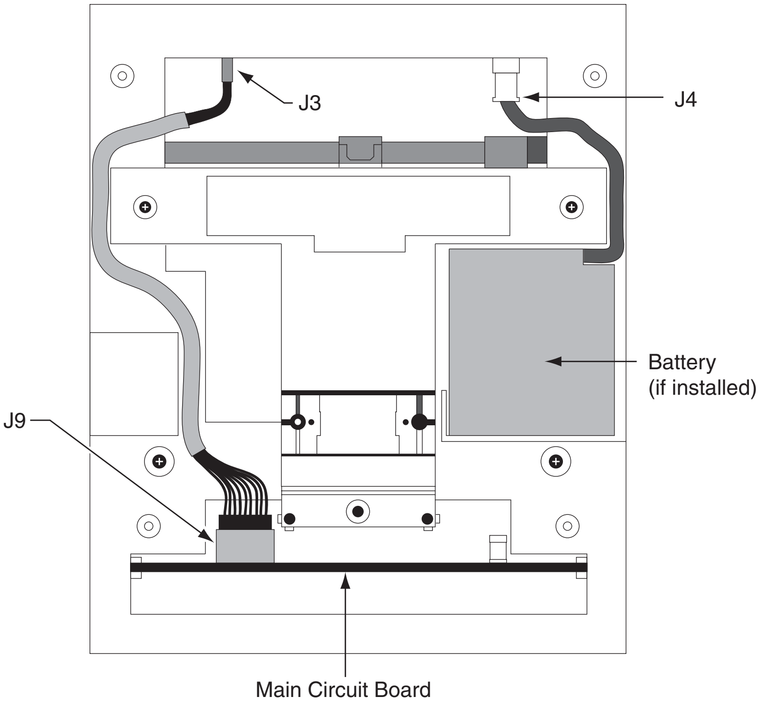


Figure 3

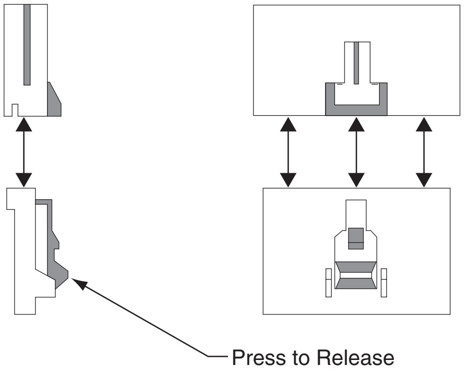


Figure 4

7. Remove the two screws that hold the top panel assembly to the front case. Carefully slide the top panel out from the front case. See figure 5 below.

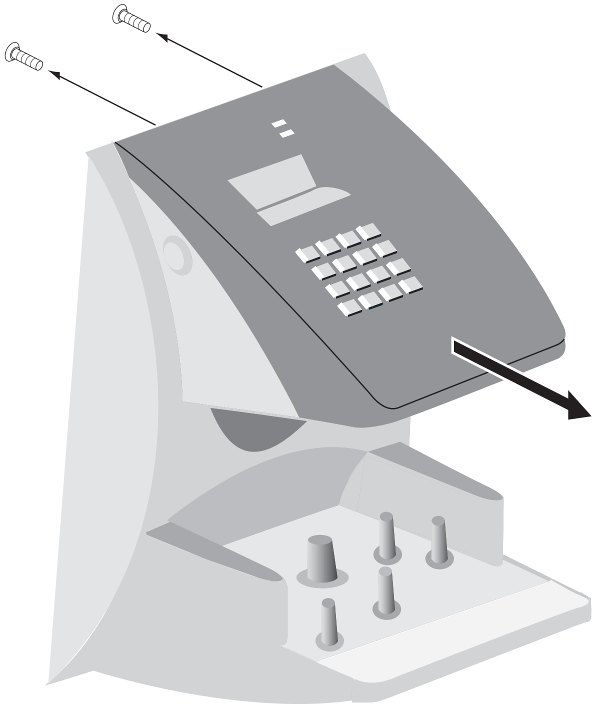


Figure 5

8. Carefully align and install the new top panel assembly. Secure with the two screws removed in step 7 above.

⚠ CAUTION: Torque the top panel screws to 3.8 – 4.4 in. lbs. (.43 - .49 Nm). Excessive torque may damage the screw bosses in the top panel.

9. Locate the cable that runs from the main circuit board to the top panel PCB. Route the cable as shown in figure 3. Re-insert the connector into J3 on the top panel PCB. Make sure the connector snaps into J3.

⚠ **CAUTION:** **If the battery backup option is installed, replace the J7 jumper. Be sure that both pins of J7 are shorted by the jumper. See figure 2. Re-connect the battery cable to J4 on the top panel PCB. See figures 3 and 4.**

10. Replace the back plate. Attach the grounding screw to the main circuit board using the lower right hole on the back plate. If a ground lug is present, do not allow it to come into contact with J7. Secure the back plate with the four screws removed in step 5.

⚠ **CAUTION:** **Torque the back plate screws to 3.8 – 4.4 in. lbs. (.43 - .49 Nm). Excessive torque may damage the screw bosses on the front case.**

11. To re-install the HandReader, reverse steps 1 – 4.

⚠ **CAUTION:** **Do not force the HandReader onto the wall mount when the latch is in the locked position.**

12. With the key in the unlocked position, rotate the HandReader back upright. Turn the key counter-clockwise to lock the HandReader into place. See figure 6 below.

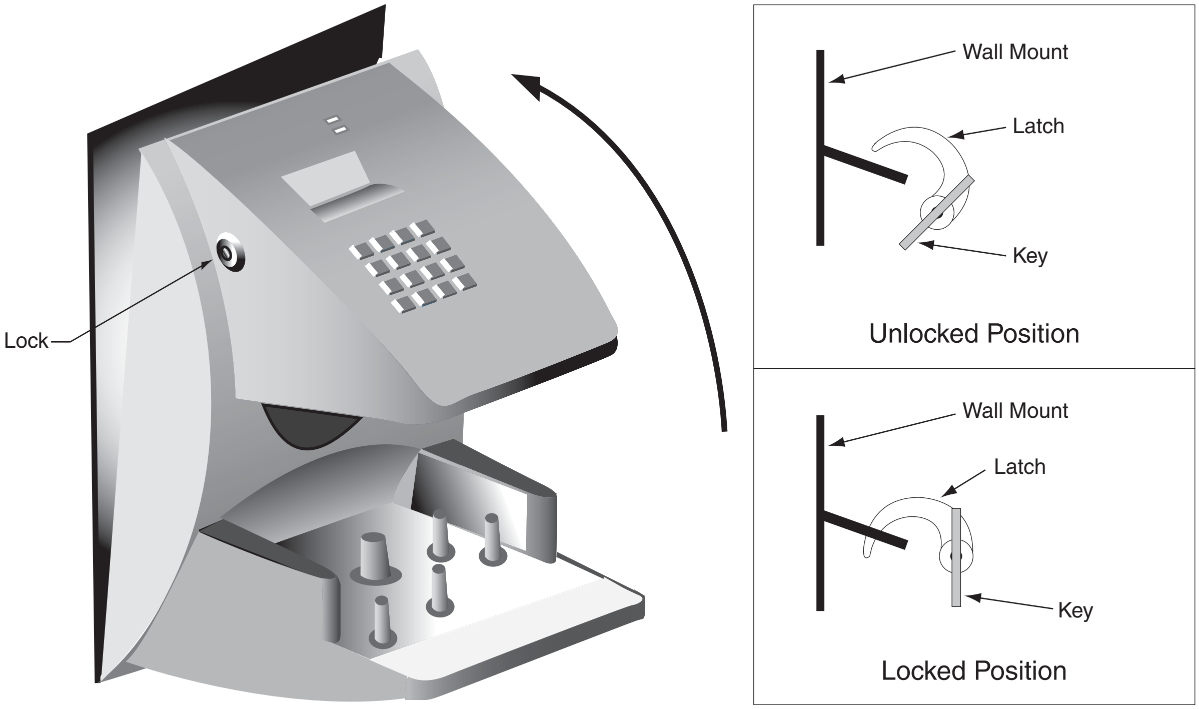


Figure 6

70200-0010

F Series Circuit Board Firmware Upgrade

Installation Instructions

Periodically, enhancements to the HandKey or HandPunch are introduced that offer added functionality and performance. Should it be necessary to incorporate the enhancements into the F Series circuit board (HP-2000, HP-3000, HP-4000, HK-2 and HK-CR), use the following procedures.

⚠ **CAUTION: This procedure requires erasing the existing hand templates. Save the existing hand templates before proceeding.**

1. Unlock the reader and rotate.

⚠ **CAUTION: If the unit is equipped with an optional battery backup, remove the J7 jumper before proceeding. Refer to figure 2 on the next page for location of J7.**

2. Disconnect the power supply from the board.
3. Remove and tag all external connections to make correct re-attachment.
4. Remove HandReader from wall by sliding it to the right, away from the wall mount. See figure 1 below.

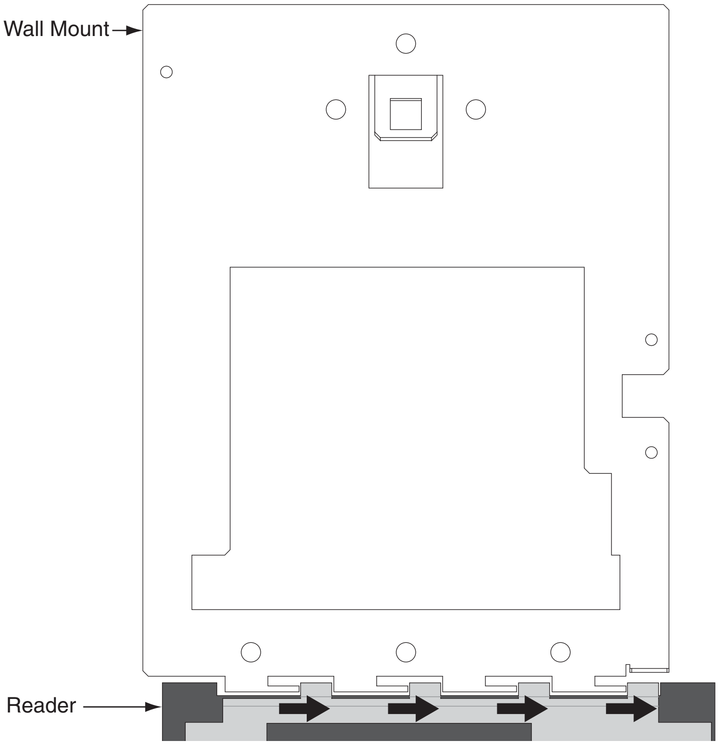


Figure 1

⚠ **CAUTION: Before removing back plate of reader, wear a grounding wrist strap to help aid in protecting the circuit board from any ESD damage that might occur from improper handling.**

5. Set the reader on a firm surface such as a table. Remove the four screws that secure the back plate to the HandReader. Remove the grounding screw and/or ground lug (if present). See figure 2 on next page.

(877) 671-7011
Printed in Country

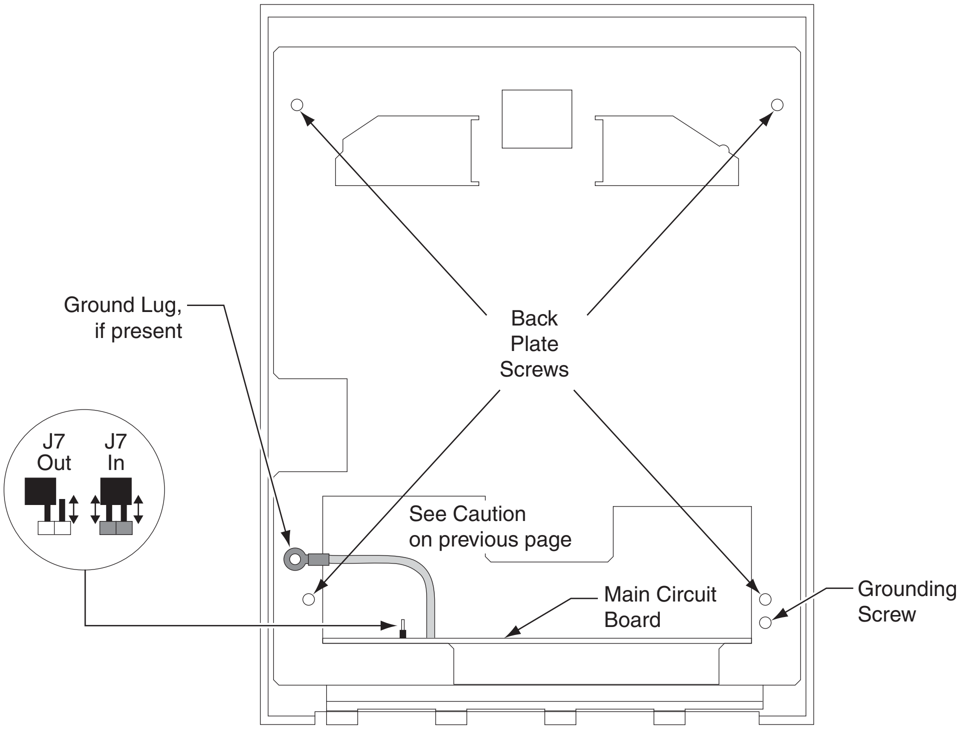


Figure 2

6. Remove the back plate.
7. Locate the cable that runs from the top panel circuit board to the main circuit board. Disconnect this cable from J9 on the main circuit board. See “1” on figure 3. To remove the J9 connector on the main circuit board (lower board), depress the retaining clip on the connector and pull upwards. See figure 4 below.

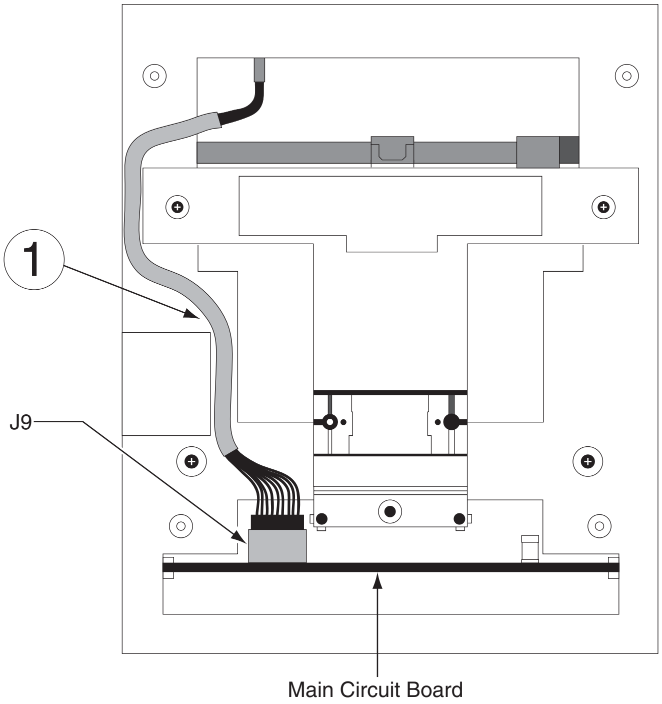


Figure 3

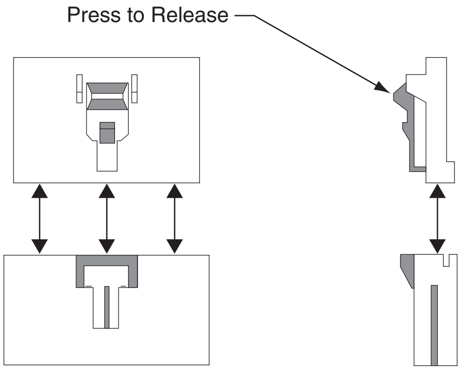


Figure 4

8. Carefully slide the main circuit board out until the ribbon cable between the camera assembly and J2 on the main circuit board is accessible. First, disconnect the J5 connector from the main board. To remove, depress the retaining clip on the J5 connector and pull upwards. See “2” on figure 5 on the following page. Next, remove the ribbon cable from J2 by gently pulling up on this cable, being careful not to pull down as damage may occur to the camera assembly. See “3” on figure 5 on the following page.

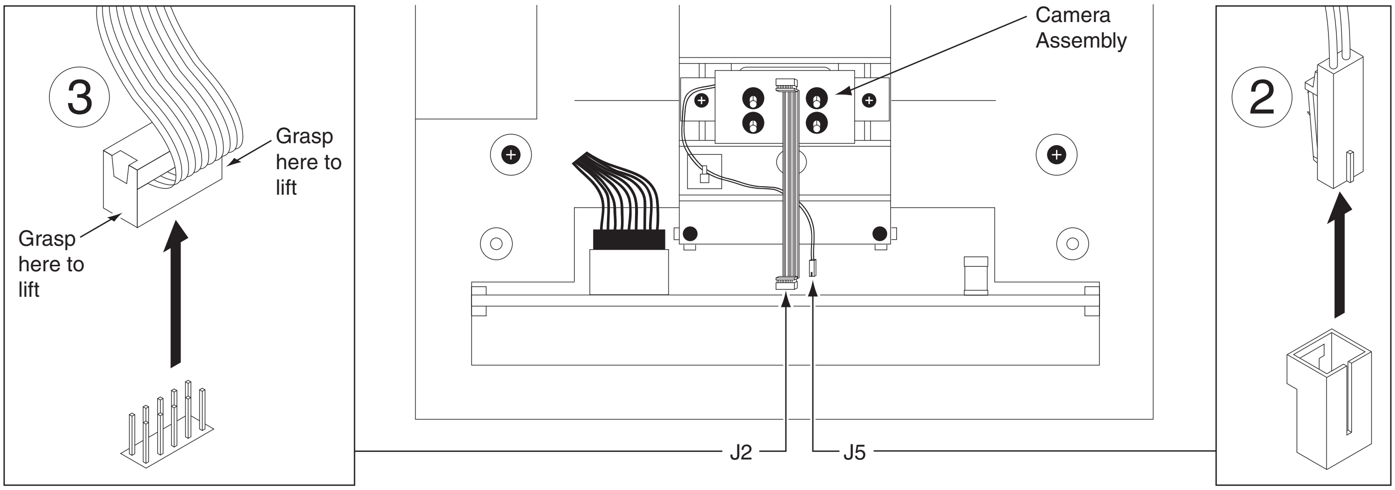


Figure 5

9. Carefully remove the main circuit board by sliding it free from the chassis.
10. On the bottom side of the board, locate the PROM socket labeled U24. Please take notice that there is a flat corner located in the lower right corner of the socket. This flat corner will align with a flat corner on the PROM. See figure 6 below.

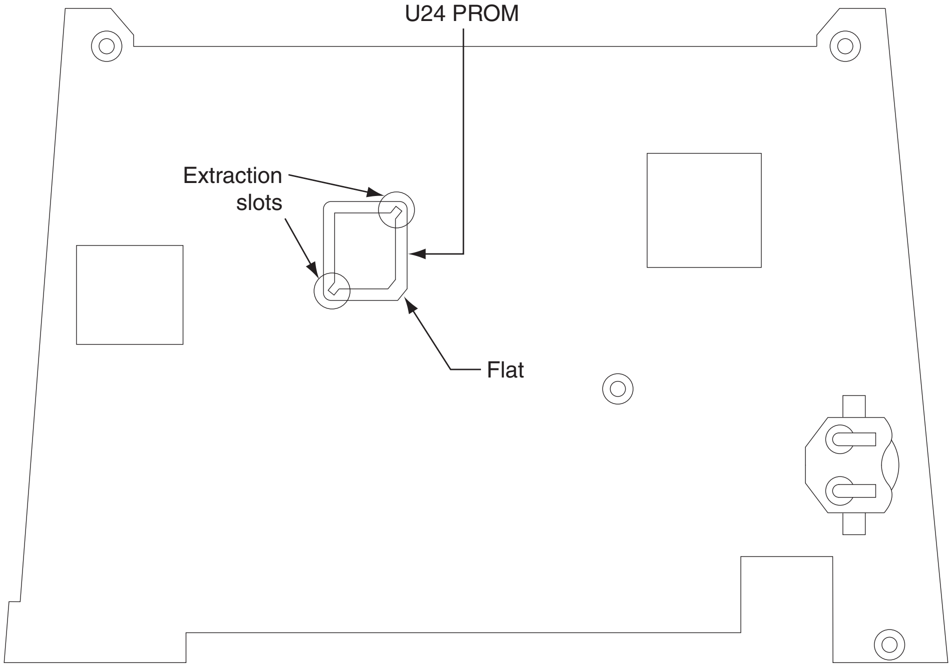


Figure 6

11. Remove the PROM currently installed in the U24 PROM socket using the steps below in conjunction with the provided PROM extraction tool.
    a. Insert the extraction tips into the extraction slots of the socket until the tool bottoms on the socket. See figure 7, drawing number 1 for details.
    b. Squeeze the tool handles until the PROM backs out of the socket. See figure 7, drawing number 2 for details.

⚠ CAUTION: Do NOT pull upward on the tool to loosen the PROM – slowly squeeze the tool handles while maintaining a slight downward force toward the socket.

    c. Remove the PROM and tool.
    d. Inspect the PROM socket and socket pins for any damage or misalignment.
    e. Store the original PROM in a safe location so it does not get confused with the new PROM.

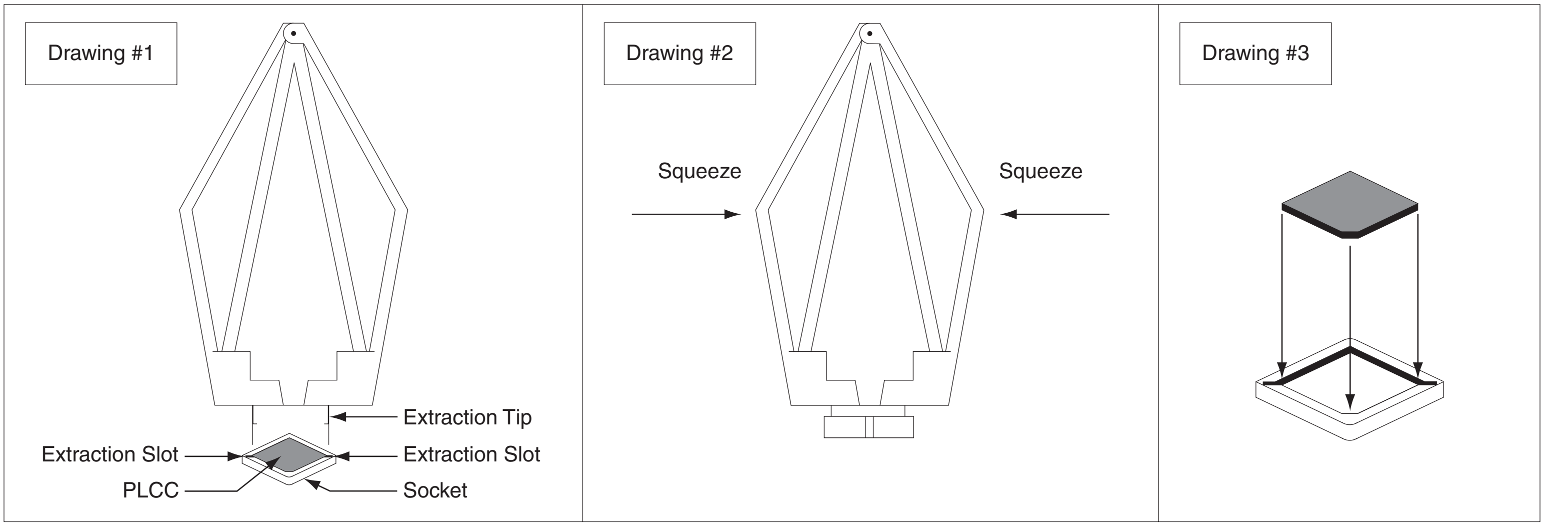


Figure 7

12. Install the new PROM in the U24 PROM socket using the steps below.
    a. Inspect the pins of the new PROM for bent or misaligned pins.
    b. Place the new PROM over the socket, aligning the flat corner of the PROM with the flat corner of the socket. See figure 7, drawing number 3 for details.
    c. Gently press the PROM down into the socket until it snaps into place.
    d. Inspect the PROM to insure that it has been fully seated in the socket.

Re-installing

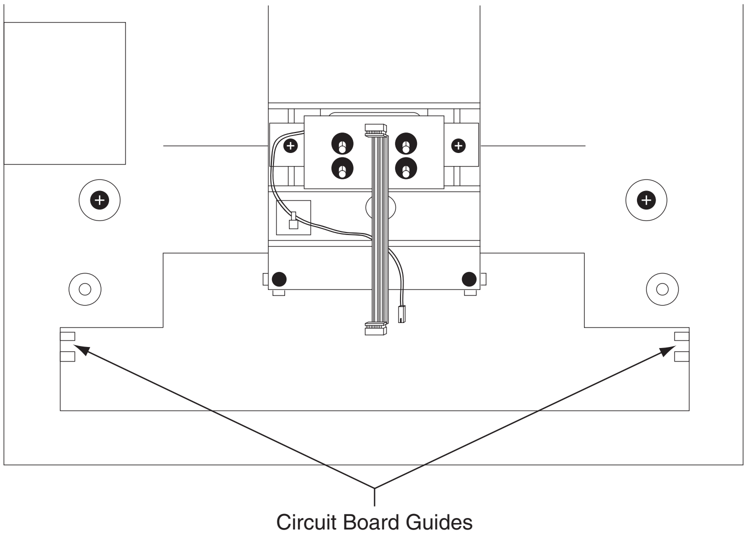


Figure 8

13. Being careful to align all pins, attach the camera cable to J2 on the main circuit board.
14. Plug in the J5 connector.
15. Locate the cable that runs from the top panel circuit board to the main circuit board. Connect this cable to J9 on the main circuit board. Make sure the connector snaps into J9.
16. Replace the back plate. Attach the grounding screw to the main circuit board using the lower right hole on the back plate. If a ground lug is present, do not allow it to come into contact with J7.
17. Secure the back plate with the four screws removed in step 5.
18. Line up the slots at the bottom of the reader’s back with the four hinge pins at the bottom of the wall mount. Slide the reader to the left so the pins go in the slots. This fastens the reader to the wall and wall mount and forms a hinge.
19. Reconnect all external connections removed in step 3.
20. Power up the unit and install J7 (if applicable).
21. Secure the unit to wall mount with key. Upgrade is completed.

70200-0093

S-BB-BAT
Spare Backup Battery

Installation Instructions

The F Series family of readers uses an internal switching regulator to obtain internal operational power via an internal lead acid battery and a power fail protection PCB or onboard circuitry. With the latter in use, switchover to battery power is automatic and occurs when the main input voltage falls to approximately 10.5 volts. At that state, the internal battery charger is disabled to save power and uninterrupted operation continues on battery power. When input power is restored, the unit switches off of battery operation and the battery charger is re-enabled to recharge the battery. A fully discharged battery requires approximately 12 hours of charge to fully recover. Additional options installed and specific configurations within the unit make it difficult to predict precisely how long battery support will last, but in general two hours of battery operation is not unreasonable. While operating on battery backup, the reader will shut down when the battery voltage reaches approximately 9.5 volts. This is done to prevent full exhaustion of the battery. A yellow indicator on the top panel illuminates to indicate that the unit is running off of battery power. This indicator extinguishes when main input power is restored.

Placement of the shunt/jumper on J7 on the main logic board enables or disables battery operation on those units equipped with an optional battery backup. To fully power down a unit equipped with battery backup, remove or reposition shunt J7 so that the two pins protruding up from the main logic board are not connected to each other. Main input power can then be removed and the unit will fully shut down. If shunt/jumper on J7 is not properly installed, the internal backup battery will not be charged, and in the event of a main input power loss, the unit will shut down.

⚠ **CAUTION: This procedure requires erasing the existing hand templates. Save the existing hand templates before proceeding.**

1. Unlock the reader and rotate.
2. Disconnect the power supply from the board.
3. Remove and tag all external connections to make correct re-attachment.
4. Remove HandReader from wall by sliding it to the right, away from the wall mount. See figure 1 below.

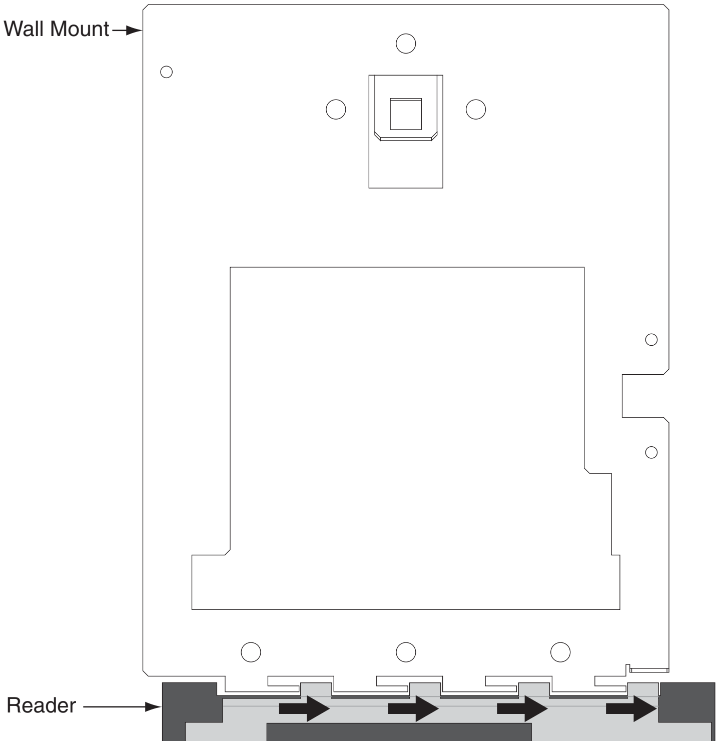


Figure 1

⚠ CAUTION: Before removing back plate of reader, wear a grounding wrist strap to help aid in protecting the circuit board from any ESD damage that might occur from improper handling.

5. Set the reader on a firm surface such as a table. Remove the four screws that secure the back plate to the HandReader. Remove the grounding screw and/or ground lug (if present). See figure 2 below.

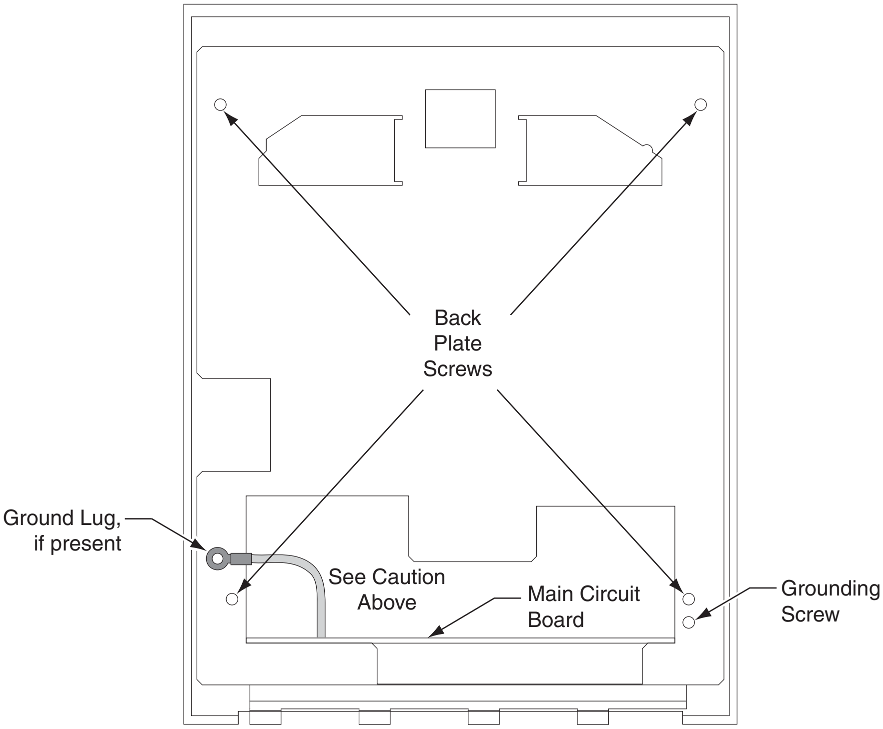


Figure 2

6. Remove the back plate.
7. Install the battery into the chassis. Route the cable as shown and attach to J4 on the top panel PCB as shown in figure 3 below.

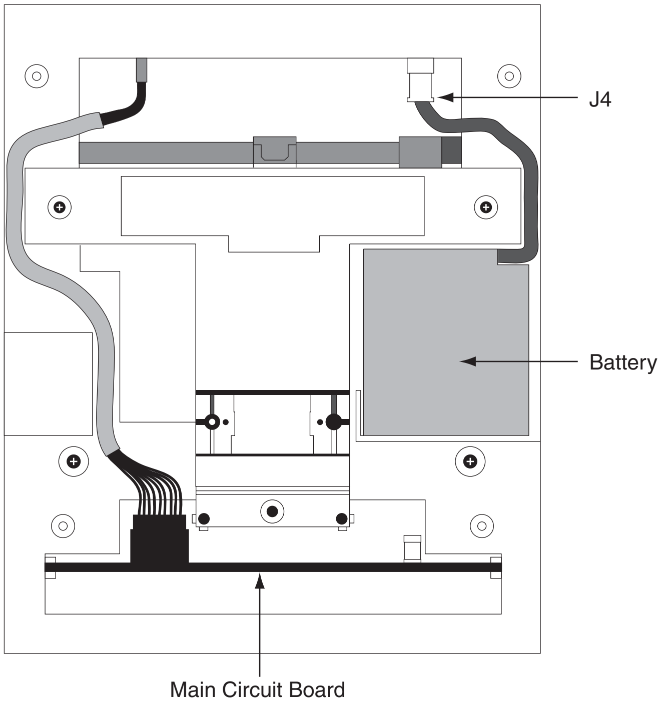


Figure 3

8. Reinstall the back plate onto the chassis. Reinstall grounding screw and/or ground lug (if present). Do not allow ground lug to come into contact with J7. Secure the back plate with the four screws removed in step 5.
9. Line up the slots at the bottom of the reader’s back with the four hinge pins at the bottom of the wall mount. Slide the reader to the left so the pins go in the slots. This fastens the reader to the wall and back plate and forms a hinge.
10. Reconnect cables removed in step 3.

11. If not already installed, install the J7 jumper (if applicable). See figure 4 below.

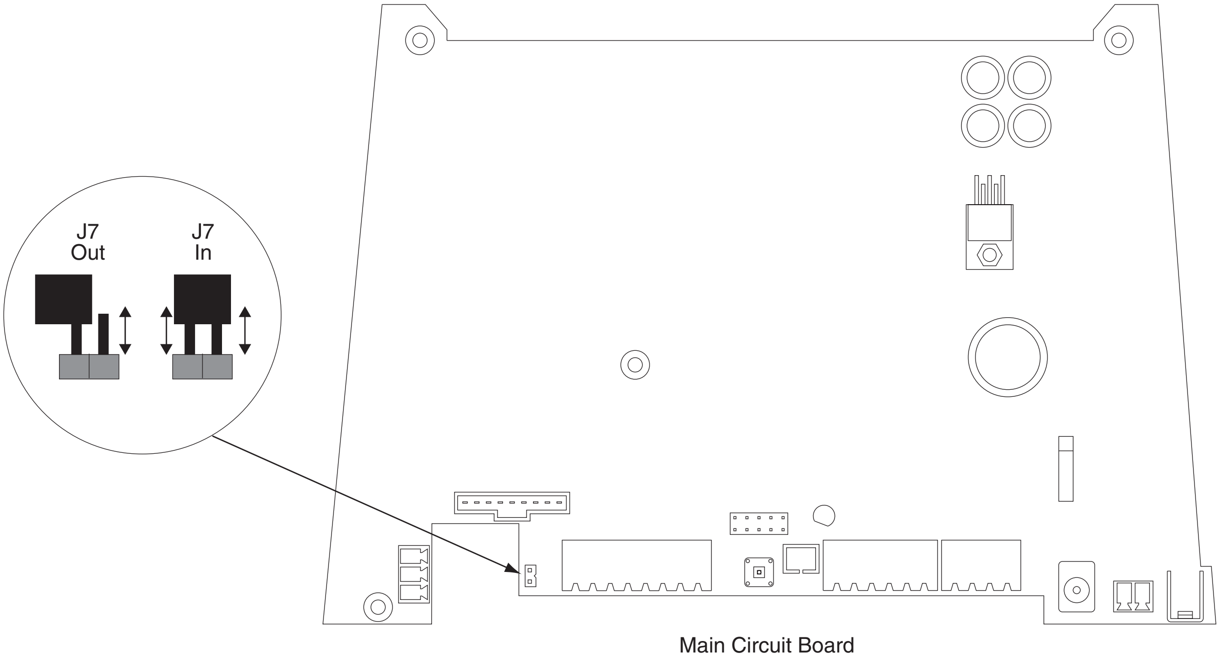


Figure 4

12. Power up the unit.

13. Secure the unit to wall mount with key. Upgrade is completed.

(877) 671-7011
Printed in Country

Wi-Fi 3rd Party Use: F-Series & G-Series

This document stands to act as a procedural guide for when using a 3rd party Wi-Fi adapter with the HandReaders, both F-Series & G-Series[1]. Schlage has performed testing to confirm that when using a Wi-Fi adapter[2], the HandReader will operate normally; so long as connections and addresses are properly set. Please use the following instructions as a guideline for initial set up of the Wi-Fi adapter.

Setup Summary of the Wireless Router and Bridge:

Host --> Switch --> Primary Wireless Router --> Wireless Router (Repeater/Bridge) --> HandReader[3]

Repeater/Bridge Setup

1. Configure the wireless router with LAN connection from the computer
   a. Set the computer to static IP mode
      i. i.e. Set the wireless router address to 192.168.0.1
      ii. i.e. Set the computer IP address to 192.168.0.100
2. Set the wireless router to repeater/bridge mode
   a. Need to make sure the primary wireless router address is different from repeater/bridge router
      i. i.e. Set the primary wireless router to 192.168.1.1
      ii. i.e. Set the repeater/bridge router to 192.168.1.10
3. Ensure that the DHCP server is disabled on the repeater/bridge router
4. Set the repeater/bridge router to connect to the primary wireless router by using security password
5. Connect a HandReader to the repeater/bridge router LAN port
   a. The GT-400 can be set either DHCP or static IP
   b. The F-Series HandReaders can be set as static IP

[1] F-Series models include: all HandPunch & HandKey models that have Ethernet enables. G-Series includes the GT-400.
[2] Wireless N150 Router: Encore 3G Mobile Broadband Wireless N150 Router plus Repeater, ENHWI-3GN3
[3] Note that the Host and the HandReaders are on the same network.

70200-0029

F Series Wall Mount Replacement

Installation Instructions

The following instructions apply to all F Series HandReader versions.

1. Unlock the reader and rotate.
2. Disconnect the power supply from the board.
3. Remove and tag all external connections.
4. Remove HandReader from wall by sliding it to the right, away from the wall mount. See figure 1 below.

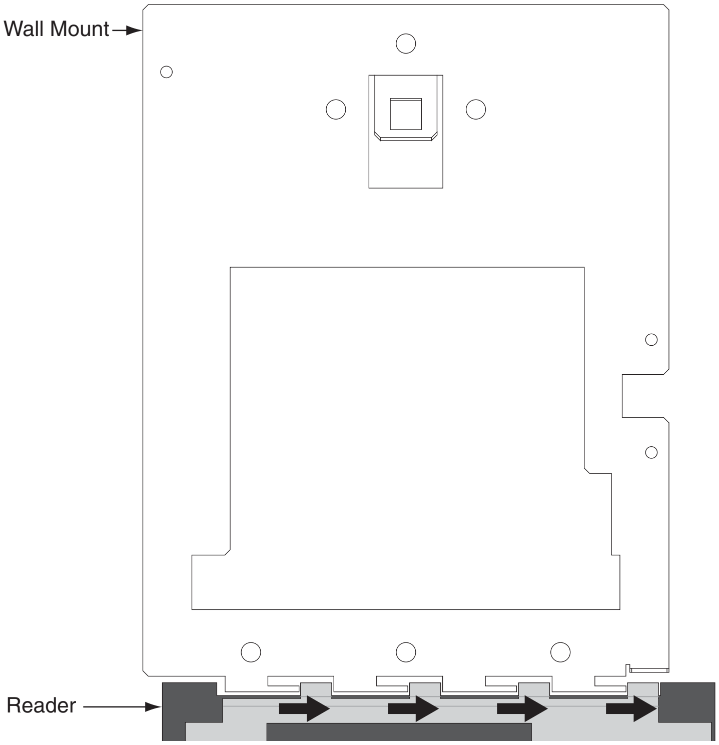


Figure 1

5. Remove the five screws that hold the wall mount in place. See figure 2 below.
6. Either hang the new wall mount or the paper template at the same height as the original wall mount. The wall mount must hang 48½” from the floor as measured from the top center hole on the panel. Ensure that the bottom line of the new wall mount/template is horizontal to the floor. Mark the locations of the five new screw holes.

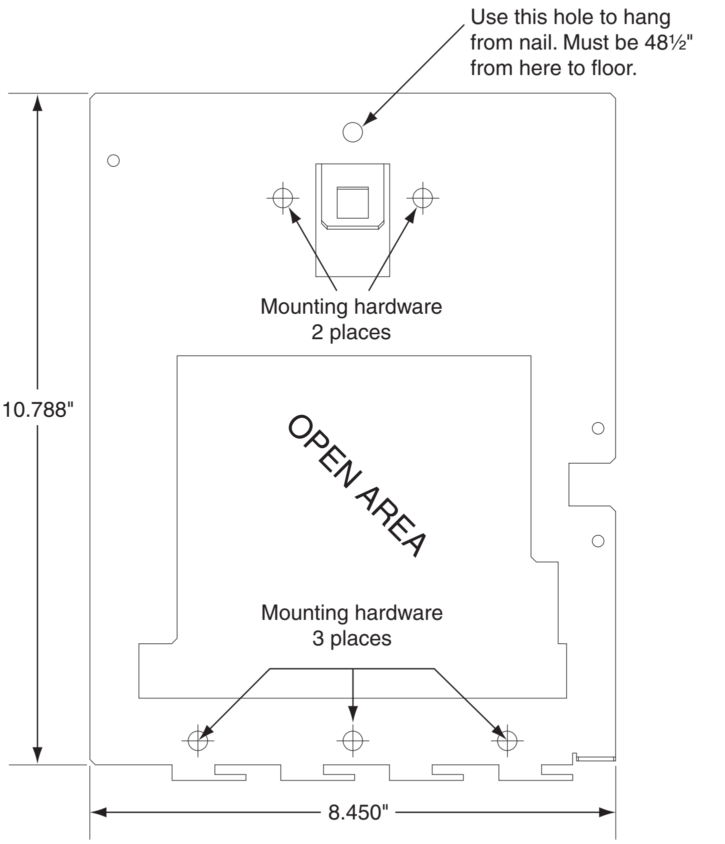

Use this hole to hang from nail. Must be 48½" from here to floor.
Mounting hardware 2 places
10.788"
OPEN AREA
Mounting hardware 3 places
8.450"

Figure 2

7. Install the new mounting hardware to the wall. Place the new wall mount panel against the wall, and install the panel.
8. Line up the slots at the bottom of the reader’s back with the four hinge pins at the bottom of the wall mount. Slide the reader to the left so the pins go in the slots. This fastens the reader to the wall and wall mount and forms a hinge. See figure 3 below.

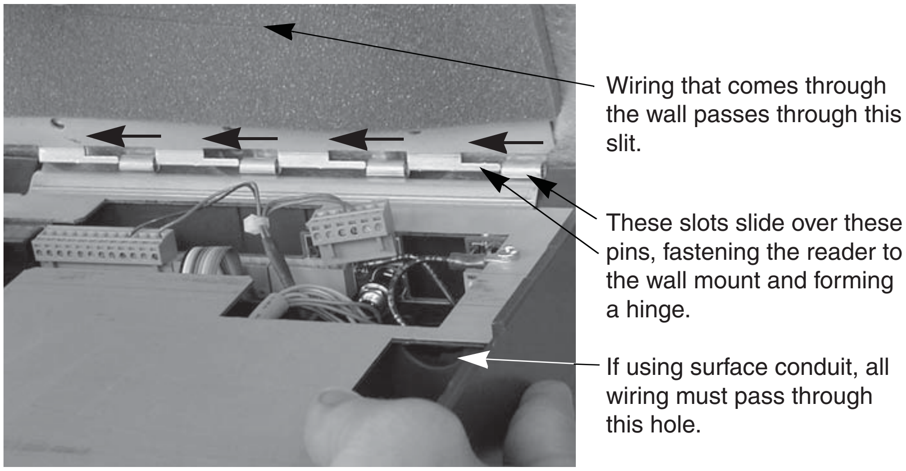

Wiring that comes through the wall passes through this slit.
These slots slide over these pins, fastening the reader to the wall mount and forming a hinge.
If using surface conduit, all wiring must pass through this hole.

Figure 3

9. Reconnect all cables removed in step 3 above.
10. Rotate the HandReader back towards the wall, and lock the unit into place with key.

Ingersoll Rand
Security Technologies

(877) 671-7011
Printed in Country

Technical Note

Product	HandNet for Windows
Date	May 22, 2014
Subject	Microsoft Windows Compatibility

HandNet for Windows, Microsoft Windows Compatibility

Hand Net for Windows has been tested with the following operating systems:

- Windows XP Professional Service Pack 2
- Windows XP Professional Service Pack 3
- Windows Vista Business Service Pack 1
- Windows 7 Pro Compatible 32 Bit
- Windows 7 Pro Compatible 64 Bit

All basic functionality was tested and performs as expected.

The only exceptions that users may experience when running on one of the mentioned operating systems are noted below.

Windows Vista

1) The Activity Report may fail to generate and or display an error to the effect of “This function is already being run.” Specifically this may occur immediately after install. The recommended course of action is to reboot the machine, and the activity report should be generated correctly without error.
Windows XP

1) An error may occur when there are multiple user accounts on the PC. A user may encounter a HandNet for Windows error stating, “Cannot open SQL Server.” This may happen when HandNet for Windows was installed under User #1’s login on the PC, and then User #2 logs into the same PC and runs HandNet for Windows, logs in, and tries to generate a report. It is possible that this may be attributed to User #2 not having full administrative rights to the folder that HandNet for Windows is installed in. In order to prevent the error, the user should verify that he/she has full administrative rights on the machine and or should have HandNet for Windows installed under his account.

If more errors are encountered, we will make addendums or additions to this technical note.

For additional information, please contact Customer Care at 877-671-7011.

ALLEGION™

Technical Note

Product	HandNet for Windows
Date	May 22, 2014
Subject	Microsoft Windows Compatibility

HandNet for Windows, Microsoft Windows Compatibility

Hand Net for Windows has been tested with the following operating systems:

- Windows XP Professional Service Pack 2
- Windows XP Professional Service Pack 3
- Windows Vista Business Service Pack 1
- Windows 7 Pro Compatible 32 Bit
- Windows 7 Pro Compatible 64 Bit

All basic functionality was tested and performs as expected.

The only exceptions that users may experience when running on one of the mentioned operating systems are noted below.

Windows Vista

1) The Activity Report may fail to generate and or display an error to the effect of "This function is already being run." Specifically this may occur immediately after install. The recommended course of action is to reboot the machine, and the activity report should be generated correctly without error.
Windows XP

1) An error may occur when there are multiple user accounts on the PC. A user may encounter a HandNet for Windows error stating, "Cannot open SQL Server." This may happen when HandNet for Windows was installed under User #1's login on the PC, and then User #2 logs into the same PC and runs HandNet for Windows, logs in, and tries to generate a report. It is possible that this may be attributed to User #2 not having full administrative rights to the folder that HandNet for Windows is installed in. In order to prevent the error, the user should verify that he/she has full administrative rights on the machine and or should have HandNet for Windows installed under his account.

If more errors are encountered, we will make addendums or additions to this technical note.

For additional information, please contact Customer Care at 877-671-7011.

3rd Party Biometric Testing on the HandReader

The HandReader has existed for over 20 years and has seen consistent and superior biometric performance. However, some error rates seen at a particular site are very dependent on several factors, most notably:

- population
- training and habituation
- threshold setting

Due to the variability of factors involved at individual sites, Allegion does not quote static performance rates. However, we often refer customers to two well-respected tests run by independent third-parties. The attached documents describe test methodology and state the corresponding performance metrics. Customers with similar use case environments can reasonably expect similar results.

In brief summary, the attached reports will show the following 3-try results:

a.	Type I error rate (false rejection rate) -			
	as low as	<0.1% (Sandia)	0.25% (CESG)	
b.	Type II error rate (false acceptance rate) -			
	as low as	0% (Sandia)	0.001% (CESG)	
c.	Crossover error rate (CER) -			
	as low as	0.1% (Sandia)	0.5% (CESG)	

The two reports are attached for your reference.

CESG Biometric Product Testing Final Report
Sandia Report

CESG contract X92A/4009309

Biometric Product Testing Final Report

Issue 1.0
19 March 2001

Tony Mansfield
Gavin Kelly
David Chandler
Jan Kane

Centre for Mathematics and Scientific Computing
National Physical Laboratory
Queen’s Road
Teddington
Middlesex
TW11 0LW

Tel: 020 8943 7029
Fax: 020 8977 7091

EXECUTIVE SUMMARY

This is a report of a performance evaluation of seven biometric systems conducted by NPL over the period May to December 2000. The test programme was sponsored by the Communications Electronics Security Group (CESG) as part of their Biometrics Work Programme in support of the "Modernising Government" and other initiatives.

The objectives of the test programme were:

- To show the level of performance attainable by a selection of biometric systems;
- To determine the feasibility of demonstrating satisfactory performance through testing;
- To encourage more testing to be sponsored, and to promote methodologies contributing to the improvement of biometric testing.

Face, Fingerprint, Hand Geometry, Iris, Vein and Voice recognition systems were tested for a scenario of positive identification in a normal office environment, with cooperative non-habituated users. The evaluation was conducted in accordance with the "Best Practices in Testing and Reporting Performance of Biometric Devices" produced by the UK Government Biometrics Working Group, and used 200 volunteers over a three-month period.

Results presented include:

- Failure to Enrol and Failure to Acquire Rates;
- The trade-off between matching errors (False Match Rate vs. False Non Match Rate) and between decision errors (False Acceptance Rate vs False Rejection Rate) over a range of decision criteria;
- Throughput rates of users in the live application, and of the matching algorithm in off-line processing;
- Sensitivity of the systems' performance to environmental conditions, and the differences in performance over different classes of users.

Biometric system performance is dependent on the application, environment and population. Therefore the performance results presented here should not be expected to hold for all other applications, or in all environmental conditions. In particular caution should be exercised when comparing these results with those of other systems tested under different conditions.

CONTENTS

FIGURES

TABLES

1 INTRODUCTION

1. This is a report of a performance evaluation of seven biometric systems conducted by NPL over the period May to December 2000. The test programme was sponsored by the Communications Electronics Security Group (CESG) as part of their Biometrics Work Programme in support of the "Modernising Government" and other initiatives.

2. The test programme had three main objectives:
   a. To show the level of performance attainable by a selection of biometric systems;
   b. To determine the feasibility of demonstrating satisfactory performance through testing;
   c. To encourage more testing to be sponsored, and to promote methodologies contributing to improvement of biometric testing.

3. The tests provide factual, vendor-independent data on the performance of biometric devices. This will inform CESG on the general capability of biometric technology, and will help in the development of policy on the use of biometrics in Government. It will also assist members of the UK Government Biometrics Working Group (BWG) in the assessment of the applicability of biometric technology to their potential applications.

4. The tests will implement and validate the BWG proposed methodology for biometric testing. The outcome will support the further development of this methodology for use with Common Criteria evaluations of biometric products and systems.

5. It is also hoped that this initial evaluation will, by example:
   a. Promote the methodology to a wider audience and contribute to the improvement of biometric testing by other organisations; and
   b. Encourage further testing to be sponsored.

   To allow wider dissemination of the results (given that open publication of results was not a requirement for vendors participating in the trials), the report has been organised into two parts with different restrictive markings. The intention is that Part I excludes any commercially sensitive information and can be made publicly accessible, while Part II contains full details for CESG and Government Departments.

2 SELECTION OF SYSTEMS

6. The Test Programme was announced on the Biometrics Consortium list server, and some thirty companies responded to the call for submission of devices for testing. Because of overlap in terms of devices proposed, about twenty different systems were considered for inclusion in the test programme.

7. The criteria for selection of systems to test were agreed by CESG and the Biometrics Working Group.
   a. Fingerprint, hand and iris technologies must be included. Other systems tested should use different technologies, except for fingerprint where two systems might be tested.
   b. Within a technology, selection should be on the basis of wide availability and commonality of use.
   c. Systems should be capable of meeting basic CESG performance requirements.
   d. Systems should be testable under the agreed methodology (and, implicitly, the system performance should not be adversely affected by the proposed test protocol).
   e. The vendor should be able to support the trials within the required timescales.

8. Using these criteria, seven systems were selected for testing, using face, fingerprint, hand geometry, iris, vein pattern, and voice and recognition. There were two fingerprint systems: one using optical fingerprint capture, the other a chip sensor. Table 1 gives brief details of the tested systems. Systems have been named where vendors are happy for their results to be publicly available. (Full details of all systems are given in Part II of this report, which has a more restricted circulation.).

Short name	Brief description
Face Face (2)	Visionics – FaceIt Verification Demo Alternative enrolment and matching algorithms for this system
FP-chip FP-chip (2)	VeriTouch – vr-3(U) Alternative enrolment and matching algorithms provided by Infineon
FP-optical	*Fingerprint recognition system.*
Hand	Recognition Systems – HandKey II
Iris	Iridian Technologies – IriScan system 2200
Vein	Neusciences-Biometrics – Veincheck development prototype
Voice	OTG – SecurPBX Demonstration System

Table 1. Brief details of systems tested

9. As there is just one device per technology, it should be noted that the performance results presented are not necessarily fully representative of all systems of the same type. Indeed, even relatively minor modifications to the systems tested can give considerably different performance.

3 TEST SCENARIO

10. The test scenario was one of positive verification in a "normal office environment", with co-operative non-habituated users. The tests were conducted with 200 volunteers, over a three-month period. The typical separation between enrolment and a verification transaction was one to two months.

3.1 Volunteer crew

11. To obtain participants, a call for volunteers was issued by e-mail and in the NPL in-house newsletter. A small payment offered as an incentive for participation (and adherence to the trial "rules"). All those responding were invited to participate, though some withdrew when they could not attend an appointment for enrolment. A limited further call was issued to some staff of the other laboratories on site (NWML and LGC) to achieve slightly over 200 participants. The volunteer crew were thus self-selecting, consisting mostly of staff working on the NPL site. The age and gender profile is shown in Figure 1. This approximates that of the workforce on site.

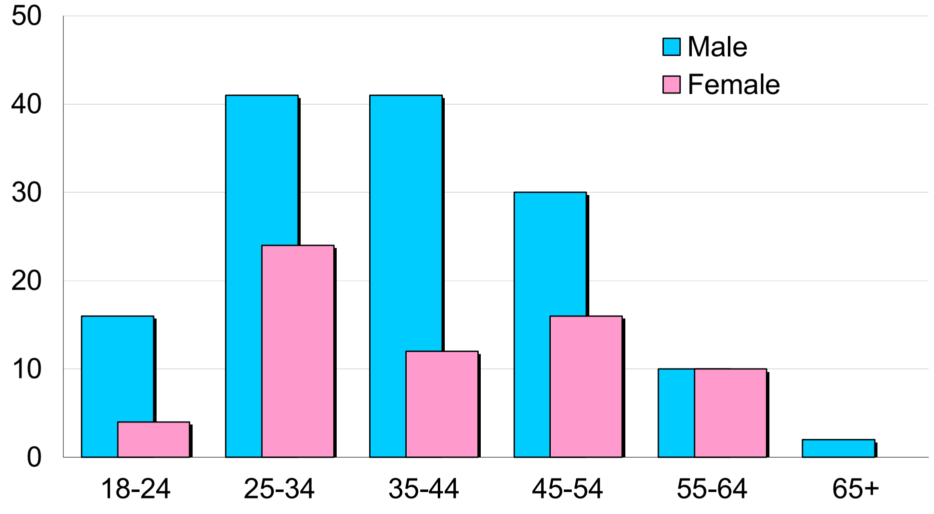


Figure 1: Age and gender of volunteer crew

12. This volunteer crew is not fully representative of the general UK adult population. Women and those older than 45 are under-represented, also the balance between different ethnic

groups is probably incorrect (ethnic origin of volunteers was not recorded). Moreover, as the volunteer crew are used to working in a scientific environment, they are more accepting of technology than the population at large. Potentially this might reduce errors due to the behavioural element in biometric system use.

3.2 Environment.

13. The tests were conducted in a room previously in normal office use.

14. Lighting levels were controlled. The room's fluorescent lighting was always on, and the window blinds kept down to reduce effects of daylight variations. The devices were sited in accordance with recommendations of the product suppliers, and those most sensitive to changes in illumination were positioned away from the window. Similarly one device whose use was sensitive to background noise was located in a quieter area off the main test laboratory. These adjustments are documented with the test results for each device.

15. The temperature and humidity of the test laboratory were not controlled. Figure 2 indicates how outdoor temperature[1] and humidity[2] varied between the days of the trials

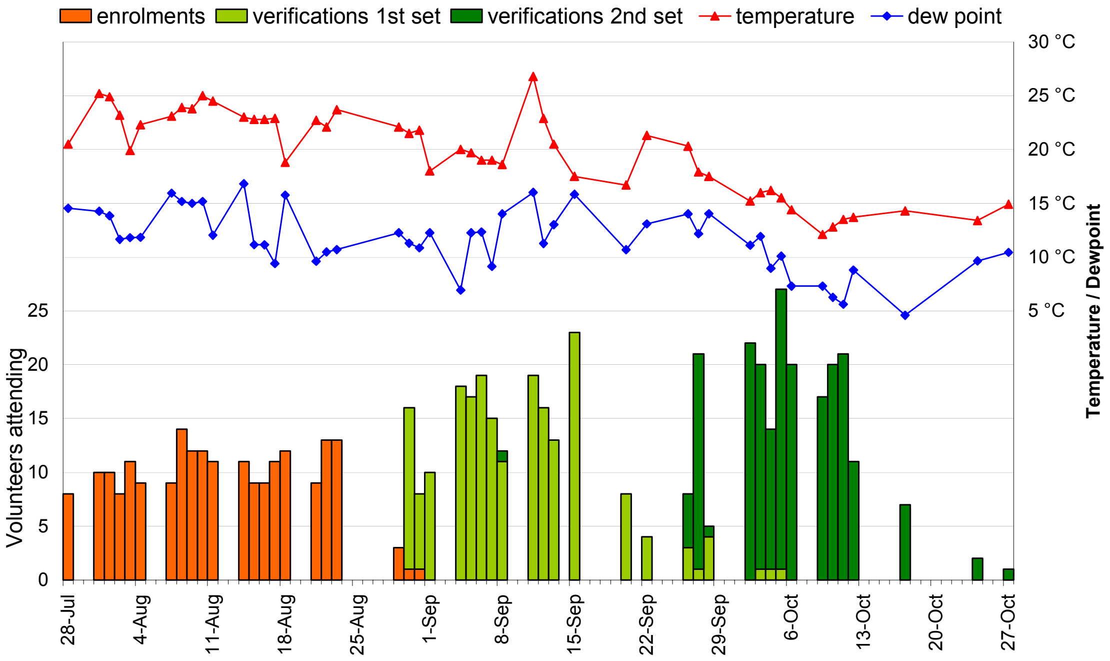


Figure 2. Environmental conditions during the trials

3.3 Enrolments & verifications

16. Figure 2 also shows the daily distribution of enrolment and verification transactions. On average the first set of verifications was made 29 days after enrolment, and the second set of verifications, 55 days after enrolment.

3.3.1 Order effects

17. The order in which the devices were used could potentially affect performance.

[1] Figures based on readings from local weather station.

[2] Dew point is plotted instead of relative humidity. This removes the strong (inverse) correlation with temperature, and to allows the same °C scale to be used.

a. On arriving at the test laboratory, volunteers could be out of breath (if they have hurried to make their appointment) or have cold hands/fingers (when cold outside), recovering to a more normal state after a few minutes.

b. The illumination for the face recognition system increased the amount of iris visible (i.e. reduces pupil size) with a potential effect on iris recognition when this occurs shortly after.

c. Feedback from one fingerprint device might affect user behaviour (e.g. finger pressure) on the other.

18. Other than volunteers attempting speaker verification when out of breath, these order effects did not appear significant. Further order effects may also exist, but are also believed to be insignificant. In view of this, a complex fully randomised sampling plan was not adopted.

a. Transactions on the Voice system were not conducted until the volunteer had regained their breath.

b. The order in which the devices were used alternated between a clockwise order around the room, and anti-clockwise. However, this ordering was often modified to avoid queuing at any system. There were no order correlations between visits.

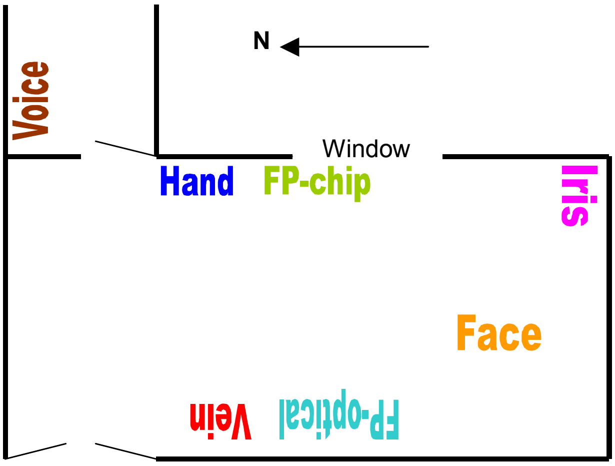


Figure 3. Positioning of systems in test laboratory

4 TEST METHODOLOGY

19. The performance trials were conducted in accordance with

Best Practices in Testing and Reporting Performance of Biometric Devices[3]

produced by UK Government Biometrics Working Group. The test protocol followed is described in

A test protocol for the Technical Performance Evaluation of Biometric Devices

For completeness this Test Protocol is included in Appendix A.

20. Modifications and enhancements to the general test protocol are discussed below.

4.1 Dealing with enrolment failures

21. Observations during preliminary testing showed:

a. Often more than two attempts would be required to obtain an enrolment. This seemed to be particularly the case with the Voice and both Fingerprint systems, where obtaining a good quality “image” is more dependent on user behaviour and familiarity.

b. For some systems, the enrolment software did not provide for re-enrolment. In such cases, problem enrolments needed to be deleted, using the underlying operating system, before re-enrolment was possible. For data-integrity reasons, we were reluctant to do this

[3] Available at http://www.cesg.gov.uk/biometrics/

while under the pressure of processing volunteers, and as a result re-enrolments had to occur on a subsequent visit.

c. Some systems did not automatically record every enrolment attempt failure.

22. The protocol for dealing with enrolment failures was therefore modified. Where practical, immediate re-enrolment was attempted, (as previously). However, at subsequent visits, whenever a volunteer had failed to enrol on one of the devices, they were asked to try re-enrolling regardless of the number of previous enrolment attempts.

4.2 Avoiding data collection errors

23. Additional procedures were put in place to help avoid data collection errors:

a. Errors due to the use of the wrong hand, finger, etc.

b. Errors due to attributing the attempt to the wrong identity.

4.2.1 Avoiding use of wrong hand, finger, etc.

24. Users were asked to always use their right index finger, eye or hand as appropriate. Without this consistency, it would be difficult for supervisors to observe and prevent use of the wrong finger, hand or eye at enrolment or verification. The saved images allow further checks that the correct iris, hand or finger was used, though this is easier for iris and hand images than for fingerprint images.

4.2.2 Avoiding attribution of attempt to wrong identity.

25. Each user was allocated a PIN for the trials, which was shown on the named data sheet collected by the user at each session (see e.g. Appendix C). The following possibilities for attributing attempts to the wrong identity must be addressed by checking procedures.

a. The user picks up the wrong data sheet[4].

b. The user mistypes their PIN, producing another valid PIN[5].

c. The user forgets to enter their PIN on a system where the PIN is not cleared between attempts. As a result the attempt is made against the previous user's identity[6].

These were addressed as follows.

26. **Feedback on claimed identity**
The Voice, Face and Iris systems provided feedback on the claimed identity. This would show the individual and supervisor that failures were due to the wrong PIN being used.

27. **Error detecting PINs**
The PINs used to claim an identity were chosen to minimise the chance that mistyping would produce another valid identity. This was done using the ISBN error-detection scheme (though avoiding use of "X" as the check digit). The 4-digit PINs `abcd` have the property that `4a+3b+2c+d` is exactly divisible by eleven. This detects all single digit errors and transpositions. From the available PINs, the set used was as widely spaced as possible, in the range 1000 – 9999, giving robustness against more complex typing errors.

28. **User makes at least 3 attempts per device per session**
If a PIN not being entered causes attempts to be recorded against the previous user's identity, these will be the 4th or subsequent attempts. However, these will be ignored as only the first 3 attempts per user per session are analysed.

29. Any incorrect attempts were recorded on the user's data sheet, allowing for annotation of the logged data and exclusion from analysis. Where possible, prior to conducting analyses, the

[4] This happened twice (of a possible 412 occasions), where the volunteers had very similar names.

[5] One of the systems recorded when incorrect PINs were entered. Of some 2000 entered PINs, 5 were entered incorrectly. Two single digit errors, one transposition, and two 2-digit errors.

[6] This could happen on three of the systems tested, occurring twice, once, and no times (of a possible approx 400 occasions).

data saved for verification failures were checked further, to determine if the cause of failure was a mis-acquisition or a mis-labelling.

5 RESULTS OVERVIEW

5.1 Failure to enrol

30. The "failure to enrol" rate measures the proportion of individuals for whom the system is unable to generate repeatable templates. This includes those unable to present the required biometric feature (for example the Iris system failed to enrol the iris of a blind eye), those unable to produce an image of sufficient quality at enrolment, as well as those unable to reproduce their biometric feature consistently. Enrolment failure rates for the systems tested are shown in Table 2. Note that, in cases of difficulty, several attempts were allowed to achieve an enrolment. If necessary, these further enrolment attempts were made at subsequent visits by the volunteer.

System	Failure to enrol rate
Face	0.0%
Fingerprint – Chip	1.0%
Fingerprint – Optical	2.0%
Hand	0.0%
Iris	0.5%
Vein	0.0%
Voice	0.0%

Table 2. Failure to enrol rates

5.2 Failure to acquire

31. The "failure to acquire rate" measures the proportion of attempts for which the system is unable to capture or locate an image of sufficient quality. This includes cases where the user is unable to present the required biometric feature (e.g. having a plaster covering his or her fingerprint); and cases where an image is captured, but does not pass the quality checks. Failure-to-acquire rates for the systems tested are shown in Table 3. The figures exclude cases where the image was not captured due to user error (e.g. the user not positioning themselves correctly) as in these cases the attempt was simply restarted.

System	Failure to acquire rate
Fingerprint – Chip FP-chip (2)	2.8% 0.4%[7]
Face	0.0%
Fingerprint – Optical	0.8%
Hand	0.0%
Iris	0.0%
Vein	0.0%
Voice	2.5%

Table 3. Failure to acquire rates

5.3 False match rate (FMR) vs false non-match rate (FNMR)

32. The fundamental operation of a biometric system is the comparison of a captured biometric image against an enrolment template. The false match and false non-match rates measure the

[7] For verification, minimal quality checks were performed.

accuracy of this matching process. By adjusting the decision criteria there can be a trade-off between false match and false non-match errors; so the performance is best represented by plotting the relationship between these error rates in a detection error trade-off graph.

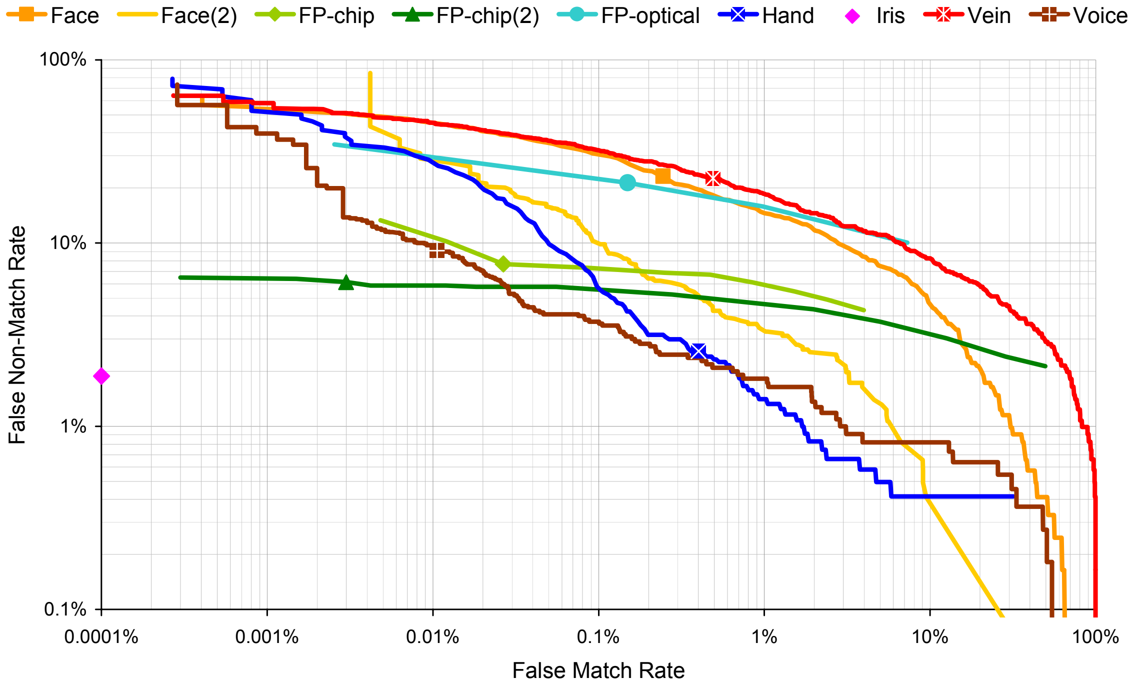


Figure 4. Detection error trade-off: FMR vs FNMR

33. Matching algorithm performance for each system, over a range of decision criteria, is shown in Figure 4. (The lower and further left on the graph, the better the performance). The node on each curve shows performance at the default decision threshold. No curve is shown for the Iris system, which operates with a pre-determined threshold. The iris system had no false matches in over 2 million cross-comparisons. For all the other systems the leftmost point on each curve represents a single false match in the total number of cross-comparisons made.

34. Observing images corresponding to false non-matches showed that some of matching failures were due to poor quality images. Systems vary in how they deal with poor quality images, some will “fail to acquire” such images, while systems will often cope with poor image quality. Therefore the matching error rates should not be considered in isolation from the failure to acquire and failure to enrol rates.

5.4 False acceptance rate (FAR) vs. false rejection rate (FRR)

35. False acceptance and rejection rates measure the decision errors for the whole system. These measures combine matching error rates, and failure to acquire rates in accordance with the system decision policy. When the verification decision is based on a single attempt:

$$\mathrm{FAR}(\tau) = (1\text{-}\ \mathrm{FTA})\ \mathrm{FMR}(\tau)$$

$$\mathrm{FRR}(\tau) = (1\text{-}\ \mathrm{FTA})\ \mathrm{FNMR}(\tau) + \mathrm{FTA}$$

where τ is the decision threshold, and FMR, FNMR, FTA, FAR and FRR are the false match rate, false non-match rate, failure to acquire rate, false acceptance rate and false rejection rate respectively.

36. The false acceptance false rejection trade-off curve is shown in Figure 5. The curves for the face, hand geometry, iris and vein systems are unchanged, as these systems had no failures to acquire.

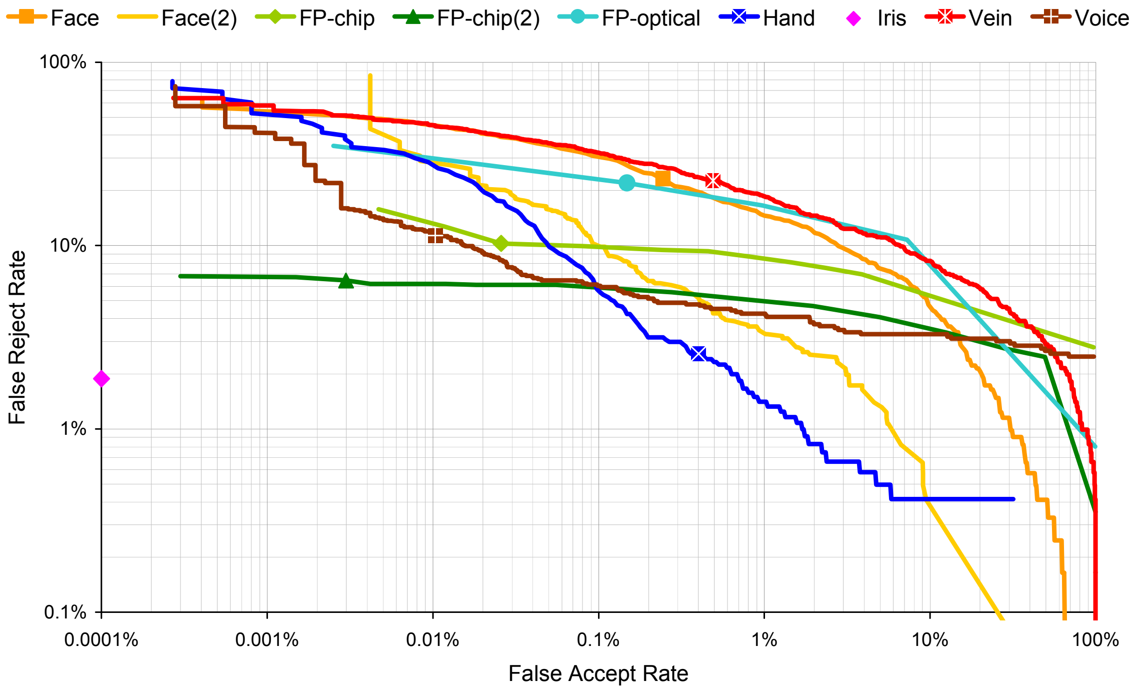


Figure 5. Detection error trade-off: FAR vs FRR

5.5 Multiple attempt error rates

37. Many systems allow multiple attempts, in their normal mode of operation. The effects on error rates of a "best-of-3" decision policy are examined in this section.

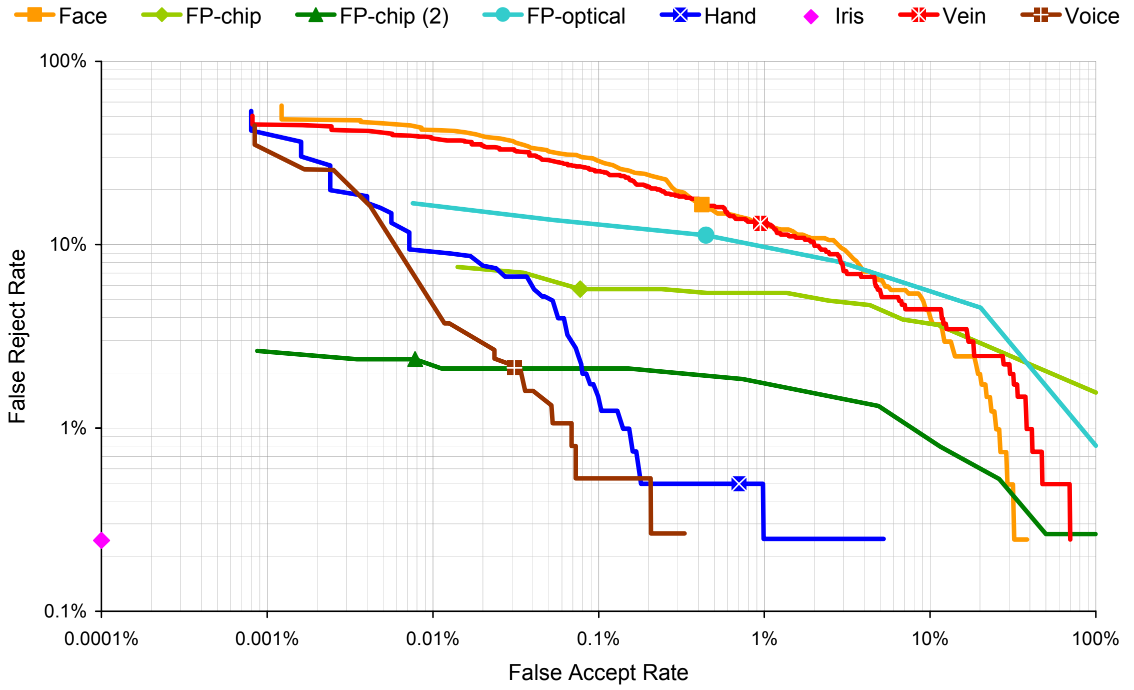


Figure 6. Detection error trade-off: Best of 3 attempts

38. The 3-attempt genuine and impostor scores are the best matching score from the 3 attempts made at the person-visit (scored against the chosen template). The resulting detection error trade-off (DET) curves are shown in Figure 6.

39. This method of obtaining the DET curve is appropriate when all attempts are constrained to use the same finger, face or hand etc. In real life, it may be possible to substitute a different finger, face, hand, etc at the second or third attempt. If so (and assuming the individual impostor attempts are fully independent) the 3-attempt false acceptance rate at any decision threshold is given by $1-(1-\alpha)^3$ where α is the false acceptance rate for a single attempt at the same threshold. Thus, two detection error trade-off curves may be shown:

a. Where all three attempts are constrained to use the same finger, hand, face, etc; and

b. Where substitutions are allowed between attempts.

In the case of the trial systems and data, the two curves follow each other closely[8], so Figure 6 shows a single curve for each system[9].

5.6 User throughput

System	Transaction Time (Seconds)			Time includes entry of PIN?
	Mean	*Median*	*Minimum*	
Face	15	14	10	Excluded
Fingerprint-Optical	9	8	2	Excluded
Fingerprint-Chip	19	15	9	Excluded
Hand	10	8	4	Included
Iris	12	10	4	Included
Vein	18	16	11	Included
Voice	12	11	10	Excluded

Table 4. User transaction times

40. The time for a user transaction has been calculated using the time differences logged between consecutive transactions (as detailed in Appendix A.6.7). Table 4 shows the mean, median and minimum transaction times to indicate the spread of results. The differences in operation of the trial systems accounts for much of the difference in timings.

a. The Face system collected a sequence of images over a 10 second period, saving the best match obtained. The transaction times would be somewhat shorter if the system stopped when the threshold was first exceeded; however, this would not have allowed us to examine performance over a range of decision thresholds.

b. The Iris system would normally work in identification mode, not requiring PIN entry. This would reduce transaction times.

c. The keypad of the Vein system could not cope with rapid entry of the PIN. The time to do this dominates the overall transaction time.

d. The transaction times for the Voice system were dominated by the time taken in giving user prompts and feedback. The prompting and speeds were chosen to be suitable for users unaccustomed to the system, rather than for maximum throughput.

5.7 Matching algorithm throughput

41. The measured throughput of the programs for batch mode running of the matching algorithms is shown in Table 5. These diagnostic programs had significant overheads, for example logging all matching attempts to a file, or handling the Windows interfaces. Therefore, the matching algorithm throughput may be significantly higher than those shown, perhaps by a factor exceeding 100. (In the case of the chip-based fingerprint system, the difference in throughput of the two diagnostic programs illustrates the improvement possible. In an

[8] The ratio FAR_b/FAR_a of the false acceptance rates derived under the different assumptions varies from 1 to 1.3 for the voice system and fingerprint systems; from 1 to 1.7 for the vein system, and from 1 to 2 for the hand and face systems.

[9] For the FP-chip, and FP-optical systems, a cross-comparison scoring of all attempts against each template was not available, and the curve shown is derived as detailed in paragraph 39. For FP-chip (2) and all the other systems, the curve was derived using a full set of genuine and impostor scores.

equivalent implementation, the basic FP-chip algorithm would be faster than the more complex alternative FP-chip(2).)

System	Matches per minute	Program interface	System, processor speed, memory, & OS			
Face	800	Windows	Pentium			Win2K
FP-chip	60	Windows	Pentium	133MHz	32Mb	Win98
FP-chip (2)	2,500	Command Line	Pentium	500MHz	64Mb	Win95
FP-optical	50	Windows	Pentium	500MHz	64Mb	Win95
Hand	80,000	Command Line	SunUltra5	270MHz	128Mb	SunOS5.8
Iris	1,500,000	Command Line	SunUltra5	270MHz	128Mb	SunOS5.8
Vein	130	Windows	Pentium	500MHz	64Mb	Win95
Voice	680	Command-Line	Pentium	500MHz	64Mb	Win95

Table 5. Diagnostic program throughput

5.8 Performance differences by user & attempt type

42. Attempts can be categorised by:

a. Whether made at enrolment visit or at the second or third visit by the volunteer;
b. The gender of the volunteer;
c. The age of the volunteer;
d. Whether the volunteer was wearing spectacles in the case of Face and Iris systems;
e. The length of the user's pass-phrase in the case of the Voice system.

Performance differences between these subsets have been analysed, and are reported for each system in Part II. The general findings are summarised in Table 6.

System	Gender	Age	Visit	Other
	Observations:	lowerFRR<higherFRR		Less significant
		lowerFRR<higherFRR		**More significant**[10]
Face	**male<female**	younger<older	**enrol<later**	without<with glasses
FP-chip	male<female	**younger<older**	**enrol<later**	
FP-chip(2)	male<female	younger<older	enrol<later	
FP-optical	male<female	**younger<older**	**enrol<later**	
Hand	male<female			
Iris				without<with glasses
Vein	**male<female**	younger<older	**enrol<later**	
Voice	female<male	younger<older	**enrol<later**	

Table 6. Summary of performance differences by user type

43. False rejection rates for attempts made immediately following enrolment were generally significantly lower than (less than half) those made at volunteer's second or third visit.

44. Generally men had a lower false rejection rate than women (the voice system being the only exception), and younger volunteers a lower false rejection rate than their older colleagues. The gender differences appeared the more significant for the Face, Hand and Vein systems, and the age differences the more significant for the Fingerprint systems.

45. As women and over 45's were under-represented in our volunteer crew, our results may be biased. For a given threshold, with equal numbers of men and women, a slightly higher false non-match rate might be expected. However since false matches are more likely within the same gender class, the equalisation would reduce the false match rate at the same threshold.

[10] The more significant observations have a χ^2 value exceeding 15. (See Appendix D for details.) The probability of such observations being due to the random nature of the sample is in the range 0.01% - 20% dependent on the degree of correlation between different attempts by the same person.

6 VALIDATION OF METHODOLOGY & FUTURE ENHANCEMENTS

46. The evaluation has implemented the BWG proposed methodology for biometric testing, validating many aspects of this methodology. For example:

a. Demonstrating the feasibility of the methodology;

b. Showing that the number of volunteers used (200) is sufficient to evaluate performance of biometric systems at their current level of accuracy;

c. The practical significance of issues described in "Best Practices" has been demonstrated:
The need for time separation between enrolments and verification attempts;
The need to minimise the chance of labelling errors;
The modified procedures to simulate unknown impostor attempts when there are dependencies between templates.

A single evaluation cannot demonstrate repeatability of the results. However, some of the devices evaluated have been tested elsewhere in similar scenarios, and the results are consistent.

47. The evaluation revealed further issues concerning the applicability of the test protocol, and enhancements to best practices. These are noted below.

6.1 The requirement for additional system functionality

48. The test protocol required systems to save data for off-line calculation of genuine and impostor matching scores. This capability is often not provided in a vendor's standard supplied system. This raises the following issues:

a. Some systems will be unable to meet this requirement for testing (for example standalone systems which store templates are stored locally, but have insufficient memory to log transaction attempts). This point was raised by some of the vendors who initially expressed an interest in participation in the trials.

b. When the required functionality is achievable with vendor support, it is important that protocols are sufficiently consistent across testing organisations. Otherwise the vendor needs to develop a different customisation for each test, and support costs can be very significant.

c. Sometimes achieving the desired functionality can affect system performance. For example the time taken in logging images may slow the system and affect user behaviour. It is also possible that implementing the required functionality at minimal cost will introduce errors into the system.

49. If all testing, including impostor tests, are conducted "live" these problems are avoided. However, this requires:

a. Data collection to be very closely supervised as all results must be logged by the supervisor;

b. Extra attempts to be made to show performance at a variety of decision thresholds; and

c. Extra attempts to be made for live impostor tests.

6.2 One attempt may involve a sequence of images

50. With many biometric systems, a sequence of images is processed in a single verification attempt. For example, with the trial system it appears that:

a. The Face system collects images over a period of 10 seconds, and gives the best match obtained;

b. The Chip-based Fingerprint system collects images until a match is obtained, or until timeout;

c. The Optical Fingerprint system scans for fingerprints until an image of sufficient quality is obtained, or the timeout is reached;

d. The Hand Geometry system occasionally requires a second hand placement, when the score is very close to the decision threshold;

e. The Iris system collects images until a match is achieved or until timeout.

51. The current version of "Best Practices" does not explicitly deal with these cases, yet this mode of operation can sometimes bias off-line calculations using the collected data. For example with the face system, in a real impostor attempt the score would be based on the image that best matches the impersonated template. A cross-comparison of stored genuine images uses the image that best matches the genuine template, and therefore may underestimate the false match rate.

52. The questions that must be addressed are:

a. Would the decision be based on a different image if comparison were against a different template?

b. If so, would live impostor attempt scores be higher/lower than off-line scoring with genuine attempt images?

In the case of the tested Optical Fingerprint, Hand Geometry and Iris systems, the image collected does not depend on the template being matched. With the Fingerprint Chip, the collected image might instead be last before timeout; and, apart from image quality, should be equivalent to the image saved from a genuine attempt.

6.3 Failure to acquire

53. As noted in Section 5.3 (paragraph 34), different systems handle poor quality input in different ways. With some systems this may result in a failure to acquire, and with others a matching failure. In this respect the FAR-FRR trade-off graph provides a better comparison of performance than the FMR-FNMR trade-off graph.

6.4 Other performance trade-offs

54. Systems may have other adjustable parameters affecting performance in addition to (or instead of) an adjustable decision threshold. These allow different performance trade-offs (which, depending on the application, may be more important than the FAR-FRR trade-off). For example, with the Face, Iris, and Chip-Fingerprint systems, which try to match collected images over a fixed time period, there is a trade-off between the time allowed and the false rejection rate.

APPENDIX A. TEST PROTOCOL

A.1 Introduction

This report describes the test protocol planned for the UK Government Biometric Test Programme. The protocol is for "scenario testing" and conforms to the guidelines in "Best Practices in Testing and Reporting Performance of Biometric Devices". The protocol is intended to be practical in terms of effort and costs, and applicable to many of today's commercially available biometric devices when operating in their intended environments.

Several systems will be tested at the same time, in a standard indoor (office) environment and using a volunteer crew similar to the general adult UK population. The trials will involve approximately 200 volunteers using each of the systems being tested. Volunteers will attend the trials on three occasions: firstly for enrolment and practice attempts; and later, one and two months after enrolment, to collect "genuine" attempts Detection Error Trade-off (ROC) analysis.

Impostor attempts will be simulated using cross-comparison of genuine attempts against enrolment templates for other enrolees. This will be carried out off-line using vendor-provided software with the collected enrolments and genuine-attempt images and data.

A.1.1 Applicability of this protocol

Biometric limitations — The protocol cannot be used if it takes much longer than a few seconds for the system to extract the required biometric features. For example we could not test a system that uses 10 minutes of typing at a keyboard to make an identity decision. The separation between enrolment and test attempts will be approximately 1 month. If we are interested in the effects of template ageing time over a timespan much greater than this, the protocol may also be inappropriate.

System functionality — We can only test complete systems. These must be able to operate in "verification" mode, matching a single attempt against a single stored template. It is also necessary for the system to log specific information about each attempt, and there must be a capability for off-line generation of matching scores

System Error Rates — We shall not be able to measure error rates to values of 1% or below with any certainty. For example, if 1% of the population have (or lack) some feature causing enrolment failure, there is a 13% chance that no-one in a 200 person sample have that peculiarity. On the other hand to measure error rates exceeding 10% we may be using more volunteers than required, and a smaller test may be more cost effective.

A.1.2 Modelled Scenario

The scenario modelled is that of a verification application in an indoor environment.

Co-operative users — It is hard to replicate the actions and motivations of an uncooperative user.

Overt system — We shall be using volunteers who will be brought to a specific location for testing, and who will test several devices. This effectively rules out covert testing.

Non-habituated users — Our volunteers will use the system a few times only, with gaps of a few weeks between each use. The level of habituation will therefore be quite low. We shall avoid using volunteers who have extensively used one of the systems under test, so that comparisons are fair. We do not propose replicating a higher level of habituation by allowing practice attempts: this would create additional complexities to be able to separate practice attempts from the real test attempts.

Supervised enrolment, lightly-attended use — Enrolment will be supervised. Subsequent attempts will be lightly attended: there will be someone on hand to sort out problems should these occur. However, it should be noted that, after enrolment, the main role of the supervisor is to ensure the integrity of the data collection process rather than to assist volunteers in their attempts.

Standard environment — The tests will be conducted indoors, in a standard office environment. It is harder, and more costly to conduct the trials in an outdoor environment, and currently relatively few devices will operate satisfactorily in an outdoor environment.

Public users (UK adults) — Volunteer user attitudes are likely to be closer to those of the general public, than that of company employee. Also, volunteers will be local to the testing laboratory, and their biometric features will reflect the UK demographics. Results may be different with other population demographics. We note that our volunteers are probably more scientifically aware (and perhaps better able to follow instruction) than the general public.

Closed system — We shall enrol and test using the same system. Note that if the system would normally used several sensors, where there are considerable variations between sensors, the proposed protocol may not be appropriate.

A.1.3 Performance Measures

The proposed tests will measure the following aspects of performance (where applicable).

- Failure to enrol rate
- Failure to acquire rate
- Detection error trade-off graph (i.e. ROC)
- System false match and false non-match rates
- Penetration rate (where appropriate)
- Binning error rate (where appropriate)
- User throughput
- Matching algorithm throughput (reported with processing system used)
- Sensitivity of performance to (potentially problematic) changes in environment, population, or usage

A.2 Device setup

We allow vendor involvement during device set-up to help ensure that the systems are correctly installed and operating optimally.

A.2.1 Install systems & familiarisation

The complete system will be installed at the test site. Account will be taken of vendor recommendations regarding positioning, illumination, and background noise etc. in so far as these are realistically achievable in a general office/indoor environment. Threshold, image quality and other settings will be set in accordance with vendor advice.

A.2.2 Test sensitivity of performance to environment, population, usage

Some pre-trial tests will be carried out to determine environmental and other factors that may cause problems. This will be a limited investigation, mainly using the testing team. The aim is to determine:

- what potential problems exist,
- if these problems are controlled by the system,
- how significant the problems appear to be,
- whether we need to impose environmental or other controls to minimise the problem during the trials,
- what additional information we need to record to identify difficult subsets of volunteers during subsequent analyses.

Some of the potential sensitivities to test, and what may be done to analyse or control any problems are shown in the following table:

Technology	Effect to test	If effects seem significant
All	age, gender, template-ageing	Compare of error rates for different subsets of volunteers/attempts
All	lighting level & direction	Control lighting levels during trial
All	dirt/smears on sensor	Set policy for cleaning devices
All	movement during attempt	Provide appropriate instructions for volunteers
All	positioning	Provide appropriate instructions for volunteers
Fingerprint	Dry / cold / cracked / damp / wet fingers	Advise volunteers on improving fingerprint quality. Record temperature & humidity
Hand geometry	rings, plasters, etc.	Log attempts made with rings etc. Provide separate error rates for these cases
Iris, Face	Glasses	Record those who wear glasses/contact lenses Provide separate error rates for these cases

A.2.3 Set enrolment & transaction attempt policies

The enrolment policy will be set to deal with the problems identified, with the aim of achieving the greatest number of good enrolments.

The supervisors who will conduct enrolment will be trained and familiar with each system and its common problems.

A.2.4 Produce system information for volunteers.

For each system, a short description of how the system operates, and how it should be used will be prepared in consultation with the system vendor. This is to reduce the burden of describing full details of the systems at enrolment, and before later transaction attempts.

A.3 Volunteer crew

A call for volunteers will be issued. To encourage participation a small reward will be offered. If more than 200 people volunteer, participants will be selected at random from the volunteers.

Before enrolment participants will be informed of the purpose of the trials, what is required of them, and what information will be collected and stored. They will be asked to sign to give their consent to the collection of biometric images and information, and to confirm that they have not previously used any of the devices being tested. Age category and gender of participants will be recorded, together with any information found useful in identifying problem cases in the preliminary trials.

A.4 Enrolment

Each participant will attempt to enrol on each system under test. The order of enrolment on the devices being tested will be randomised. Only one set of equipment will be used for each system to avoid "channel" effects. Enrolment will be conducted using the enrolment functions of the supplied systems, and will supervised by a member of staff who had been trained for this purpose.

Enrolment images will be collected by the system. *(We use the word image to refer to the actual input signal; this may not strictly be an image in the case of non-optical devices. If the system is unable to record actual enrolment images, it may be possible to conduct the required analyses using the image templates.)*

Immediately after enrolment, several attempts will be made to check that the participant can be reliably verified. Advice to help users achieve successful verifications will be given if necessary. If they cannot be reliably verified this shall count as an enrolment failure.

If enrolment fails, one re-enrolment will generally be attempted. *(In some cases it may be clear that subsequent attempts must fail, for example if the volunteer does not have the required biometric feature. In such cases no re-enrolment attempt would be made. In other cases the enrolment failure may due to a clearly identifiable error which can easily be overcome, for example failures due to not following the proper enrolment process. In such cases more than two enrolment attempts might be made.)*

Some systems allow an "override" to register a poor quality image as an enrolment template in cases of difficulty; such features will not be used. Any problems with enrolment will be noted by the enrolment supervisor.

Cases where the enrolment template cannot be generated, or where all practice attempts fail, are

considered to be failed enrolments. In these cases, subsequent verification attempts are not required of the participant on the device in question. Data from failed enrolments will be removed from the enrolment database and will not be used in analysing false match or false non-match error rates.

A.5 Test data collection

Volunteers will make two sets of transactions, at approximately one and two months after enrolment. On each occasion they should make (at least) three attempts. This will allow direct calculation of "best of three attempt" rejection rates, and can also reveal whether some users are much more error prone than others.

Attempts will be largely unsupervised, but there will be a supervisor on hand to help in case of difficulty. Users may observe attempts made by others, but will not be allowed to make practice attempts (apart from those they made as part of enrolment). This is to ensure that only the genuine transactions are recorded. It is also the case that practice attempts could artificially lower the failure to acquire rate. Additional attempts (i.e. after the required 3 attempts) may be made. It is important to ensure that no attempt is made against the identity of another participant. If a volunteer is keen to see a rejection, it is permitted that they may make an attempt against a non-participating identity. Again, such attempts should not take place immediately prior to their "genuine" attempts.

The order of using the devices will be random across users, and not correlated with the order of use on other occasions. Users will be asked to try to make these attempts successful, and to refrain from making bogus attempts (e.g. using the wrong finger on fingerprint devices, or pulling faces on face recognition devices). As an incentive to obey these instructions, payment for participation is linked to making the required number of good attempts.

Attempt images will be collected by the system, and user details, date and time logged. To avoid data entry errors, user identity will be entered using a swipe card or smart card if possible.

The supervisor will note any problems that arise during the test data collection, so that non-genuine attempts are not included in the analyses. Details of such attempts should be reported.

A.6 Analysis & Reporting

A.6.1 Data collected

Collected by system

- event logs as collected automatically by each system
- images of all test attempts
- enrolment database
- enrolment images

Collected by supervisor:

- log of failed enrolments
- log of (non-genuine) attempts to be excluded
- user details, e.g. age, sex *(The relevant user information to collect will depend on the sensitivities identified in preliminary tests.)*

A.6.2 Failure to enrol rate

The proportion of volunteers failing to obtain an enrolment (of sufficient quality) will be reported along with the enrolment policy and any quality threshold settings.

A.6.3 Failure to acquire rate

The proportion of attempts resulting in a failure to acquire error, averaged across all enrolees, will be reported together with any quality settings.

A.6.4 Detection Error Trade-off plot

The following enrolments and attempts will be excluded when deriving false match and false non-match rates:

- enrolment templates associated with any failed enrolment,
- attempts made on the day of enrolment,
- attempts made by non-enrolees, non participants in the trials, or by participants not completing the trials,
- attempts noted as a non-genuine in the supervisor log book,
- attempts resulting in failure to acquire errors
- extra attempts (4th or later attempt) made by any user on any day. (This is to ensure there is no imbalance due to some users making many more attempts than others).

Distance scores for genuine transactions may have been generated "live" during data collection. Otherwise we use vendor provided software for generating these distance scores off-line from the collected images.

Some systems do not generate distance scores, but can operate at various security settings. In such cases the attempts will be analysed using off-line software at different security settings. In such cases we consider the distance measure to be the strictest security setting at which the attempt results in a match.

We use the supplied software to generate impostor attempt distance scores, by comparing each attempt against the templates for all other enrolees. In the case of non-independent templates it will be necessary to re-enrol all enrolees apart from the one who made the attempt.

The Detection Error Trade-off curve plots the proportion of genuine transaction scores exceeding the matching threshold *(we assume that low scores imply a good match and high scores a poor match)* against the proportion of impostor transaction scores below that threshold, as the threshold varies.

A.6.5 System false accept & false reject rates

In cases where the usual decision policy of the system is not based on a single attempt-template comparison, we give the false accept rate and false reject rate using the actual decision policy, at the system settings used.

A.6.6 Penetration rate & binning error rate.

If a binning algorithm is used, we need to know the "bin" for each template and each genuine attempt.

The penetration rate is the average proportion of the database that would need to be searched if the system were operating in identification mode, where the average is taken over all genuine attempts. This can be estimated if we know the number of attempts in each bin, and which bins are compared against each other. A bin error occurs when an attempt is placed in a bin which is not compared with the correct bin for the biometric entity used, and hence will fail to match.

A.6.7 User throughput & matching algorithm throughput.

User throughput measures the elapsed time of a single transaction. All attempts are to be timed at a consistent point during the transaction (e.g. the start time). The difference in times between the first and second, or second and third attempts, by an individual on one day approximates the total transaction time. This assumes that the 2^{nd} and 3^{rd} attempts immediately follow the first attempt.

We can time the off-line calculation of impostor distance scores and compute the number of template-attempt matches performed to obtain the matching algorithm throughput. As the time is hardware dependent, the system used should be specified with the resulting throughput rate.

A.6.8 Sensitivity to population & environment

Where there appear to be differences in performance due to population, environment or usage changes (see section A.2.2), in some cases we will be able to assess the affects on performance by analysing subsets of the attempts. For example we can compare the error rates for different age categories, for people with glasses against those without glasses etc. We can also compare the error rates for attempts one month after enrolment with those two months after enrolment (and with error rates immediately after enrolment) to see the effects of template ageing. Comparing the error rates for the first attempt with those for the second and third attempt made on any occasion may show possible improvement in performance due to habituation.

APPENDIX B. CONSENT FORM & ENROLLMENT DATA SHEET

Name

Laboratory

Phone

Email

TRIAL ID

□ Male □ Female

Age:
□ 18-24 □ 25-34 □ 35-44
□ 45-54 □ 55-64 □ 65+

Other
□ Glasses
□ Contact Lenses

I am happy to participate in these trials. I consent to my biometric data being collected during the trial and stored electronically.
I permit use of this data for the purposes of evaluating performance of biometric devices, by the National Physical Laboratory, the Government Biometrics Working Group, and by the manufacturers of the devices under test. *[Data made available outside NPL will consist of only the collected biometric data, and the personal details in the box above.]*

Signed:

System	Enrolled OK	Problems / Notes
Face		
Iris		
Vein		
Hand Geometry		
Voice		
Fingerprint Optical Reader		
Fingerprint Chip Reader		

Return for recognition attempts on:

APPENDIX C. VERIFICATION DATA SHEET

«FirstName» «LastName»

TRIAL ID **«PIN»**

Please make **3** attempts on each system

Try your best to be correctly recognised - Do **NOT** try and trick the systems

System & Brief Instructions — Comments

VEIN

1. Place **RIGHT** hand on pad □
2. Click button under your fingers to take image □
3. Enter **«PIN»** on keypad, check on screen, then press * □

FINGERPRINT – OPTICAL SENSOR

Enter **«PIN»** in ID box – Check this before proceeding □

1. Press VERIFY to make a verification □
2. Use **RIGHT INDEX** finger □

FACE

Enter **«PIN»** and check your image displayed □

1. Press START VERIFICATION □
2. Stand on marked spot and face camera □

IRIS

1. *If needed click START or* 🔍 *to show ID entry box* □
2. Enter **«PIN»** and click OK □
3. Use **RIGHT** eye □

FINGERPRINT – CHIP SENSOR

Enter **«PIN»** in ID box – Check this before proceeding □

1. Press START to commence verification □
2. Use **RIGHT INDEX** finger □

HAND GEOMETRY

1. Enter **«PIN»** and press "#YES" key □
2. Use **RIGHT** hand □

□

VOICE

Dial 6901 and follow instructions □

□

□

For impersonation attempts use ID **«PIN-impostor»** □

□

□

Options for payment

□ (NPLML Staff) Please make payment with my November salary
My staff number is:

□ (non NPLML staff) Please send a cheque to:

□ Please donate my payment to the NPL Sports Club Pavilion Rebuild Fund

□ Please donate my payment to Save the Children

□ I wish to waive payment

Signed:

APPENDIX D. SIGNIFICANCE OF USER & ATTEMPT VARIATIONS

55. Attempts can be categorised by:

a. Whether made at the enrolment visit or at the second or third visit by a volunteer;

b. The gender of the volunteer;

c. The age of the volunteer;

d. Whether the volunteer was wearing spectacles in the case of Face and Iris systems;

e. The length of the user's pass-phrase in the case of the Voice system.

Performance differences between these subsets have been analysed, and are reported for each system in Part II.

56. To determine the statistical significance of any observed differences (i.e. the probability of the difference being attributable to sampling error) a simple χ^2 test was used.

a. The number of correct and failed verifications at the default threshold were counted for each class. E.g.

Observed	Under 35	Over 34	Combined
FRR	3.9%	11.5%	8.3%
Rejected	29	116	145
Verified	710	893	1603
Total	739	1009	1748

b. If there were no difference between classes the combined error rate would apply to both classes.

Expected	Under 35	Over 34	Combined
FRR	8.3%	8.3%	8.3%
Rejected	61.3	83.7	145
Verified	677.7	925.3	1603
Total	739	1009	1748

Observed-Expected		
	-32.3	32.3
	32.3	-32.3

c. The test statistic used is

$$\sum \frac{(Obs.\ -\ Exp.)^2}{Exp.} = (32.3 - ½)^2 \left(\frac{1}{61.3} + \frac{1}{83.7} + \frac{1}{677.7} + \frac{1}{925.3} \right) = 31.17$$

(The subtraction of ½ represents the correction for continuity; and is used because the observed values can only take integer values.)

d. If all attempt results are statistically independent, the test statistic would follow a χ^2 distribution (with 1 degree of freedom). In the example case χ^2 exceeds 31.17 with probability less than 0.01%. However, this overstates the significance since there are dependencies between each attempt made by the same user.

e. If all *N* attempts by any user had the same result (the maximum correlation possible), while attempts by different users are independent, then the test statistic divided by *N* follows a χ^2 distribution (with 1 degree of freedom). In the example case, if there are 9 attempts per user, the probability of χ^2 exceeding $\frac{31.17}{9} = 3.46$ is 6.28%. This understates the significance, since user attempts are not correlated to such an extent.

f. Both results are shown, the true significance lies between these values.

SANDIA REPORT

SAND91–0276 • UC–906
Unlimited Release
Printed June 1991

A Performance Evaluation of Biometric Identification Devices

James P. Holmes, Larry J. Wright, Russell L. Maxwell

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550
for the United States Department of Energy
under Contract DE-AC04-76DP00789

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

NOTICE: This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors, or their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, any agency thereof or any of their contractors or subcontractors. The views and opinions expressed herein do not necessarily state or reflect those of the United States Government, any agency thereof or any of their contractors.

Printed in the United States of America. This report has been reproduced directly from the best available copy.

Available to DOE and DOE contractors from
Office of Scientific and Technical Information
PO Box 62
Oak Ridge, TN 37831

Prices available from (615) 576-8401, FTS 626-8401

Available to the public from
National Technical Information Service
US Department of Commerce
5285 Port Royal Rd
Springfield, VA 22161

NTIS price codes
Printed copy: A03
Microfiche copy: A01

SAND91-0276
Unlimited Release
Printed June 1991

Distribution
Category UC-906

A Performance Evaluation of Biometric Identification Devices

James P. Holmes and Larry J. Wright
Facility Systems Engineering Division

Russell L. Maxwell
Systems Engineering Division
Sandia National Laboratories
Albuquerque, NM 87185

Abstract

When an individual requests access to a restricted area, his identity must be verified. This identity verification process has traditionally been performed manually by a person responsible for maintaining the security of the restricted area. In the last few years, biometric identification devices have been built that automatically perform this identity verification. A biometric identification device automatically verifies a person's identity from measuring a physical feature or repeatable action of the individual. A reference measurement of the biometric is obtained when the individual is enrolled on the device. Subsequent verifications are made by comparing the submitted biometric feature against the reference sample. Sandia National Laboratories has been evaluating the relative performance of several biometric identification devices by using volunteer test subjects. Sandia testing methods and results are discussed.

Contents

Figures

A Performance Evaluation of Biometric Identification Devices

Introduction

In many applications, the current generation of biometric identification devices offers cost and performance advantages over manual security procedures. Some of these applications are: physical access control at portals, computer access control at terminals, and telephone access control at central switching locations. An installation may have a single, stand-alone verifier which controls a single access point, or it may have a large networked system which consists of many verifiers, monitored and controlled by one or more central security sites.

Establishing how well a biometric identification device operates should be an important consideration in any security application. Performance data, however, is neither easy to obtain nor to interpret. Because there are no test standards yet to test against, test methods must be well documented. To measure its theoretical performance limit, a verifier could be tested in an ideal environment with robotic simulation of biometric data. The results of such a test would probably differ greatly from its real-world performance. The human element greatly affects the performance of any identity verifier. Environmental factors such as noise, light, electromagnetic radiation, moisture, dust, and temperature could also affect the verifier's performance.

Sandia began its latest verifier test series in November, 1989. Nearly 100 volunteers attempted many verifications on each machine. Environmental conditions were nominal, as the tests were all performed in a laboratory room for the convenience of the test volunteers. The biometric features used by the suppliers of the latest generation of verifiers in the Sandia tests include:

1. Fingerprint by Identix, Inc.[1]
2. Hand geometry by Recognition Systems, Inc.[2]
3. Signature dynamics by Capital Security Systems, Inc. Sign/On Operations.[3] (Formerly Autosig Systems, Inc.)
4. Retinal vascular pattern by EyeDentify, Inc.[4]
5. Voice by Alpha Microsystems, Inc.[5]
6. Voice by International Electronics, Inc.[6] (Formerly ECCO, Inc.)

General Test Description

Statistics have been compiled on false-rejection error rates and false-acceptance error rates for each verifier. The error rates are described as a percentage of occurrence per verification attempt. "Attempt" is used in this report to describe one cycle of an individual using a verifier as proof of being a validly enrolled user (enrollee). Most verifiers allow more than one try per attempt. "Try" describes a single presentation of an individual's biometric sample to the verifier for measurement. "False-rejection" is the rejection of an enrollee who makes an honest attempt to be verified. A false-rejection error is also called a Type I error. "False-acceptance" is the acceptance of an imposter as an enrollee. A false-acceptance error is also called a Type II error. False-acceptance attempts are passive; these are cases where the imposter submits his own natural biometric, rather than a simulated or reproduced biometric of the enrollee whose identity is claimed. To sum up:

false-rejection error = Type I error = rejection of an enrollee
false-acceptance error = Type II error = acceptance of an imposter.

Each verifier in the test is a commercially available unit. Because of the differences in these units and because we needed an equitable basis of comparison, we attempted to modify some of the units. One goal was to have each verifier report a final decision score for every verification try. Although the manufacturers were generally cooperative, it was not possible to achieve all our goals within the time and budget constraints of the testing. The Identix fingerprint verifier did not generate score data at all. The Capital Security signature verifier scores were not directly related to the accept or reject decision because of some additional decision making after the scores were generated. If a biometric testing standard ever becomes a reality, it should include a section on score data generation and reporting.

Software and/or firmware modifications were made by the manufacturer on some units to allow Sandia to collect the desired test data. All verifiers and specified modifications were purchased by Sandia. Where possible, each verifier was set up in accordance with the manufacturer's recommendations. In most cases, a representative from each manufacturer visited the testing laboratory to verify that his device was properly set up. Where problems were pointed out, attempts were made to rectify them. Some attempts were more successful than others within the limits of our test facility resources.

Testing and Training

The verifier tests at Sandia were conducted in an office-like environment; volunteers were Sandia employees and contractors. A single laboratory room contained all of the verifiers. Each volunteer user was enrolled and trained on all verifiers. There were both male and female volunteers and the efforts of both were valuable to this study. However, for the purpose of simplifying the text, we will use the term "his" rather than "his/her."

There is a learning curve for the proper use of a biometric identification device. As a user becomes more familiar with a verifier, his false-rejection rate decreases. This curve differs for individual users and verifiers. This learning effect was minimized for the Sandia testing by training the individuals before the test, by monitoring their performance, and by eliminating the first few weeks of test data in the results. A number of users were reenrolled on verifiers where there was indication of below-average performance. The transactions prior to the reenrollment were not included in the test results. Some manufacturers recommend that the users be reenrolled as many times as necessary to produce the best enrollment scores. We tended to limit reenrollments to known problem cases due to the relatively short duration of our test, and also to give the verifiers more nearly equal treatment. Verifiers on which it is more difficult to enroll would therefore tend to give somewhat less than optimum performance in our test. This effect is less significant for verifiers which modify the stored reference template by averaging in the biometric samples from successful verification attempts. The EyeDentify and the Identix units are the two tested verifiers that do not modify the reference template.

Other known errors were identified for removal by instructing the users to note on a real-time hardcopy printout any transaction where he made a mistake, or was "experimenting" and did not feel that the verification attempt was valid. A similar method was used to identify invalid transactions on the false-acceptance test. Many hours were devoted to identifying and removing invalid transactions from the data files. There is no doubt, however, that a small number of unrecognized errors remain in the data.

The problem of selecting a representative test user group is most vexing when testing biometric identification devices. While the differences in physiological and behavioral properties of humans are the bases for the devices, these same differences can bias test results between test user groups. The best solution to this problem seems to be to use many users and to make numerous attempts. The larger the numbers, the more likely the results will represent true performance values. Relative performance must be measured against absolute performance. A verifier's relative performance within a user group is generally easier to defend than is the absolute performance.

No extraordinary incentives were offered the volunteer users who performed the tests. Treats in the test room were used to tempt users to remain active. A drawing for a free lunch was offered to the regular users. About 80 of the 100 enrolled users remained fairly active in the tests. Work and travel schedules accounted for the loss of some users. Others simply became disinterested.

First Test Series: False-Rejection Testing

- users attempted verification on each machine many times
- test period was three months long
- users were allowed up to three tries per verification attempt.

Second Test Series:
Passive False-Acceptance Testing

- user submitted the personal identification number (PIN) of other users
- user then submitted his own natural biometric
- users were allowed up to three tries per verification attempt.

Data Processing

The first step in the data processing was to remove the invalid transactions that were noted on the printed data logs generated at each verifier. The data files were then processed to remove incomplete records and to convert the data to a common format. The data was sorted into individual user groups. Records from users making less than six transactions were deleted. User data obtained prior to user group reenrollment on a verifier was also deleted.

A verifier can usually be configured to accept up to three "tries" on a verification attempt. A "try" is one cycle of the user presenting his biometric to the verifier for measurement. To simulate verifier performance on one-, two-, and three-try attempt configurations, our users were instructed to try a third time if verification was not successful on the first or second try. Recorded time- of-day information allowed each score to be identified as either a first, second, or third try.

Up to three tries in a five-minute time interval were considered one verification attempt. Additional tries within this interval were ignored. Tries beyond the five-minute interval were considered another verification attempt. At any given threshold value, a score will produce either an accept or a reject. An accept on the first try is counted as an accept for one-, two-, and three-try configurations. An accept on the second try is counted as a reject on a one-try configuration and an accept on a two and three-try configuration. An accept on the third try is counted as a reject on a one and two-try configuration and an accept on a three-try configuration. Three rejects are counted as a reject on all three configurations. To sum up:

	Configuration Test Result		
Verification Action	one-try	two-try	three-try
Accept on first try	accept	accept	accept
Accept on second try	reject	accept	accept
Accept on third try	reject	reject	accept
No accepts with three tries	reject	reject	reject
No accepts with less than three tries	only actual rejects counted		

The false-reject error rate is the ratio of false-rejects to total attempts at verification. A false reject will be represented as "FR" and is reported in this document as a percentage value. Where transaction score data was available, the FR was calculated for each user for one-try, two-try, and three-try verifier configurations over a range of possible thresholds. The scores were used to find the number of errors that would have occurred had the verifier test threshold been set at each of the possible thresholds.

The false-accept error-rate is the ratio of false-acceptances to total imposter attempts. It will be represented as "FA" and was calculated for each user over the range of possible thresholds and presented as a percentage value.

The FR and FA for each verifier was calculated by averaging the user-percent error rates at each threshold value selected. The FA and FR error-rate curves are shown in the next section, entitled "Results of the Testing." Where possible, error-rate curves are shown for one-try, two-try, and three-try verification attempts. These curves exhibit two general characteristics. One characteristic is the non-zero value of the crossover point of the FA and FR curves. A second characteristic is the trend toward a lower rejection rate as the number of tries at verification increases. Both these characteristics force some tradeoffs in using these verifiers.

The non-zero error value at the crossover point means that there is no threshold setting where both the FA and FR error-rates are zero. The user must choose a threshold setting to fit the application. As the threshold is moved toward tighter security (higher rejection error rates), both imposters and valid users face higher rejection rates. Both are rejected less often when the threshold is moved toward lower security. The point at which the FA and FR curves cross over is referred to as the equal-error setting. This single-value error rate has been accepted as a convenient value to describe the performance of a verifier in the Federal Information Processing Standards Publication (FIPS PUB) 83. This and other single-value criteria have been used to characterize verifier performance, but no single value can provide much insight into the true performance capability of any verifier. The FA and FR error-rate curves provide much more insight into performance and should be examined for suitability in any security application.

Multiple-try attempts at verification can improve the performance of some biometric verifiers. The rejection rate for valid users generally decreases faster than the rejection rate for imposters, as more verification tries are allowed. Valid users are generally rejected because of inconsistent presentations of their biometric input. Additional tries allow the valid user to correct the inconsistencies and to generate an acceptable input that matches the reference template. Imposters are generally rejected because their biometric is not close enough to the reference to be accepted. Additional tries increase the chances of imposter acceptance if the biometric differences are small enough to be masked by the inconsistent user inputs and by tolerant threshold settings.

The Identix fingerprint verifier we tested did not have a customer adjustable system threshold. While individual thresholds could be adjusted, we did not get any test data at other than the factory-set threshold. The other verifiers tested did provide test score data, but the Capital Security signature verifier scores could not be used to generate error-rate curves because of a second calculation that it uses to make the accept or reject decision.

Our transaction time results were obtained by timing the users from when they touched the verifier until the verification attempt verdict was given. The users were not told that they were being timed. We feel that the results reflect verification times that would be typical in an actual installation. These times are substantially longer than the minimum times of a skilled user in a hurry.

Results of the Testing

Alpha Microsystems Results

Alpha Microsystems of Santa Ana, California bought out Voxtron and is now selling an updated system called Ver-A-Tel. This voice verification system makes use of a personal computer (PC), which contains the speech board hardware and the software programs. User terminals are touch-tone telephones. The Ver-A-Tel system is offered in two similar versions: the telephone intercept system (TIS) and the remote-access system (RACS). We tested the public TIS version, but not the direct-line RACS version.

The software supplied with the system provides the necessary management functions to enroll and delete users, to configure the system parameters, to display activities and alarms and to generate reports. Because this password-protected software is menu driven, it allows the security manager to select options from the screen and to fill in the blanks to configure the system. A supplied user's guide provides any additional information that might be needed.

Users were enrolled on the same touch-tone telephone that was later used to access the system. Prior

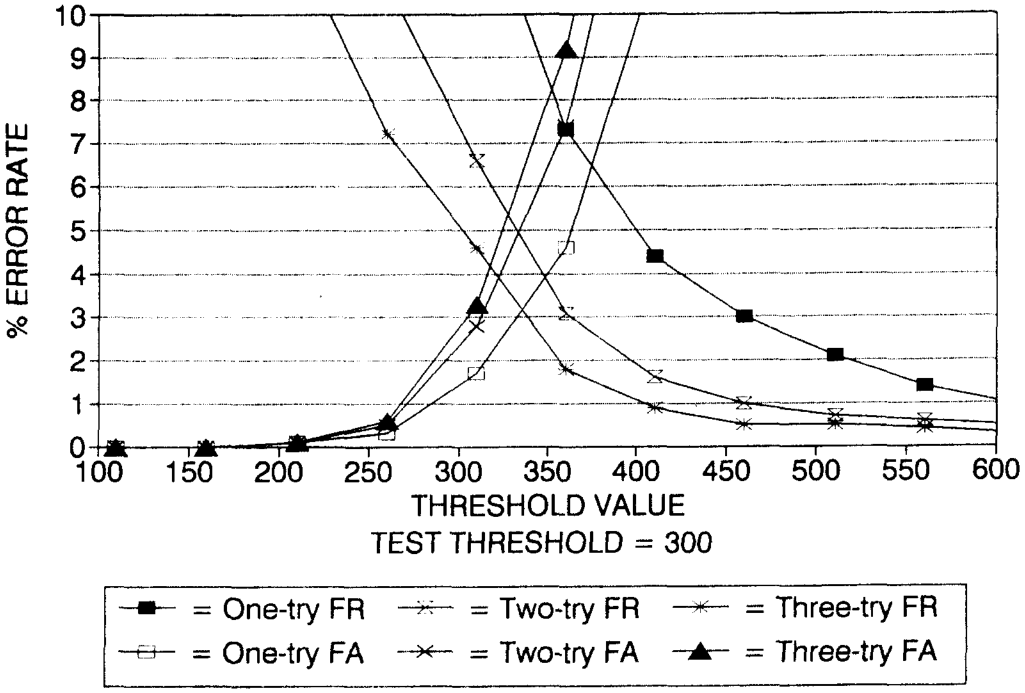


Figure 1. Alpha Microsystems Voice Verifer

Capital Security Systems, Inc. Results

Capital Security Systems, Inc. of Columbia, MD purchased the signature dynamics verifier line from Autosig Systems, Inc. This verifier consists of a user interface tablet and a controller which is designed to integrate into a host-computer access control system. The Capital security system offers products for both physical entry control and data access control. The user interface is similar for both applications. A variety of hardware and software options allow the system to function in applications from stand-alone protection of a single entrance to networked, host-based systems.

The user interface is a desk top tablet (~9 3/8 by 11 inches) that incorporates a digitizer tablet, a magnetic stripe card reader, and a tethered pen. The digitizer tablet (~2 1/2 by 5 inches) is the area where the user actually signs his name with the tethered pen. The system measures the dynamics of the user's signature to form the biometric template for enrollment and verification.

The controller can function as a stand-alone device with the user interface and door interface hardware, but must be connected to a computer for programming and user enrollment. An IBM PC or a higher class, compatible computer with a serial port and a floppy disk drive can be used. The computer class must match the controller interface requirement.

Software is provided to allow the security manager to configure the system and to enroll users. A menu-driven program provides the manager with the necessary options. Before a user can be enrolled, a user data record must be generated in the user data file. The manager selects the options and fills in the blanks to generate the record. For the model tested, a magnetic stripe card was required for ID entry. It was coded with the user's PIN and provided to the user for verifiers in this test series.

To enroll, the user must follow the illuminated prompts on the interface tablet. First the user PIN is entered with a swipe of his magnetic stripe card through the card reader. Next, the user is prompted to alternately sign on and wait while the system generates a template. Finally, the user is prompted when the sequence is complete. It normally takes two signatures and one verification signature to enroll. The signature must be within the marked digitizer pad area, using the tethered pen. The system can be used with a regular ball-point pen tip and a stick-on paper sheet over the pad, or with an inert, inkless pen tip system directly on the digitizer pad.

Verification is similar to enrollment. The user PIN is entered with the magnetic card and the user signs his name on the digitizer pad with the tethered

to enrollment, the security manager created a record for each user and each was assigned a unique PIN. An optional secret enrollment passcode, to prevent an imposter from enrolling in place of the authorized user, was not tested.

A phrase is required for enrollment and subsequent verification. The security manager can select from a number of standard phrases on the menu display; from this selection, he can allow the user to make up his own phrase. There are some restrictions on user-selected phrases, such as the minimum and maximum length and the optimum number of syllables. These options are discusssed in the User's Guide which is supplied with the system.

Voice verifier manufacturers are quick to point out that security is enhanced if each user has a secret phrase. These manufacturers, however, do not address the problem of how to keep a phrase secret that must be uttered into a microphone. On the other hand, it is certainly less likely that an imposter would be accepted if he does not know the proper phrase. It is even plausible that a valid user could have a lower false-reject error rate with a chosen phrase that was more natural or familiar to him. The objective of our test was to measure the ability of the system to verify users based solely on their biometric properties. Thus, we assigned the same phrase to all users.

To enroll, a user calls the verifier telephone number. The system answers and instructs the user to enter his PIN on the touch-tone keypad. If the system finds that the PIN belongs to someone who is not yet enrolled, it tells the user what he must do to enroll. This may include an instruction to enter the proper enrollment passcode on the keypad. The user is instructed to say the verification phrase a number of times. The system performs checks on each response and may prompt the user to be more consistent and to repeat the phrase again. When the system parameters for a successful enrollment are met, the system so informs the user. A user template is generated from the enrollment data and is stored for future verification of the user's identity. The system may tell the user that the enrollment was better than most. This indicates that the enrollment phrases were very consistent. It is also possible for the user to fail. In this case, the user is told to practice and try again. The security manager can also check the enrollment scores to get a measure of the enrollment performance. Individual accept or reject thresholds can be set by the security manager to compensate for differences in user performance. This adjustment is made (plus or minus) to the system threshold setting.

On verification attempts, an enrolled user's PIN is recognized by the system and is used to retrieve the proper template from the enrollment database for verification. The user is then prompted to say the phrase for verification. Optionally, the new phrase data may be averaged into the stored template to update the template each time the verification is successful. In time, if the user becomes more consistent and the verification scores improve, the security manager may opt to adjust the user threshold value to a more secure value. Experienced users generally skip the voice prompts because a preceding tone signals the user that he can go ahead without further delay if he does not need the voice instruction.

The time information given for the Alpha Microsystems voice verifier is different from other verifiers because it includes dialing a 5-digit telephone number and waiting for the verifier to answer. We included this scenario because the telephone access method was also used in our test verifier. Other access methods may result in different transaction times. The minimum time of ~13 seconds was necessary to perform the following steps:

- lift the phone and dial a 5-digit extension
- wait for the voice system to answer and generate the tone prompts (without waiting for the subsequent voice prompts)
- enter a 4-digit PIN on the phone keypad
- say "yankee doodle dandy"
- be verified.

The average user in our test took ~19.5 seconds for a complete verification. This average includes multiple-try attempts when this was required by the system.

The crossover point where the one-try false-reject and the one-try false-accept curves are equal has an error rate of 6.5% at a threshold value of ~375. At the test threshold setting of 300, the three-try, false-reject error rate was 5.1% and the three-try, false-accept error rate was 2.8%.

There were 5434 transactions in the false-reject test and 2990 transactions in the false-accept test. The results of these tests are shown in Figure 1.

pen. A prompt then tells the user whether the verification was successful or if another signature try is necessary. Two tries are usually allowed. Each successful verification is averaged into the reference template to allow the system to accommodate long-term changes in the user signature. This averaging can be inhibited by the security manager.

Imposter testing consisted of each imposter entering PINs by using the magnetic stripe badges of all other users. The imposter knew the real user's name from the badge, but did not have a sample of the user's signature. The imposter was free to try to sign the actual user's name. As a matter of interest, we attempted some verifications by tracing over valid signatures. The scores were generally much worse than other imposter attempts because of the importance of the signature dynamics in verification. None of the tracing attempts were included in our test results.

The time to perform a verification depends in part on how long a user takes to sign his name. Our users averaged ~15 seconds to verify on the Capital Security system; this time includes PIN entry via a swipe card reader and some multiple-try attempts as required by the system. The minimum time observed was ~12 seconds.

Error-rate curves are not shown because the Capital Security accept or reject decision process is more than just a function of the transaction score. A second decision calculation is performed on all tries that produce a score between 16,000 and the verifier threshold setting. The threshold was set at 21,000 for our test.

All false-accept and false-reject error rates obtained were from a count of the errors at the operational threshold:

False-Reject Error Rate	Percentage
three-try	2.06%
two-try	2.10%
one-try	9.10%

False-Accept Error Rate	Percentage
three-try	0.70%
two-try	0.58%
one-try	0.43%

The Capital Security is usually set up for two tries.

There were 3106 transactions in the false-reject test and 6727 transactions in the false-accept test. The Capital Security system error-rates are shown in Figure 2.

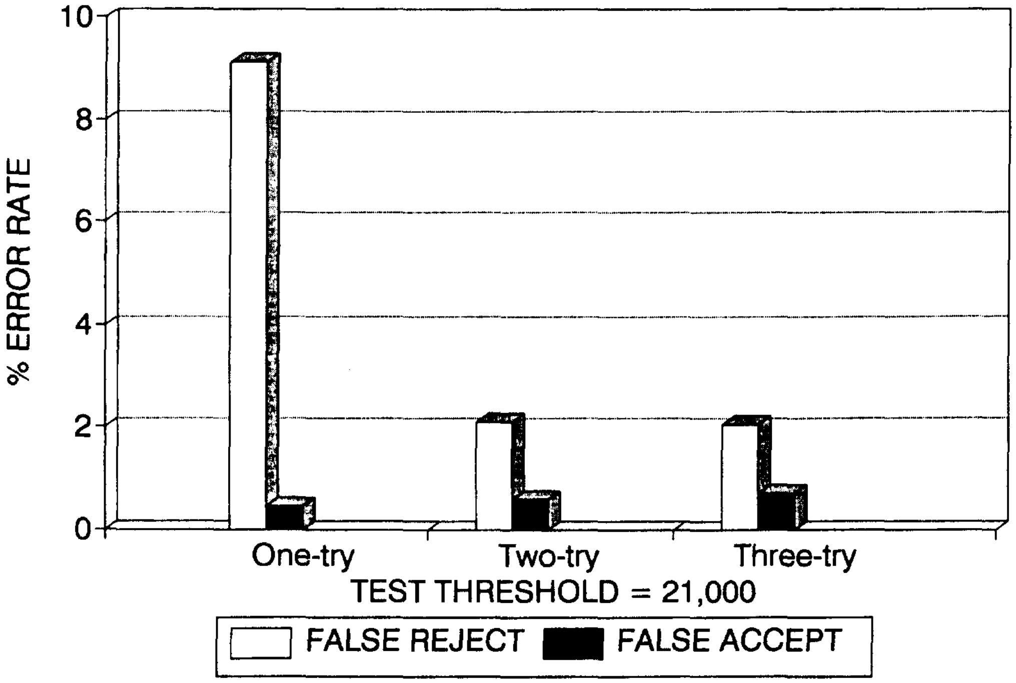


Figure 2. Capital Security Signature Dynamics

International Electronics (ECCO VoiceKey) Results

International Electronics, Inc. of Needham Heights, MA purchased ECCO Industries, Inc. of Danvers, MA and now markets the ECCO VoiceKey. The VoiceKey is a self-contained, wall-mounted user interface that communicates with a controller over a copper wire cable. The user interface contains an alphanumeric display, keypad, a microphone, an audible beeper, and indicator lights. Keys, displays, etc. allow all necessary functions to be performed at the user interface. Some of these functions are user enrollment and system management.

The user interface and controller can operate in a stand-alone mode to provide security at a single entry point, or can be networked through a network controller to other units in a security system. A VoiceKey network has a master voice reader and slave voice readers. The master voice reader is normally used for all enrollments and programming, which are then downloaded to the slave readers. Enrollment and programming can be performed at any slave, but it cannot be downloaded to any other reader. A printing capability allows audit information to be output to a printer connected to the controller of the master reader.

User enrollment is normally performed at the master voice reader by a security manager who is authorized to enter the programming mode. This authorization must be verified by voice before the programming mode can be entered. Programming is accomplished by keypad key inputs. Message displays and lights provide feedback to the programmer as the program steps are entered. A supplied programming manual provides complete information on the programming procedures. A user program allows new users to be added. This option requires the security manager to enter a unique PIN to access zone data and to enter the user authorization level for the new user. The reader then displays a series of message and colored-light prompts for the new user to initiate the sequence and to say his password several times. A red/green light display at the end of the enrollment sequence informs the new user of failure/success in enrolling. (This frustrates color-blind users who cannot distinguish between the red and green colors.) If successful, the new user can practice using his password as desired. Each successful verification causes the user's template to be modified by the new input.

Verification can be accomplished in ~5 seconds. Users averaged ~6.6 seconds per one-try attempt; in this time, they were able to enter a 4-digit PIN on the keypad and to utter the single password.

The crossover point where the one-try, false-reject curve and the one-try, false-accept curve are equal has an error-rate of 8.2% at a threshold value of 100. Only one-try, false-accept data was obtained for the VoiceKey verifier. There are three user thresholds available for the VoiceKey verifier. Security level 1 is a threshold of 75, level 2 is a threshold of 65 and level 3 is a threshold of 55. At the test threshold setting of 75, the three-try, false-reject error rate is ~4.3%, and the one-try false-accept error-rate is ~0.9%.

Voice verifier manufacturers are quick to point out that security is enhanced if each user has a secret phrase. These manufacturers, however, do not address the problem of how to keep a phrase secret that must be uttered into a microphone. On the other hand, it is certainly less likely that an imposter would be accepted if he does not know the proper phrase. It is even plausible that a valid user could have a lower false-reject error rate with a chosen phrase that was more natural or familiar to him. The objective of our test was to measure the ability of the system to verify users based solely on their biometric properties. Thus, we assigned the same phrase to all users.

We experienced high, false-rejection error rates with the assigned password. The manufacturer's representative suggested that each user be allowed to choose a password familiar or comfortable to him. We gave additional training and reenrolled ~15% of the users that were experiencing the most trouble with verification. On reenrollment, the users could choose from several suggested words. Some were allowed to select a word of their choice. This effort did produce better verification scores for many of the individuals after they were reenrolled. We were unable to correlate the effect of reenrollment on the long-term, false-rejection error rates. Several variables remain in the verification process. As the user becomes more familiar with a password, he would be expected to get more consistent in its use. The user's reference template is also modified for each successful verification, and thus should improve the verification scores of consistent users. An analysis of entire user group performance before and after reenrollment, however, did not show a significant improvement over time.

There were 4871 transactions in the false-reject test and 3270 transactions in the false-accept test. The graphical results of these tests are shown in Figure 3.

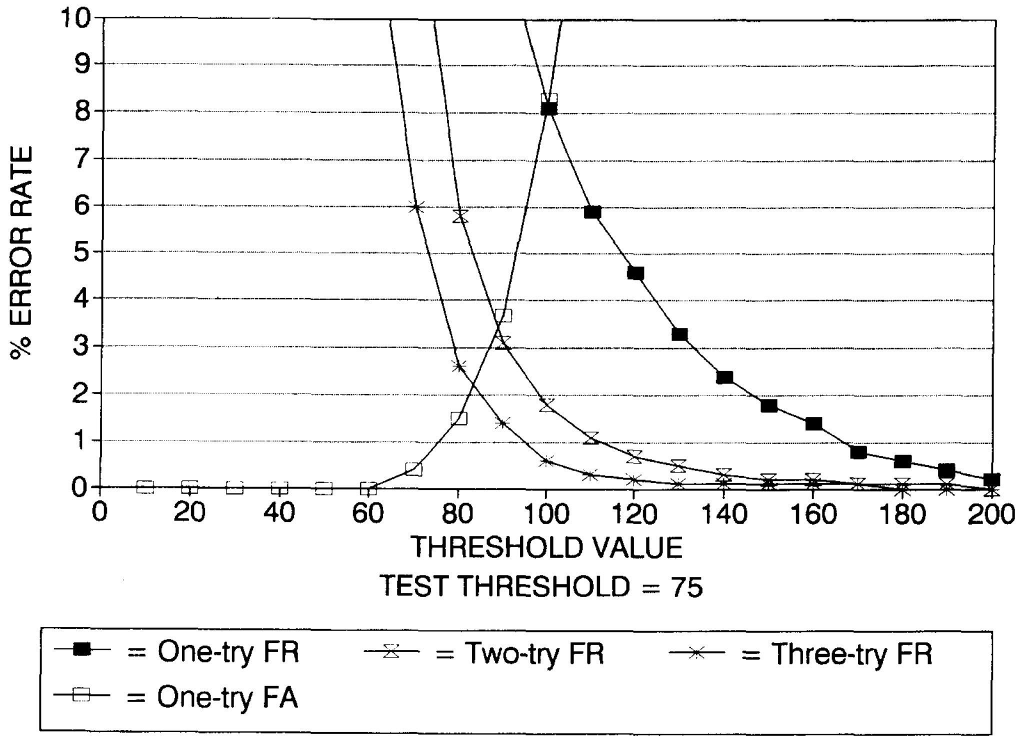


Figure 3. International Electronics Voice Verifier

EyeDentify Verify Mode Results

The retinal pattern verifier in this test series was Model 8.5, manufactured by EyeDentify, Inc. of Portland, Oregon. The verifier includes a reader and a controller. The reader contains an aperture where the user looks to align his eye with an optical target, which appears as a series of circles. As the user moves his eye around, the circles become more or less concentric. Proper alignment is achieved when the circles appear concentric and the user is looking at the center of the circles. The reader also contains a display, a keypad, and an insertion reader for magnetic stripe cards. A copper cable connects the reader to a controller box that contains processing and interface electronics.

The controller can function as a stand-alone device with the user interface and door interface hardware, but must be connected to a computer for programming and user enrollment.

Two readers were tested. Reader 1 was set up to operate in the verify mode using a PIN entered via an insertion card. Reader 2 was set up to operate in the "hands-free" recognize mode. The results for Reader 1 are discussed in this section, and the results for Reader 2 are discussed in the following section entitled: "EyeDentify Recognize Mode Results."

The software allows the security manager to configure the system and to enroll users. A menu-driven program provides the manager with necessary options. Before a user can be enrolled, a user data record must be generated in the user data file. The manager selects the options and fills in the blanks to generate the record. Once the record generation in the enrollment sequence is completed, a message instructs the user to enroll. The new user then aligns the optical target in the viewing aperture and presses the "ENTER" key on the keypad to initiate the eye-scan sequence. Each subsequent scan generates a score on the computer display and allows the security manager to accept or reject it. The user template is generated from an average of the accepted scans on enrollment. This template is not modified by subsequent verifications, so it is important to take some care during enrollment and not to accept scores below the mid 70s. It is not difficult for most properly instructed users to score above 80.

The user's PIN must be entered for verification. The EyeDentify 8.5 allows either manual entry on the keypad or automatic entry by using the card reader. Our tests used the card entry option. The average time for our users to perform the verification process was ~7 seconds. This time included some multiple-try attempts and the removal of glasses by some users after inserting their card. The quickest times were around 4.5 seconds.

The false-reject error rates for EyeDentify Model 8.5 in this test are significantly less than for the Model 7.5 we tested in 1987. There are two differences between the models we tested that could account for the decrease in these errors:

1. Improved data acquisition software for Model 8.5 now tests for eye fixation before accepting a scan. This feature reduces the chance of a rejection due to eye movement.
2. The Model 7.5 we tested used only keypad PIN entry, while the Model 8.5 we tested used magnetic card PIN entry.

The verify mode crossover point, where the one-try, false-reject error rate and one-try, false-accept error rate are equal, was ~1.5% at a threshold of ~45 for Model 8.5. At the test threshold setting of 70, the three-try, false-reject error rate was 0.4%. No false-accepts were recorded at this threshold value. There were 5134 transactions in the false-reject test and 4196 transactions in the imposter test. The test results for Reader 1 are shown in Figure 4.

EyeDentify Recognize Mode Results

A unique option of the Model 8.5 verifier is the "hands-free" mode of operation. While the verifier is operating in this mode, the user merely peers into the viewing aperture and aligns an optical target by positioning his head. The verifier senses the user's presence, takes a scan, and decides whether or not the scan data is from an eye. If a digital pattern is generated from an eye, the verifier searches the template data base for a match. If a match is found, the verifier recognizes the user as valid. Otherwise, the user is requested to "REPEAT" up to two more tries until a valid match is found. The user is rejected if a match is not found in three tries.

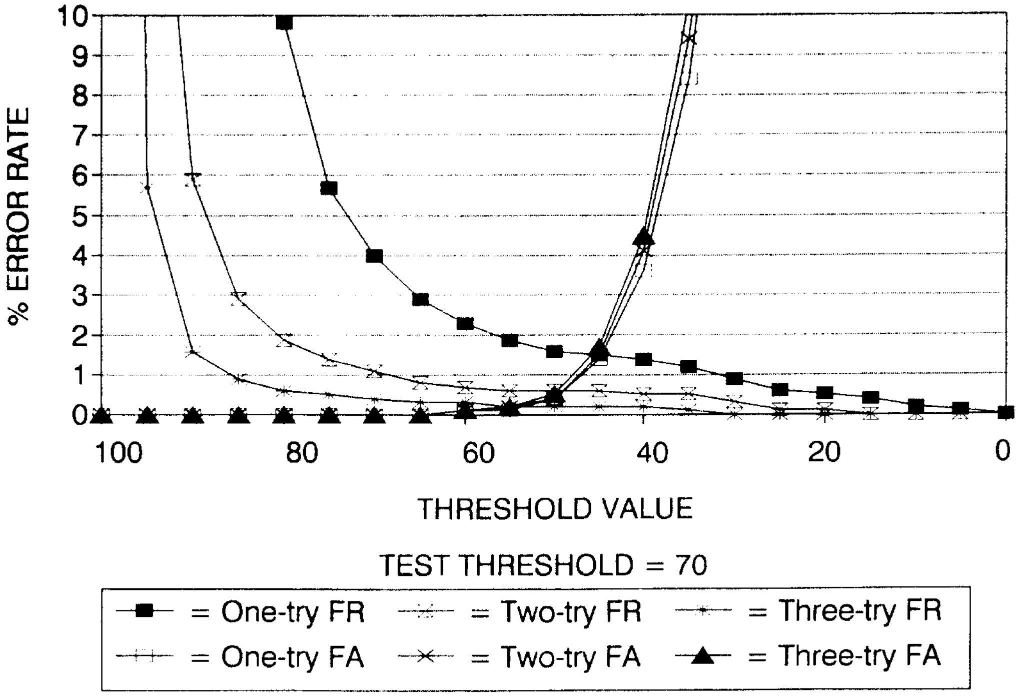


Figure 4. EyeDentify Eye Retinal Pattern

No timing information was taken for the recognize-mode operation because there is no precise point that can be observed when the user initiates the sequence. The user peers into the aperture, aligns the target, and waits for the target to turn off at the end of the scan. The auto-scan feature eliminates the need to insert the magnetic card and press the START button, cutting ~2 to 3 seconds from the verify-mode transaction time. We had a user database of ~100 users that had to be searched to find a matching template for each transaction. This searching did not add a noticeable time delay to the transaction. Larger databases will add more search time to each transaction.

The threshold was set to 75 for the recognize mode of operation. This means that any scan that produces a score of 75 or less is rejected as not being a member of the enrolled user base. A score of greater than 75 causes an accept, and the name of the identified user is displayed on the reader.

There were 5072 transactions recorded on the recognize-mode reader. A transaction is defined as any scan the machine decides meets the minimum criteria to be an eye. None of these scans resulted in a false accept. This result is especially significant because the 100 user database multiplies the possible matches to over half a million!

False-reject information cannot be reported on the "hands-free" recognize reader because there is no PIN associated with a reject that can tie it to a user. No doubt the false-reject rate is significantly higher in the recognize mode because the user does not control the start of the scan. In many attempts, the scan started before the user had the target properly aligned. With practice, most users learned to use the recognize mode to their satisfaction. EyeDentify has now modified their acquisition software to allow users more time to align the target. This change should lower the false-reject error rate.

Identix Results

The fingerprint verifier evaluated in this test was the TouchLock, manufactured by Identix, Inc. in Sunnyvale, California.

The user interface to the Identix system is a sensor module that contains the finger platen/scanner hardware, a display, a keypad and communications electronics. This module is ~8.2 inches wide, 4.4 inches tall, and 3.9 inches deep. The sensor module communicates with a remote processor module over a copper wire cable. The remote module contains the processor, memory, input/output hardware, and communications hardware to support stand-alone operation at a single entry point or in a network environment. Our test verifier was connected to a host computer with the Identix TouchNet software support system. It also was connected to a magnetic-stripe, swipe-card reader via its built-in card reader interface. The card reader was used to enter user PIN information for verification attempts.

The Identix supplied software is a password-protected, menu-driven program for IBM PC and compatibles. It provides the capability to configure the system, to set up user records, and to generate reports.

User enrollment is performed at the sensor module. A security manager must first be verified by a fingerprint scan before the enrollment mode can be entered. Messages on the sensor module display provide user prompts and status information. A unique PIN must be entered for the new user, followed by a number of finger scans that allow the system to generate a template. If the enrollment is successful, a quality rating is displayed. The manager can accept or reject the enrollment at this point. The manufacturer recommends that only "A" or "B" quality ratings be accepted. A "C" rating is the least desirable. If the enrollment is unsuccessful, the system informs the user, who is invited to try again. The templates are not modified by subsequent verifications, so if problems appear, the user should be enrolled again.

We accepted some "C" enrollments for our test. We retrained and reenrolled users that experienced the most problems with verification. The reenrollment did not always result in a higher quality rating. A number of our users appear to have poor quality fingerprints that would not produce good results, even when other fingers were tried. Another problem was caused by low humidity during our test period. User's skin would dry out to the point where the system could not verify the user. Lotion or skin moisturizer often solved the dryness problem.

Our users all had the factory-default verification threshold of 125. The host system software allows the security manager to change individual threshold values, but we did not exercise this option. Our test results do not include the error-rate curves because this verifier did not generate verification score information. Only the percentages of false-reject errors and the false-accept errors at the factory-default threshold can be reported.

The lack of score data hampered our attempts to quantify the Identix verifier. Enrollment quality ratings were generated from groups of finger scans. Individual scan quality was not available. Some clues were available from prompts to position the finger further up or down on the platen, but we could not correlate the finger positioning to scan quality. Our

false-rejection error rates were significantly worse than the estimated error rates published in the Identix TouchNet User's Guide, supplied by Identix with the TouchNet system. Identix indicates an estimated single-try, false-rejection error rate of ~3% for an enrollment threshold setting of 125. We experienced over 9% false-rejections for three-try attempts with the 125 threshold setting. The cold, dry weather effect on skin conditions in Albuquerque could account for some of this difference. Individual score data might have given us more insight into the problem.

Our users averaged ~6.6 seconds for a card PIN entry verification, including multiple-try attempts. The fastest users verified in under 5 seconds.

Two identical readers were used in this test. The two readers tested were set up for a maximum three-try attempt and only reported a single accept or reject transaction result for each attempt. If a user was accepted on either the first, second, or third verification try, the attempt was recorded as an accept. If a user was rejected on all three tries, the attempt was recorded as a reject. Individual-try data was not available from the monitoring program.

Reader 1 logged 2248 verification attempts with a false-reject error rate of 9.4% and no false accepts. Reader 2 logged 2316 attempts with a false-reject error rate of 9.5% and no false accepts. The number of false-accept attempts was 3424. The false-reject error rate equals the percentage of the three-try false-rejects that occurred in the verification attempts.

Recognition Systems, Inc. Results

The Model ID3D-U hand-profile verifier manufactured by Recognition Systems, Inc. (RSI) of San Jose, California was evaluated in this test. The verifier houses the hand geometry reader and all the electronics in one enclosure. Both the wall mount or the desk top models are available. The reader has a platen with guide pins to aid in proper hand placement; an optical imaging system acquires the hand geometry data. Displayed messages prompt the user and provide status information. A keypad and an insertion magnetic-stripe card reader record user data input. This verifier can be configured for stand-alone operation or for use with a host processor. Our test verifiers were configured for use with a host processor. The host management software we used included some custom features not required for normal system operation.

User enrollment takes place at the verifier reader. In actual security system applications, each user is assigned an authority level and, if required, a password for entering the security management command mode. A new user can only be enrolled by a security manager with the proper authority level and password to enter the enrollment sequence. The manager must first be verified on the hand geometry reader, and then he must enter the proper password within a time limit to initiate the enrollment sequence. Our test software did not require a password or manager verification for user enrollment. It provided the necessary functions with a menu-driven program that allowed the test conductors to fill in the blanks and to initiate the enrollment sequence.

User Enrollment Sequence

1. A valid PIN is entered by the new user.
2. A ** PLACE HAND ** message then appears on the reader display.
3. The user must then place his hand on the platen and against the guide pins.
4. When the imaging system determines that the hand is properly positioned within the time limit, the hand geometry data is acquired and a ** REMOVE HAND ** message is displayed.
5. The message display prompts are repeated at least two more times, and the user reference template is then generated from an average of the three inputs.

User Verification Sequence

1. Enter the user PIN by keypad or card reader.
2. Follow the ** PLACE HAND ** and ** REMOVE HAND ** instructions on the display.

The average verification time for our users was ~5 seconds, with card PIN entry. (Times as low as ~2.9 seconds were observed.)

The false-reject error rates for Model ID3D-U in this test were less than the rates were in 1987 when we tested the Model ID3D-ST. PIN entry by magnetic card rather than by keypad is the most likely reason for the lower error rates.

The crossover point, where the one-try, false-reject error rate and the one-try, false-accept error rate are equal, was ~0.2% at a threshold of ~100 for Model ID3D-U. At the test threshold value of 75, the three-try, false-reject error rate was less than 0.1% and the one-try, false-accept error rate was ~0.1%. Three-try, false-accept error rate data was not obtained in this test. The test results were very similar on both readers; thus, only Reader 0 results are plotted.

Reader 0 logged 5303 transactions in the false-reject test and 5248 transactions in the imposter test. Reader 1 logged 5285 transactions in the false-reject test and 3839 transactions in the imposter test. The results of this test are shown in Figure 5.

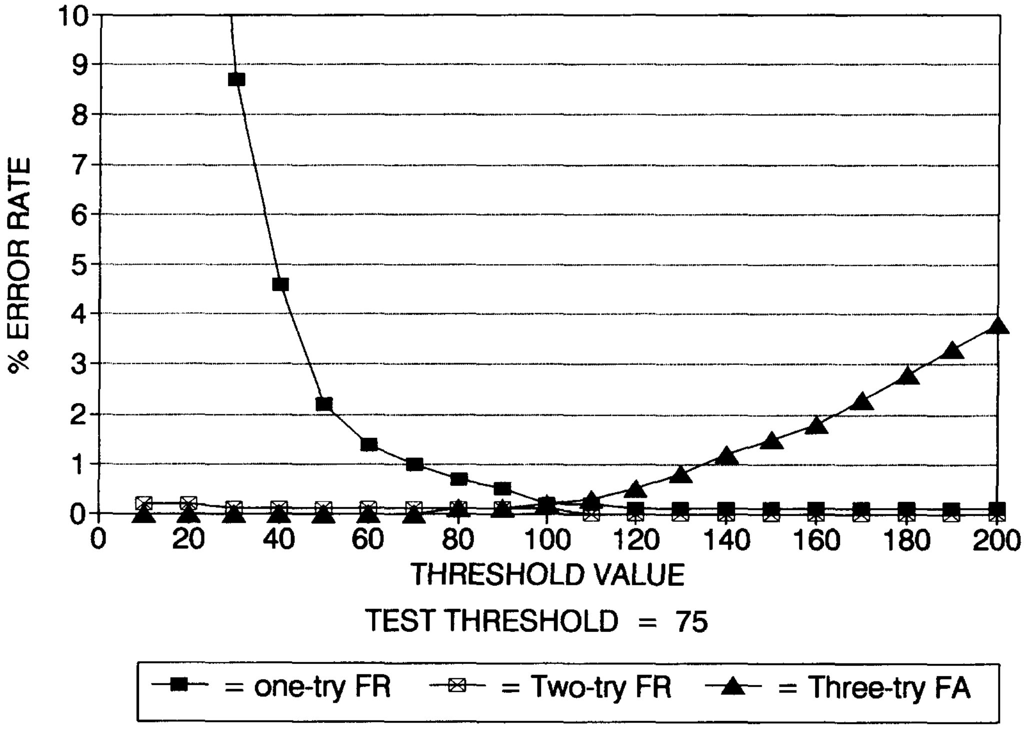


Figure 5. Recognition Systems Hand Geometry

Summary

The relative performance of the tested verifiers can be deduced from the test results. These results include the user variables in the operation of the machines and are therefore representative of the performance that can be expected with average users; at the same time, they are not a true measure of the machines absolute performance limits. The degree to which our results differ from the performance limits is an indication of the complexity of the user interface. As an interface becomes more complex, more user variables are introduced that could shift the test results away from the performance limit.

From a test viewpoint, it is desirable to have a final score value reported for each verification try. This report is not possible, however, because some verifiers do not provide the score data necessary for us to calculate error-rate curves. Verifier results in this case are given only for the one threshold value tested. It would have been possible to repeat the performance tests at a number of different threshold values to obtain points on the error-rate curves, but we did not have the resources for such an extensive test. This is only one of several roadblocks for developing biometric verifier testing standards.

A user survey was taken late in the test. The summary results are given in the appendix. Users generally preferred the verifiers that produced the fewest false-rejects and which took the least time to use. User frustration grew rapidly with high, false-rejection rates; these rates proved to be a bigger problem for them than did the slow transaction times. The RSI hand geometry was overall the user favorite.

The verification timegraph (see Figure 6) shows the average transaction times for:

- entering the PIN
- presenting the biometric feature
- verification or rejection.

The Alpha Microsystems time also includes the time necessary:

- to dial a five-digit number on a touch-tone telephone
- wait for an answer from the system.

This data was obtained by timing the users without their knowledge. These times are representative of actual-use transactions; they are not intended to indicate the minimum times possible.

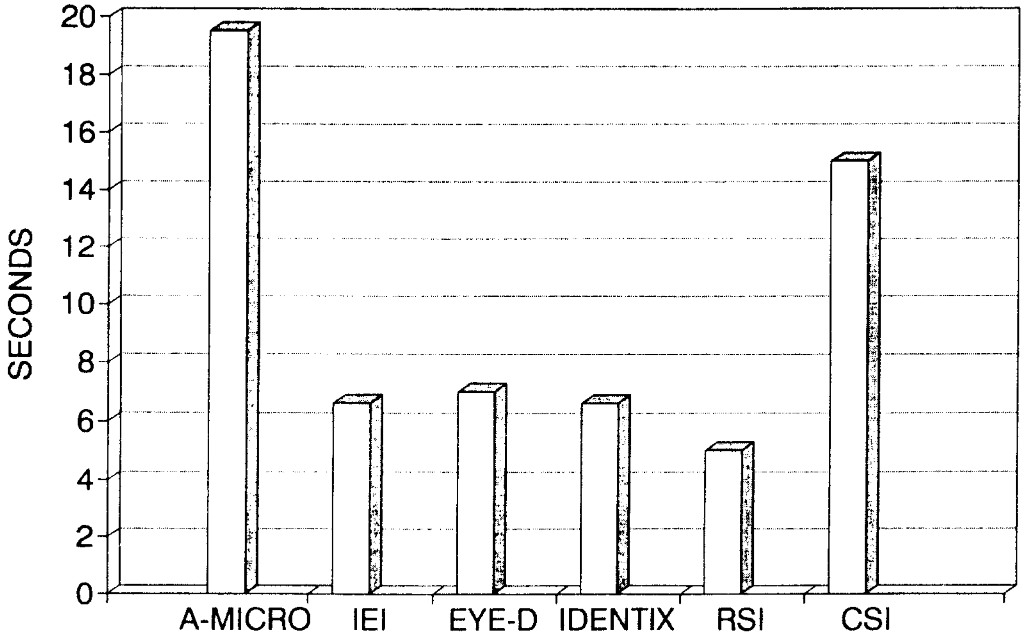


Figure 6. Average Verification Time in Seconds

Conclusions

Performance is a very important issue, but it is not the only factor in choosing a biometric identification device. The device must also be suitable for the facility in which it is installed. The present generation of biometric identification devices provides reliable and cost-effective protection of assets. Available computer interfaces and software provide effective security management with real-time control, transaction logging, and audit-tracking capabilities. The current need in the biometric identification field is to have the market make greater use of what already exists. While new biometric devices are still emerging, it is unlikely that any of them will turn the market around with a price or performance breakthrough.

The error-rate curves contain much more information about the performance of the verifiers than was included in our individual discussions. Manufacturers can provide additional information about how to apply their devices to specific requirements. Finally, it is important to keep the error rates in perspective to the real world. A 3% false accept means that there is a 97% probability that an imposter will be detected.

References

[1] Identix, Inc., 510 N. Pastoria Ave., Sunnyvale, CA 94086, (408) 739-2000

[2] Recognition Systems, Inc., 1589 Provencetown Drive, San Jose, CA 95129, (408) 257-2477

[3] Capital Securities Systems, Inc., Capital Security Operations, 9050 Red Branch Road, Columbia, MD 21045, (301) 730-8250

[4] EyeDentify, Inc., PO Box 3827, Portland, OR 97208, (503) 645-6666

[5] Alpha Microsystems, 3501 Sunflower, Santa Ana, CA 92704, (714) 957-8500

[6] International Electronics, Inc., (ECCO) VoiceKey, 32 Wexford St., PO Box 584, Needham Heights, MA 02194, (617) 449-6646.

APPENDIX

User Survey Results

Which machine do you feel:	ALPHA	ECCO	EYEDENTIFY		IDENTIX	RECOGNITION	AUTOSIG	NONE
	MICRO		VERIFY	RECOGNIZE		SYSTEMS	SIGNON	
1. is the easiest to use?	0	4	2	22	15	35	1	0
2. is the fastest?	1	4	1	28	8	35	0	0
3. is the slowest?	38	5	1	2	9	0	24	1
4. rejects you most often?	11	36	2	5	17	1	6	0
5. rejects you least often?	11	6	10	11	12	42	9	0
6. requires most concentration?	10	25	12	23	6	1	4	0
7. requires most proficiency?	11	23	9	15	11	1	9	4
8. requires least proficiency?	5	6	4	9	12	38	6	1
9. is most frustrating to use?	10	34	2	12	12	0	5	3
10. is most friendly/fun?	5	2	6	17	13	31	6	1
11. gives health/safety concerns?	1	0	23	21	1	5	0	47
12. gives invasion of privacy concerns?	0	1	2	2	3	1	16	56
13. was most difficult to enroll on?	17	21	1	1	15	2	3	18
14. was most intimidating to use?	5	16	4	6	4	0	2	41
15. best to secure a computer terminal?	7	4	12	10	22	18	7	9
16. best for door security?	3	7	18	19	13	27	3	4
17. best for bank/POS use?	1	0	13	8	21	11	23	6
18. best for large population?	2	2	5	14	16	38	3	8
19. Did you like card or pin best?	Card: 56		Pin: 17	None: 3				

NOTES:
1. Number of respondents: 76
2. Respondents were allowed to make multiple responses to each question.

DISTRIBUTION:

1 Edward J. McCallum, Director
Office of Safeguards and Security
US DOE
SA-10
Washington, DC 20545

1 William L. Barker, Acting
Dep. Asst. Secy. for Security Affairs
US DOE
SA-1
Washington, DC 20545

1 David A. Jones, Acting Director
Policy, Standards and Analysis Division
Office of Safeguards and Security
US DOE
SA-12
Washington, DC 20545

1 William J. Desmond, Chief
Physical Security Branch
Office of Safeguards and Security
US DOE
SA-121
Washington, DC 20545

1 Larry D. Wilcher, Chief
Technical and Operations Security Branch
Office of Safeguards and Security
US DOE
SA-123
Washington, DC 20545

1 Jerry C. Howell, Deputy Director
Field Operations Division
Office of Safeguards and Security
US DOE
SA-13
Washington, DC 20545

1 Donald C. Tubbs
Assessment and Integration Branch
Office of Safeguards and Security
US DOE
SA-131
Washington, DC 20545

1 Ernest E. Wagner, Chief
Weapons Safeguards and Security Operations Branch
Office of Safeguards and Security
US DOE
SA-132
Washington, DC 20545

1 A. J. Heysel, Chief
Production/Energy Safeguards/
Security Operations Branch
Office of Safeguards and Security
US DOE
SA-133
Washington, DC 20545

1 G Dan Smith, Chief
Planning and Technology Development Branch
Office of Safeguards and Security
US DOE
SA-134
Washington, DC 20545

1 Carl A. Pocratsky
US DOE
SA-134
Washington, DC 20545

1 Marshall O. Combs, Deputy Director
Headquarters Operations Division
Office of Safeguards and Security
US DOE
SA-14
Washington, DC 20545

1 David A. Gurule, Acting Director
Security and Nuclear Safeguards Division
US DOE/AL
PO Box 5400
Albuquerque, NM 87115

1 Donald J. Cook, Director
Attn: Stan Laktosic, Tom Golder
Central Training Academy
US DOE/AL
PO Box 5400
Albuquerque, NM 87115

DISTRIBUTION (Continued):

1 Donald Jewell, Assistant Director
Central Training Academy
US DOE/AL
PO Box 5400
Albuquerque, NM 87115

1 Ronald Perry
Argonne National Laboratory
Bldg. 222 Electronics
Argonne National Laboratory
9700 South Cass Avenue
Argonne, IL 60439

1 Roger L. Black
W. Patrick Keeney
Argonne National Laboratory
Bldg. 752/MS 6000
PO Box 2528
Idaho Falls, ID 83403

1 Larry Runge and George Schoener
Safeguards and Security Division
Bldg. 50
2400 Upton Road
Upton, NY 11973

1 Kris Dahms
Safeguards and Security Division
Bldg. 703
2400 Upton Road
Upton, NY 11973

1 Robert L. Windus, Security Officer
US DOE/BP
PO Box 3621
Portland, OR 87208

1 Harold W. Kelley, Director
Safeguards and Security Division
US DOE/CH
9800 South Cass Avenue
Argonne, IL 60439

1 Rudy Dorner
Fermi National Accelerator Laboratory
MS 102
Batavia, IL 60150

1 H. R. Martin, Acting Director
Safeguards and Security Division
US DOE/ID
785 DOE Place
Idaho, Falls, ID 83402

1 Timothy L. Mitchell, L 024
Lawrence Livermore National Laboratory
PO Box 808
Livermore, CA 94550

1 Darryl B. Smith
James W. Tape
N-DO/MS E550
Los Alamos National Laboratory
PO Box 1663
Los Alamos, NM 87545

1 Jack England, Division Leader
OS-DO, MS G729
Los Alamos National Laboratory
PO Box 1663
Los Alamos, NM 87545

1 E. Wayne Adams, Director
Safeguards and Security Division
US DOE/NV
PO Box 98518
Las Vegas, NV 89193-8518

1 William G. Phelps, Director
Safeguards and Security Division
US DOE/OR
PO Box 2001
Oak Ridge, TN 37831-8570

1 J. A. Bullian, Director
Safeguards and Security Division
US DOE/PNR
PO Box 109
West Mifflin, PA 15122

2 Joseph W. Wiley, Director
Safeguards and Security Div
US DOE/RL
PO Box 550
Richland, WA 99352

DISTRIBUTION (Continued):

1 Michael Hooper, Acting Director
Safeguards and Security Division
US DOE/SF
Lawrence Livermore Laboratories
L-556
PO Box 808
Livermore, CA 94550

1 Gerorge G. Stefani, Jr., Director
Security and Safeguards Division
Schenectady Naval Reactors Office
US DOE
PO Box 1069
Schenectady, NY 12301

1 Donald J. Ornick, Director
Security Division
US DOE/OR
900 Commerce Road East
New Orleans, LA 70123

1 H. B. Gnann, Chief
Safeguards Engineering and Projects Branch
US DOE/SR
PO Box A
Aiken, SC 29808

1 Joan Christopher, Security Officer
Western Area Power Administration
US DOE
PO Box 3402
Golden, CO 80401

1 Larry Cameron
Allied Signal, Inc., Kansas City Division
2000 E. 95th Street
Kansas City, KS 64131-3095

1 Edward C. McGurren, Manager
Security Operations
Allied Signal, Inc., Kansas City Division
2000 E. 95th Street
Kansas City, KS 64131-3095

1 Harley Toy, Manager
Nuclear Services
Battelle Memorial Institute
505 King Avenue
Columbus, OH 43201

1 Boeing Petroleum Services
Attn: Security Department
850 South Clearview
New Orleans, LA 70123

1 John W. Jones, Manager
Safeguards and Security
EG&G Idaho
1955 Fremont
Idaho Falls, ID 83402-3126

1 Daniel Baker, Manager
Security
EG&G Mound
Bldg. 99
PO Box 3000
Miamisburg, OH 45432

1 K. N. Gardner
Technical Security
Bldg. 99
EG&G Mound
PO Box 3000
Miamisburg, OH 45432

1 Ron Mahan, Manager
Security Administration
EG&G Mound
Bldg. 99
PO Box 3000
Miamisburg, OH 45432

1 Vince Hanson, Manager
Protective Force
Bldg. 47
EG&G Mound
PO Box 3000
Miamisburg, OH 45342

1 Curtis L. Fellers
Technologies Department
Bldg. OSE-211
EG&G Mound
PO Box 3000
Miamisburg, OH 45342

DISTRIBUTION (Continued):

1 Roy E. Gmitter, Manager
Plant Security
General Electric Neutron Division
PO Box 2908
Largo, FL 34649

1 Holmes and Narver, Inc.
Attn: Electronics Department
PO Box 93838
Las Vegas, NV 89193-3838

1 Clifford A. Druit, Manager
Y-12 Safeguards and Security
Martin Marietta Energy Systems
Bldg. 9706-1, MS 8213
PO Box 2009
Oak Ridge, TN 37831-8213

1 James Hallihan
Mason and Hanger-Silas Mason, Co., Inc.
Pantex Plant
PO Box 30020
Amarillo, TX 79177

1 James Long
Protection Technologies of Idaho
785 DOE Place
Idaho Falls, ID 83402

1 Jeffrey Jay, Team Manager
Inspection and Technical Assessment Branch
Science Applications International Company
c/o DOE/Savannah River Operations Office
PO Box A
Aiken, SC 29802

1 Wackenhut Services, Inc.
800 West Commerce Rd., Suite 100
New Orleans, Louisiana 70123

1 Walk, Haydel, and Associates
600 Carondelet
New Orleans, LA 70130

1 Edward R. Saxon, Chief
Hanford Patrol
Westinghouse Hanford Company
SO-46
PO Box 1970
Richland, WA 99352

1 E. L. Goldman
Westinghouse Idaho Nuclear Company, Inc.
PO Box 4000
Idaho Falls, ID 83403

1 Ronald D. Klingler, Manager
Safeguards and Security
Westinghouser Idaho Nuclear Co., Inc.
MS 5102
PO Box 4000
Idaho Falls, ID 83403

1 Larry Schenk, Manager
Technical Security
Westinghouse Idaho Nuclear Company, Inc.
PO Box 4000
MS 5102
Idaho Falls, ID 83403

1 James M. Miller, Manager
Safeguards and Security
Westinghouse Materials Company of Ohio
PO Box 398704
Cincinnati, OH 45239

1 W. W. Arra
Westinghouse Savannah River Co., WSRS
703-57A, Rm. 7
PO Box 616
Aiken, SC 29802

1 M. Brinton
Westinghouse Savannah River Co., WSRS
703-45A, Rm. 110
PO Box 616
Aiken, SC 29802

1 C. J. O. Cox
Westinghouse Savannah River Co., WSRS
703-45A, Rm. 150
PO Box 616
Aiken, SC 29802

1 J. W. Maloney, Manager
Safeguards and Security
Westinghouse Savannah River Co., WSRS
PO Box 616
Aiken, SC 29802

DISTRIBUTION (Concluded):

1 S. C. Nashatker
Westinghouse Savannah River Co., WSRS
703-45A, Rm. 151
PO Box 616
Aiken, SC 29802

1 W. W. Rajczar
Westinghouse Savannah River Co., WSRS
703-42A, Rm. 115
PO Box 616
Aiken, SC 29802

1 John M. Samuels, Managers
Safeguards and Security Department
Westinghouse Savannah River Co., WSRS
PO Box 616
Aiken, SC 29802

1	3430	R. P. Kelly
1	3431	J. A. Kaiser
1	3432	D. E. Kerome
1	3433	R. M. Workhoven
1	3437	R. G. Baca
1	5200	J. Jacobs
1	5210	C. C. Hartwigsen
1	5211	S. H. Scott
1	5219	R. W. Moya
1	5220	J. W. Kane
1	5230	H. M. Witek
1	5231	D. J. Gangel
1	5233	D. C. Hanson
1	5234	J. C. Mitchell
1	5238	R. F. Davis
1	5240	D. S. Miyoshi
10	5240A	M. W. Green
1	5245	I. G. Waddoups
20	5245	J. P. Holmes
1	5245	L. S. Wright
1	5248	R. P. Syler
5	5248	R. L. Maxwell
1	5249	B. J. Steele
1	5260	J. R. Kelsey
1	5268	S. J. Weissman
1	8530	M. A. Pound
1	8531	D. R. Charlesworth
1	8536	C. L. Knapp
1	8523	R. C. Christman
5	3141	S. A. Landenberger
8	3145	Document Processing For DOE/OSTI
3	3151	G. C. Claycomb

SCHLAGE

ALLEGION™

3^{rd} Party PoE Adapter Use: F-Series & G-Series

This document stands to act as a procedural guide for when using a 3rd party PoE adapter with the HandReaders, both F-Series & G-Series[1]. Schlage has performed testing to confirm that when using a PoE adapter[2], the HandReader will operate normally; so long as the minimum power requirements are met. Please use the following instructions as a guideline for initial set up of the Wi-Fi adapter.

Setup Summary of the PoE Injector and PoE Splitter (One-on-One)

Host --> Switch --> PoE Injector --> PoE Splitter --> HandReader

1. Connect from a host PC to a network switch via an Ethernet cable
2. Connect another Ethernet cable from the network switch to "LAN IN" on the PoE Injector
3. Connect between "Power/Data Out" of PoE Injector and "Power/Data In" of PoE Splitter by using Ethernet cable
    a. It is important to note the distance between the PoE Injector and PoE Splitter. PoE supported distances may vary depending on the manufacturer[3].
        i. Power degradation could occur if lengths are exceeded, which could have undesirable effects in the performance of the HandReader.
4. Connect power cable to the PoE Injector
5. Connect "LAN OUT" from PoE Splitter to HandReader Ethernet port
6. Connect "DC OUT" from PoE Splitter to HandReader power port
    a. It is important to ensure that the outputting power is at least 12V at 1A.
    b. It is important to ensure that the power (barrel) connector is compatible with HandReader.
        i. Power degradation could occur when inadequate power is outputted from the splitter, which could have

[1] F-Series models include: all HandPunch & HandKey models that have Ethernet enables. G-Series includes the GT-400.
[2] PoE Device Detail: Model Name & Number; TP-LINK PoE Adapter Kit: TL-POE200
[3] The TL-POE 200 maximum transfer length is 100 meters (330 ft)

70200-0041

BR-100

Installation Instructions

This installation guide consists of 3 sections:

- How to connect the BR-100 to an F3 HandReader
  - Bell Output - page1
  - Lock Output - page 2

F3 HandReader Models
HP-1000E, HP-1000-F3, HP-2000-F3, HP-3000-F3, HP-3000E-F3,
HP-4000-F3, HP-4000-S-F3, HK-2-F3, HK-2-CR-F3, HP-1000E-XL,
HP-1000-XL, HP-2000-XL, HP-3000-XL, HP-3000E-XL

- How to connect the BR-100 to an F1 HandReader
  - Bell Output - page 2
  - Lock Output - page 3

F1 HandReader Models
HP-50E, HP-1000, HP-2000, HP-3000, HP-3000E,
HP-4000, HP-4000-S, HK-2, HK-CR

- How to connect the BR-100 to an E Series HandReader
  - Bell Output - page 3
  - Lock Output - page 4

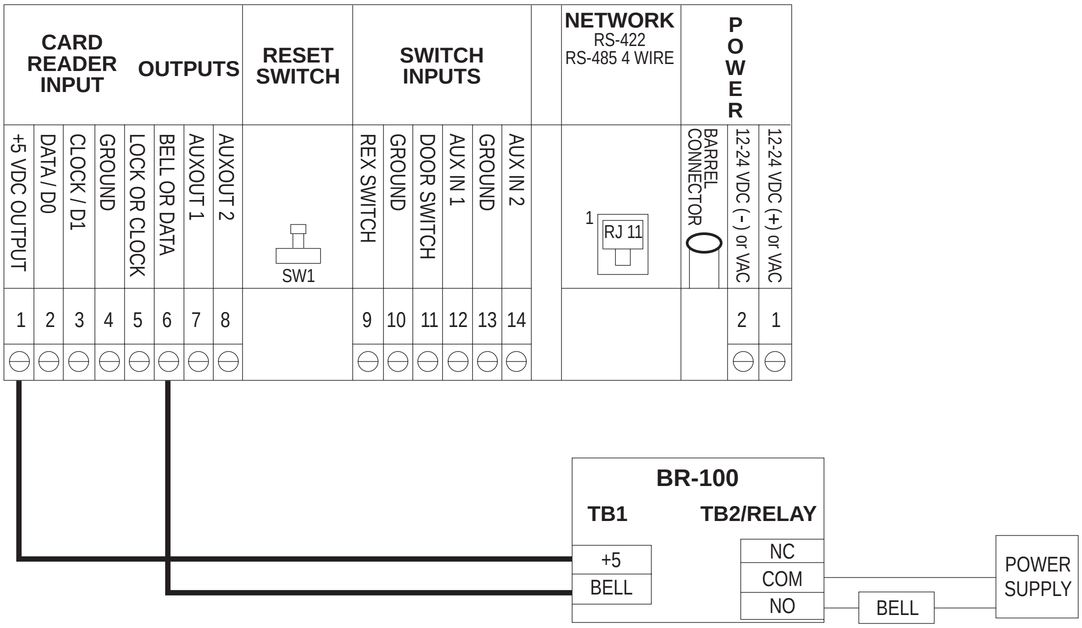
E Series HandReader Models
ID3D-R, ID3D-RW, LH-100, LH-100-RW

⚠ **CAUTION:** **Please choose your model carefully as the reader can be damaged by incorrectly wiring the relay.**

➔ *See page 4 for examples on wiring the BR-100 relay to a lock.*

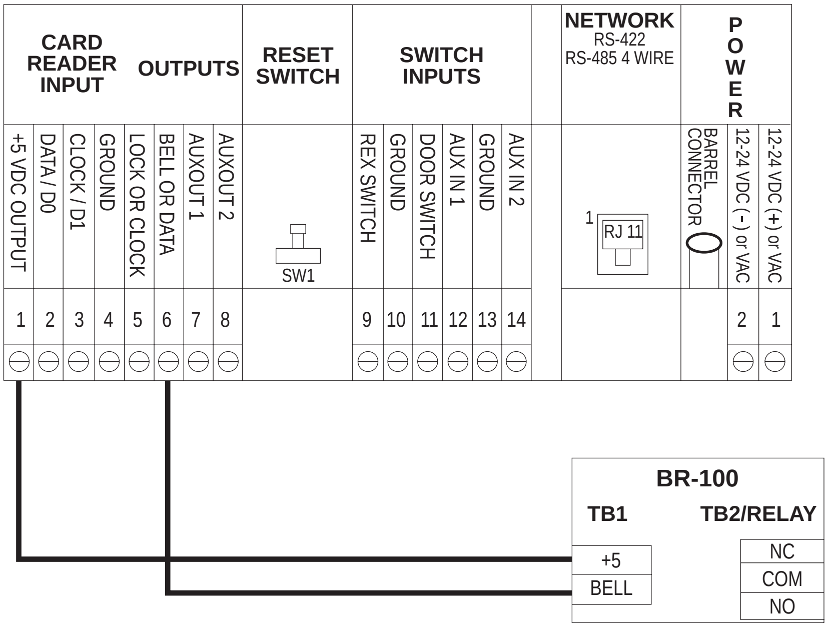
How to connect the BR-100 to an **F3 HandReader** for…

Bell Output



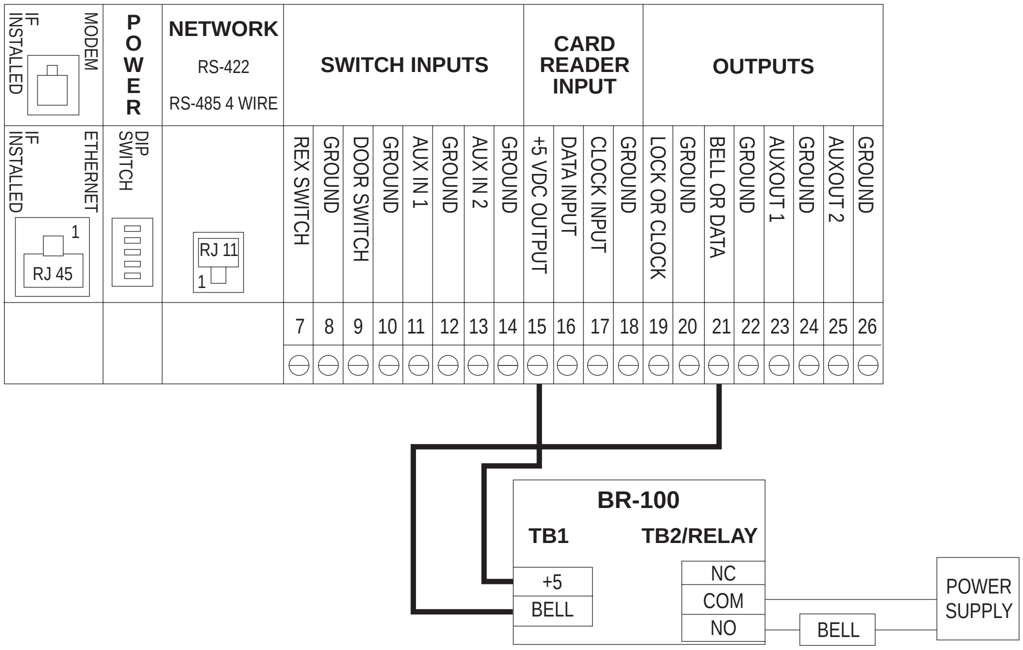
How to connect the BR-100 to an **F3 HandReader** for…

Lock Output



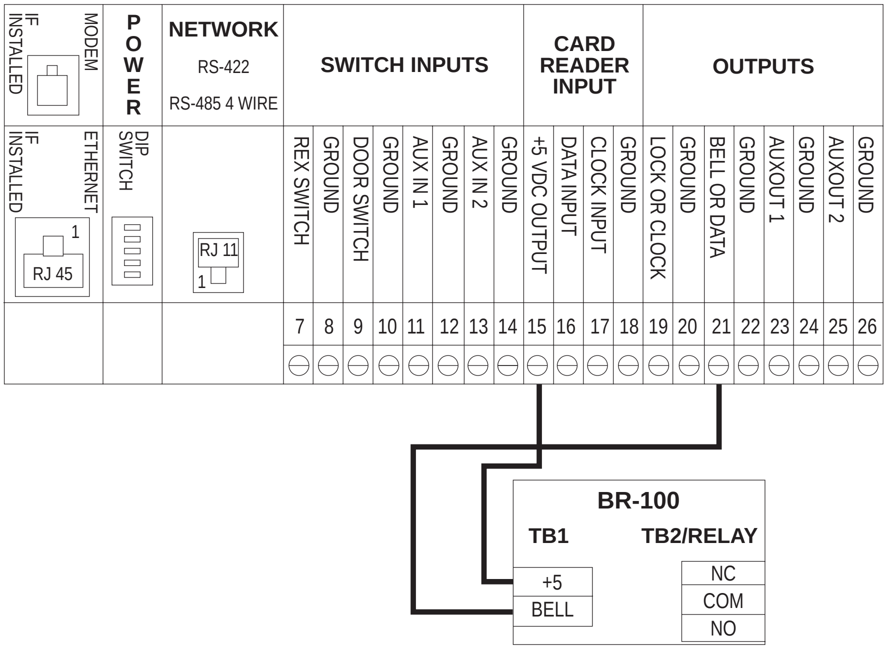
How to connect the BR-100 to an **F1 HandReader** for…

Bell Output



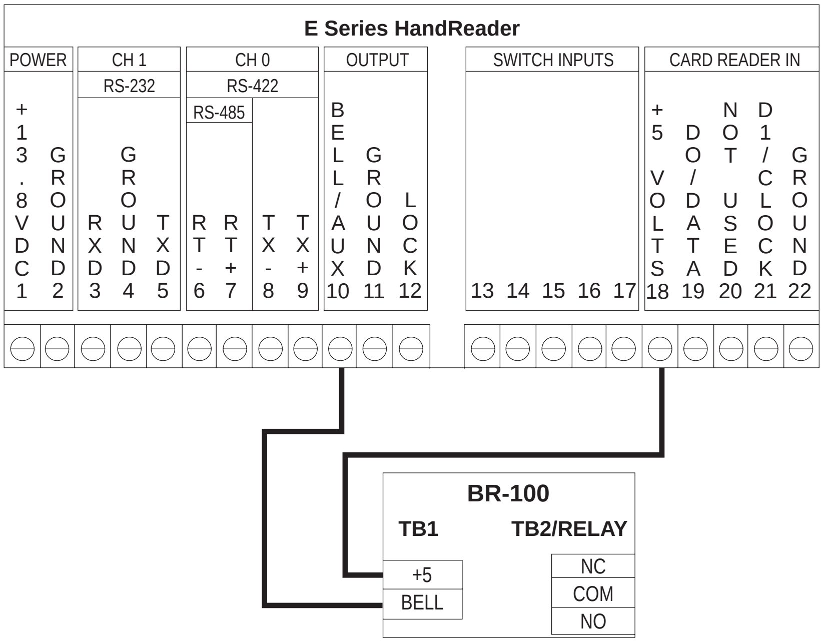
How to connect the BR-100 to an **F1 HandReader** for…

Lock Output



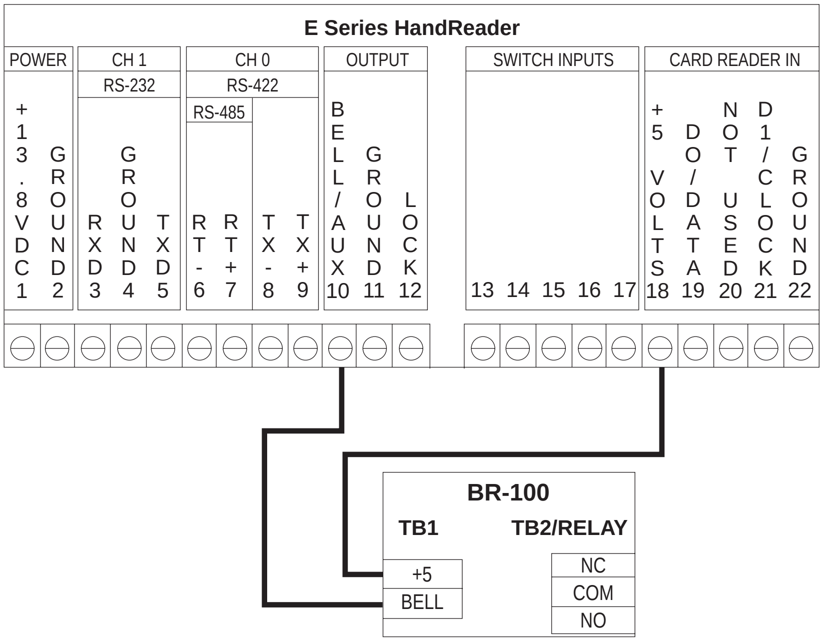
How to connect the BR-100 to an **E Series HandReader** for…

Bell Output



How to connect the BR-100 to an **E Series HandReader** for…

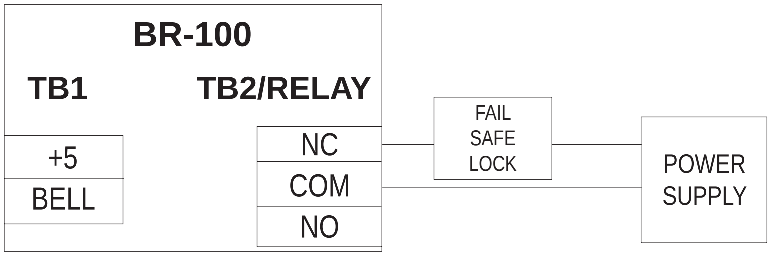
Lock Output



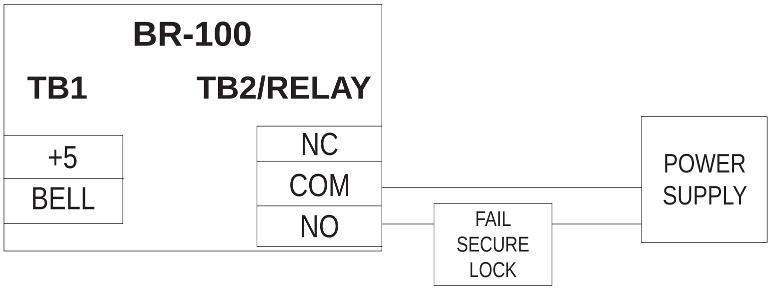
Wiring Examples

⚠ **WARNING: These are generic examples. Please follow the wiring guidelines provided by the manufacturer of the lock.**

Fail Safe Lock: The fail-safe lock guarantees access if power fails. The lock requires power to stay locked; during a power failure, access is granted.



Fail Secure Lock: The fail-secure lock guarantees security if power fails. The lock requires power to unlock; during a power failure, access is denied.



Break Compliant HandPunch Line

Schlage is pleased to announce our new line readers that are now capable of complying with labor “break” laws that have been adopted by more than 20 states. These labor laws are in place to regulate on-the-job meals and breaks for employees. When integrated with properly with a 3rd party software, the Schlage HandPunch “Break Compliance” capability will make it possible for employers to comply with laws relating to meals and breaks, avoiding potential fines and lawsuits.

The new Break Compliant Models are:

HP-1000-XL
HP-1000-E-XL
HP-2000-XL
HP-3000-XL
HP-3000-E-XL

Existing Break Compliant Models are:

HP-4000 (With prom 296 or higher)

How are we Break Compliant? / What makes this line unique?

- Each of our Break Compliant models (XL line) utilizes the Extended User Record. It is within the extended user record where we store the lock out features and information. If the host software/program is not set up to handle the extended user record, the Break Compliant feature may not work properly.
- When a current HP-1000 model is booted up, typically, the following is seen on the LCD:
  Example:	HP1.12345.312

The HP1, HP2, HP3 will now have new corresponding model identifiers numbers for the XL line.

HP-1000-XL & HP-1000-E-XL	= 1PX
HP-2000-XL	= 2PX
HP-3000-XL & HP-3000-E-XL	= PXL

Example:	1PX.12345.312

These model identifiers are also communicated via the DLL commands; these new DLL commands are required in order for the host program to properly recognize the model.

There are two ways to implement this feature:

1. The first is to integrate new DLL's to create a customized solution with the host program. This can be achieved by creating a custom solution, or utilizing the function key script compiler. In order to integrate the following will be needed:
    a. A Break Compliant Reader
    b. Prom 312 or higher
    c. Updated SDK – version 2.1.4
    The latest SDK can be obtained from technical support at SBSsupport@irco.com or 1-866-861-2480, option 1.

2. The second is to activate the capability at the reader using the TA Standoff Menu. First, activate the T&A Mode (Explicit Punch) and then set the values needed in the TA Standoff Val Menu
    a. To activate Explicit Punch
        i. Menu 2, SET ID LENGTH, (enter desired ID length) T&A MODE SET, [Yes#]

    To set TA STANDOFFs

    Step 1: Go into Menu 5, TA STANDOFF VALS,

    Step 2: Select OUT Code (TA Codes): These will be the type of punches which will activate the lock out capability
    *If no additional OUT codes are needed, enter 00, and go to STEP 3.

    Step 3: Select the STANDOFF: This is how long, in minutes, the lock out period will be active.

    Step 4: Select additional OUT Code (TA Codes): Up to three codes can be selected.
    *If no additional OUT codes are needed, enter 00, and go to STEP 5.

    Step 5: Select the STANDOFF: This is how long, in minutes, the last OUT code is to be active.

    Step 6: Select up to 3 BACK Codes: These (TA CODES) are the type of punches that will be locked out until the timer has expired. Up to 3 can be selected, but once completed, press 00. ***

    ***If 00 is the only value entered for the BACK Codes, all subsequent punches of any kind will be prohibited until the timer has expired.

TA CODE (Menu 5) StandOff Values OUT codes & BACK codes	Description	Code Displayed in HandReaders LCD Menu
FF	No Data Expected	
00	No Data Expected	
01	In	1-IN
02	Back 1	3-BACK → 1-LUNCH
03	Out	2-OUT
04	Department	
05	Back 2	3-BACK → 2-BREAK
06	Job	
07	Back 3	3-BACK → 3-CALL BACK

*Table 1: Sourced from Technical Manual

Example 1

HR Manager Holly needs to prohibit her employees from clocking back in from lunch early, ensuring that they take their full lunch period of 30 minutes. After activating the T&A Mode, she would go into Menu 5, select OUT CODE: 03, STANDOFF: 30, and BACK CODE: 02, 05.

Employee Sally clocks out for lunch at 12:00. When she tries to clock back in at 12:25, the reader will display INVALID Punch.

Example 2

HR Manager Jean wants to prohibit her employees from clocking back in from clocking out or lunch, ensuring that they take their full break of 15 minutes. After activating the T&A Mode, she would go into Menu 5, select OUT CODE: 03, STANDOFF: 15, and BACK CODE: 00.

Employee Bill clocks out for break at 2:30. When he tries to clock back in at 2:42, the reader will double beep and display INVALID Punch.

How do I make my current units 'Break Compliant'?

You can purchase a new spare main board and install it in the field.

NOTE: Replacing any main board in the field creates a risk of the HandPunches falling outside of acceptable calibration range. It is recommoned that units be sent back to the factory to have the main board calibrated to the camera.

For Pricing Information, please contact your local sales representative

New Part Number (units without Battery Backup)

S-PC-1K-XL-R
S-PC-1K-E-XL-R
S-PC-2K-XL-R
S-PC-3K-XL-R
S-PC-4K-R (specify prom 296 or higher)

New Part Number (units with Battery Backup)

S-PC-1K-XL-RB
S-PC-1K-E-XL-RB
S-PC-2K-XL-RB
S-PC-3K-XL-RB
S-PC-4K-RB (specify prom 296 or higher)

If you are going to replace the main board to upgrade existing units, we recommend purchasing a new overlay so that you can easily identify that the unit is break compliant. Below are the new corresponding overlay numbers.

New Part Number

OVLY HP-1K- XL
OVLY HP-1K-E-XL
OVLY HP-2K-XL
OVLY HP-3K-XL

You can purchase one of the new models.

New Model

HP-1000-XL

- All Options & Spares for the HP-1000 are applicable to the HP-1000-XL

HP-1000-E-XL

- All Options & Spares for the HP-1000-E are applicable to the HP-1000-E-XL

HP-2000-XL

- All Options & Spares for the HP-2000 are applicable to the HP-2000-XL

HP-3000-E-XL

- Standard memory comes with 530 users
- All other Options & Spares for the HP-3000-E are applicable to the HP-3000-E-XL **EXCEPT** memory options
  - EM-805 to 3,498 users
  - EM-815 to 12,879 users
  - EM-825 to 25,758 users
  - EM-835 to 38,637 users
  - EM-845 to 51,516 users

HP-3000-XL

- Standard memory comes with 530 users
- All other Options & Spares for the HP-3000 are applicable to the HP-3000-XL **EXCEPT** memory options
  - EM-805 to 3,498 users
  - EM-815 to 12,879 users
  - EM-825 to 25,758 users
  - EM-835 to 38,637 users
  - EM-845 to 51,516 users

Existing Models (Break Compliant)

HP-4000

- Options & spares offered are still applicable at current pricing.

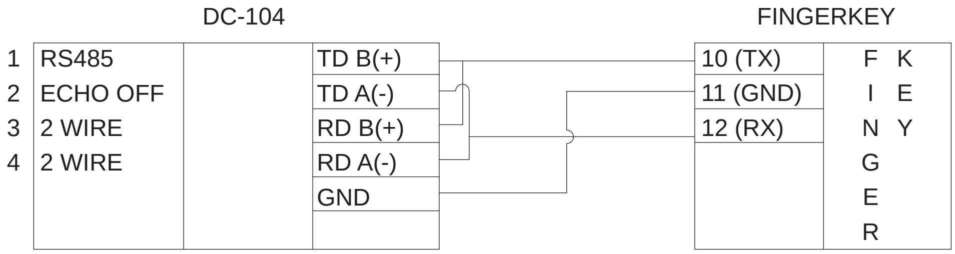
For additional information, please contact Customer Care at 877-671-7011.

Pricing/Product descriptions subject to change without notice

70200-0063

DC-104

Installation Instructions



DIP switches on the DC-104 need to be set as follows:

1. RS485
2. Echo off
3. 2 wire
4. 2 wire

SW1 DIP Switch on the FingerKey needs to be set as follows:

1. ON
2. ON
3. OFF
4. OFF

- Jumper needs to be installed between the TD B(+) and RD B(+)= TD/RD(+)
- Jumper needs to be installed between the TD A(-) and RD A(-)= TD/RD(-)
- The TD/RD(+) on the DC-104 connects to terminal #10(TX) of the FingerKey.
- The TD/RD(-) on the DC-104 connects to terminal #12(-) of the FingerKey.
- The GND on the DC-104 connects to terminal #11(Ground) of the FingerKey.

Ingersoll Rand
Security Technologies

(877) 671-7011
Printed in Country
70200-0063 Rev. 8/11-b

70200-0014

F Series Ethernet Upgrade

Installation Instructions

Ethernet Requirements

- A TCP/IP network
- CAT 5 cable or better
- 10baseT
- Static IP address, gateway and subnet addresses (if needed)
- Port 3001 must be opened

Power Up

A reader with an Ethernet adapter installed and the network cable plugged in will automatically detect the presence of the Ethernet adapter upon power up. If the network cable is not plugged in prior to power being applied, the Ethernet adapter will not see the network and the reader will ask if the cable is plugged in. Plug in the network cable and power cycle the reader. When the reader boots up and detects the network, the LCD will display an IP address and then proceed to either the “Enter ID” or “Ready” prompt.

Address Requirements

The EN-100/200 does not support DHCP; therefore a static IP address is required and must be programmed into the reader before the adapter will communicate with the network.

Obtain all addresses that are required for the network from the system administrator of the site. If there is no need for a gateway address, set it to all zeros (i.e. 000.000.000.000). If the reader is required to communicate over a WAN, the subnet mask needs to be converted to a host bit number. If a subnet mask is not needed, set the host bit to 0. Have the system administrator set Port 3001 to allow access on all switches and routers between the EN-100/200 and host program.

To configure the Ethernet adapter, follow these steps:

1. The reader’s IP address resides in the SET SERIAL command of the SETUP menu, which is by default in the menu 2 of the reader.
2. Press # when the LCD display shows.

```
SET SERIAL
* NO  YES #
```

3. Enter the 12 digit IP address using leading zeros and press #.
4. Enter the 12 digit gateway using leading zeros or enter all zeros if no gateway is required then press #.
5. Enter the host bits if the reader will be communicating over a WAN, or leave the host bits set to 0 if not needed and then press #.
6. Press CLEAR twice to exit menu.

Subnet to Host Bits Conversions

The readers will only accept a host bit, so the subnet mask needs to be converted. The only legal subnet masks and host bits are listed below:

SUBNET MASK	HOST BITS
255.255.255.255	0
255.255.255.254	1
255.255.255.252	2
255.255.255.248	3
255.255.255.240	4
255.255.255.224	5
255.255.255.192	6
255.255.255.128	7
255.255.255.0	8
255.255.254.0	9
255.255.252.0	10
255.255.248.0	11
255.255.240.0	12
255.255.224.0	13
255.255.192.0	14
255.255.128.0	15
255.255.0.0	16
255.254.0.0	17
255.252.0.0	18
255.248.0.0	19
255.240.0.0	20
255.224.0.0	21
255.192.0.0	22
255.128.0.0	23
255.0.0.0	24

Installing the EN-200 Ethernet Adapter

➔ *The EN-100 Ethernet adapter is not field installable. Call the factory for installation.*

⚠ CAUTION: This procedure requires a cold boot. Back up all data with the host program before proceeding.

⚠ CAUTION: If the reader is equipped with an optional battery backup, remove the J7 jumper before proceeding. Failure to do so could lead to risk of shock and/or main board damage, if the ground strap were to touch the main board. See figure 9.

⚠ CAUTION: Before removing the back plate of reader, wear a grounding wrist strap to help aid in protecting the circuit board from any ESD damage that might occur from improper handling.

1. Unlock the reader and rotate.
2. Disconnect the power supply from the board.
3. Remove and tag all external connections to make correct re-attachment.
4. Remove HandReader from wall by sliding it to the right, away from the wall mount. See figure 1 below.

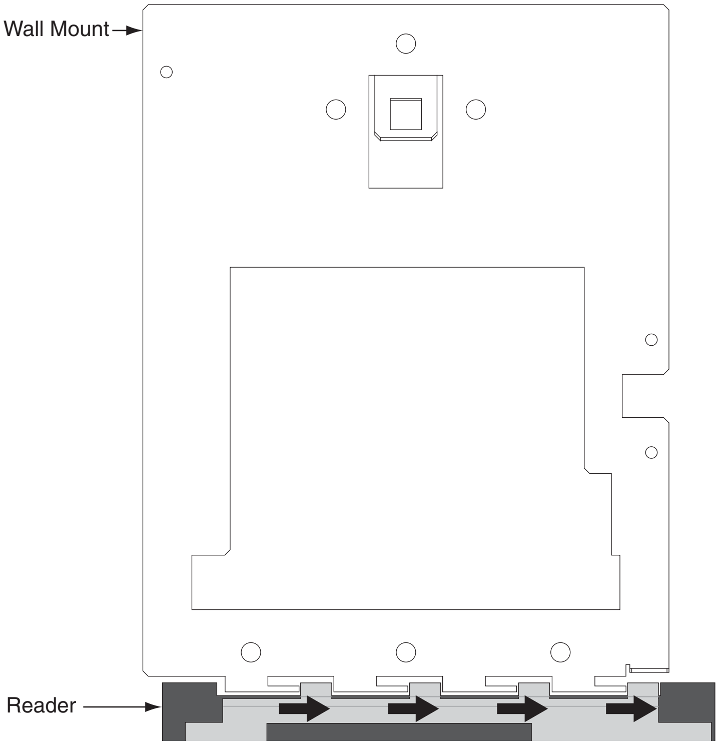


Figure 1

5. Set the reader on a firm surface such as a table. Remove the four screws that secure the back plate to the reader. Remove the grounding screw and/or ground lug (if present). See figure 2 below.

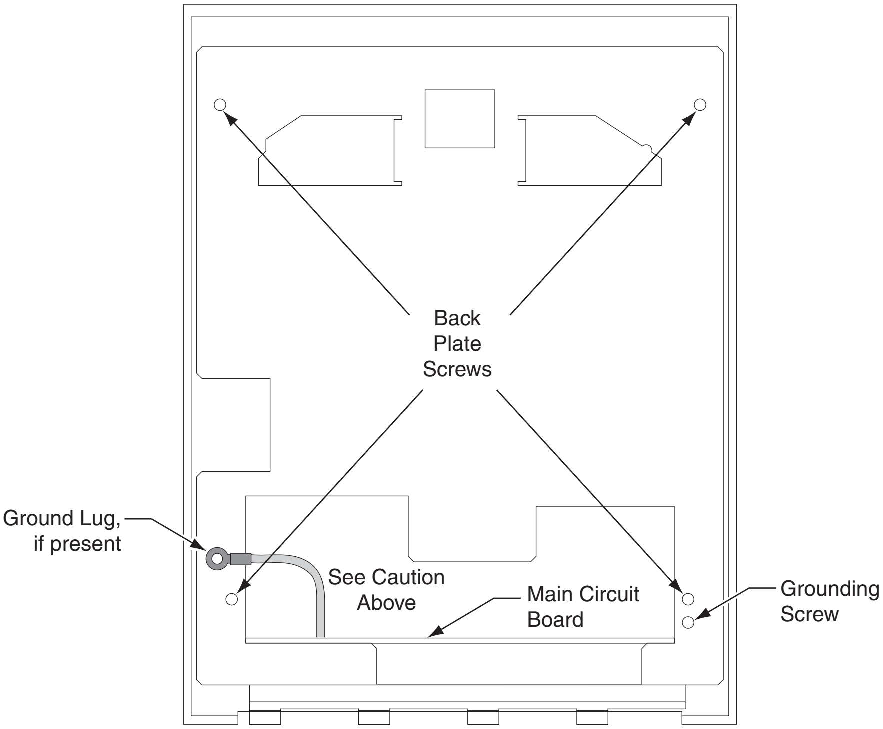


Figure 2

6. Carefully remove the back plate.

7. Locate the cable on the left side of the reader that runs from the top panel circuit board to the main circuit board. Disconnect this cable from J9 on the main circuit board. See “1” on figure 3. To remove the J9 connector from the main circuit board, depress the retaining clip on the connector and pull upwards. Take care to pull on the connector and to not pull on the cable. See figure 4 below.

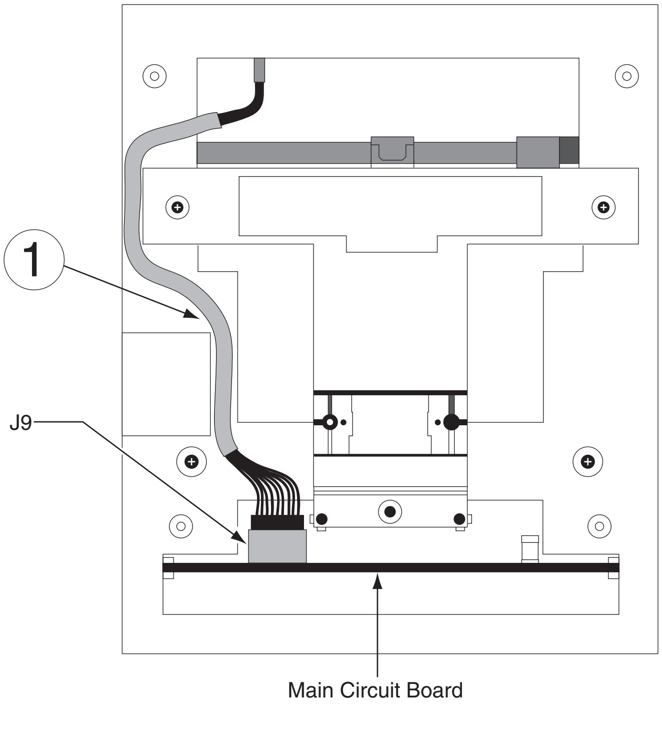


Figure 3

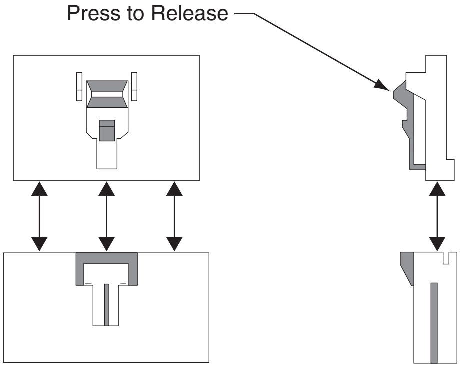


Figure 4

8. Carefully slide the main circuit board out until the ribbon cable between the camera assembly and J2 on the main circuit board is accessible. First, disconnect the J5 connector from the main board. To remove, depress the retaining clip on the J5 connector and pull upwards. See "2" on figure 5 below. Next, remove the ribbon cable from J2 by gently pulling up on this cable, being careful not to pull down as damage may occur to the camera assembly. See "3" on figure 5 below.

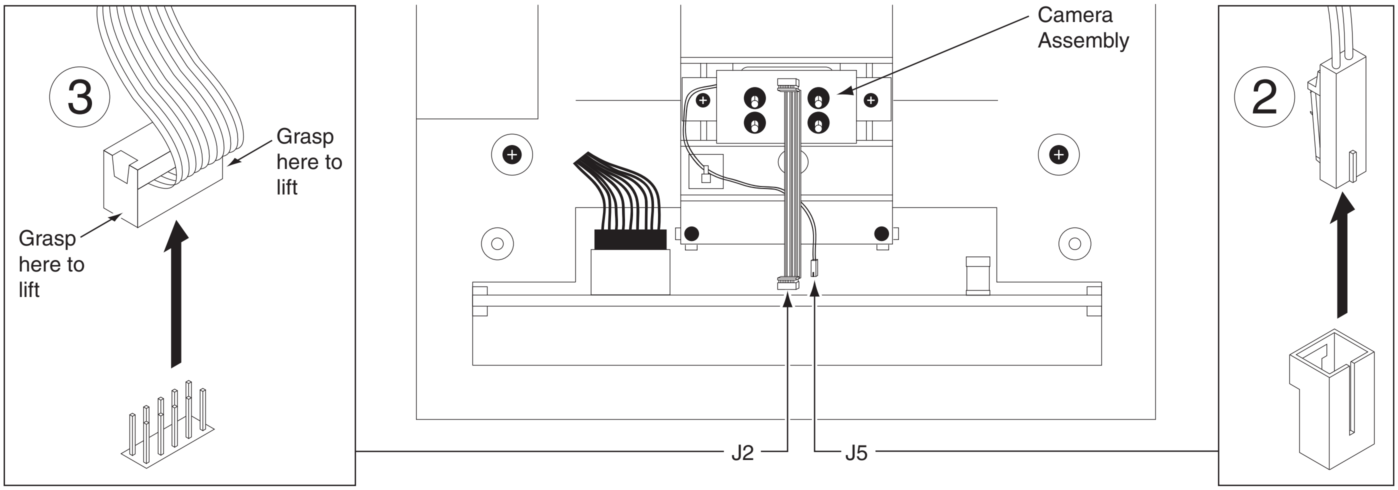


Figure 5

9. Carefully remove the main circuit board by sliding it free from the chassis.

10. Align the Ethernet adapter and carefully press the Ethernet card into place. Install the washers and nuts to secure the adapter. See figure 6 below.

CAUTION: Torque the 4-40 nuts to 4.5 – 5.5 in. lbs. (.51 - .62 Nm). Excessive torque may damage the circuit boards. After installing the Ethernet card, inspect for warped Ethernet or main PCBs.

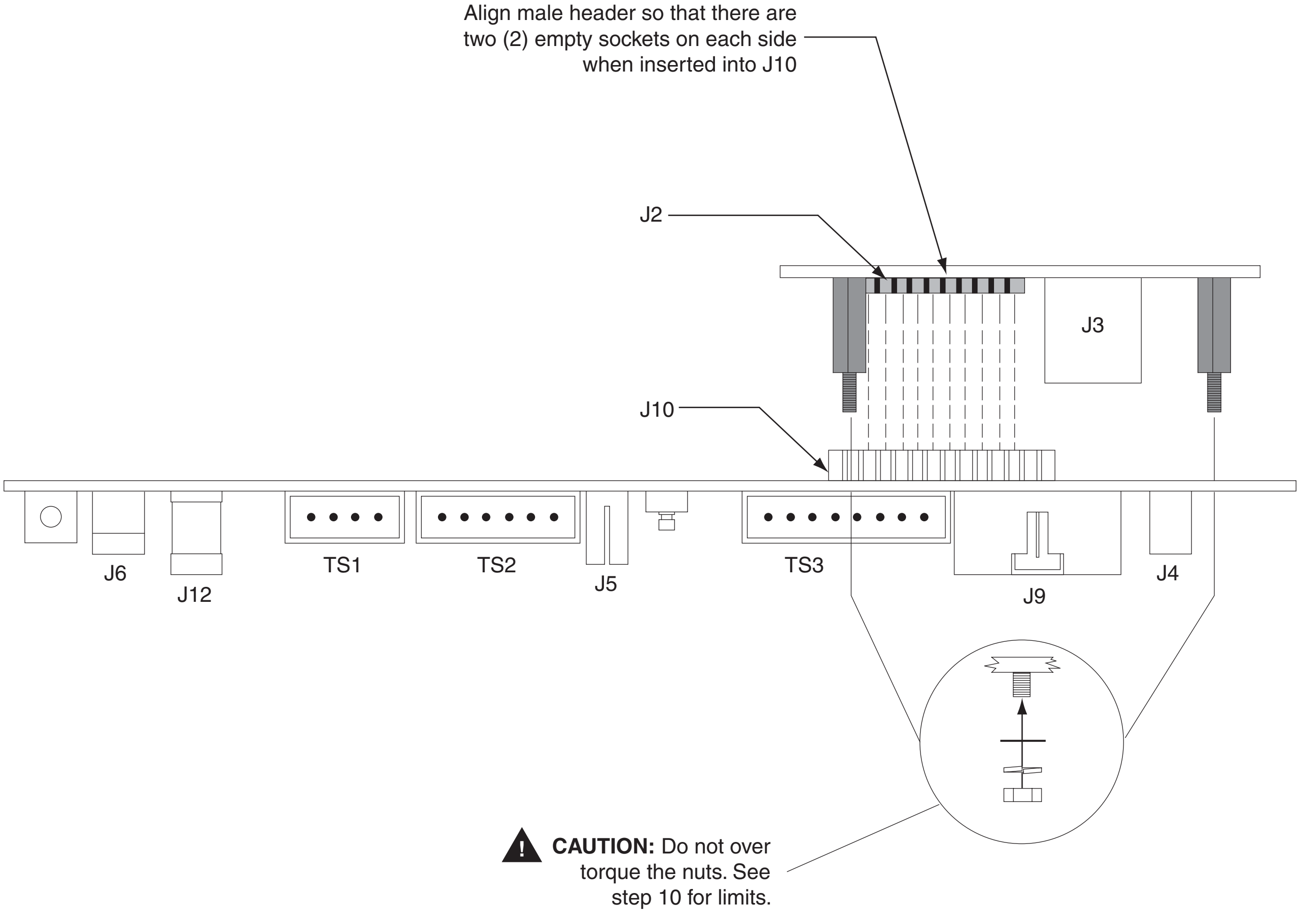

Align male header so that there are two (2) empty sockets on each side when inserted into J10
J2
J3
J10
J6
J12
TS1
TS2
J5
TS3
J9
J4
CAUTION: Do not over torque the nuts. See step 10 for limits.

Figure 6

11. Carefully slide the main circuit board back into the chassis using the guides to align the board correctly. Leave the main circuit board out about 1”.

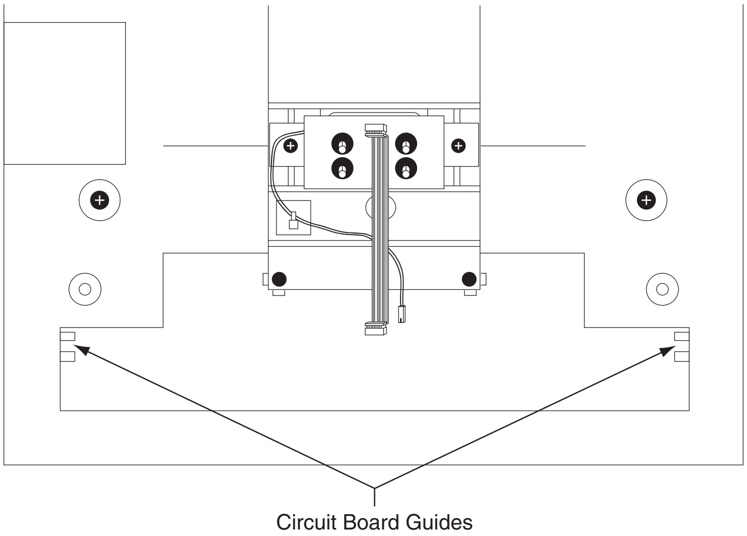


Figure 7

12. Attach the camera cable to J2 on the main circuit board. Take care to align the connector to the pins on the main circuit board and do not twist the cable, as this will damage the camera.

13. Plug in the J5 connector.

14. Locate the cable that runs from the top panel circuit board to the main circuit board. Connect this cable to J9 on the main circuit board. See figure 8 for cable routing.

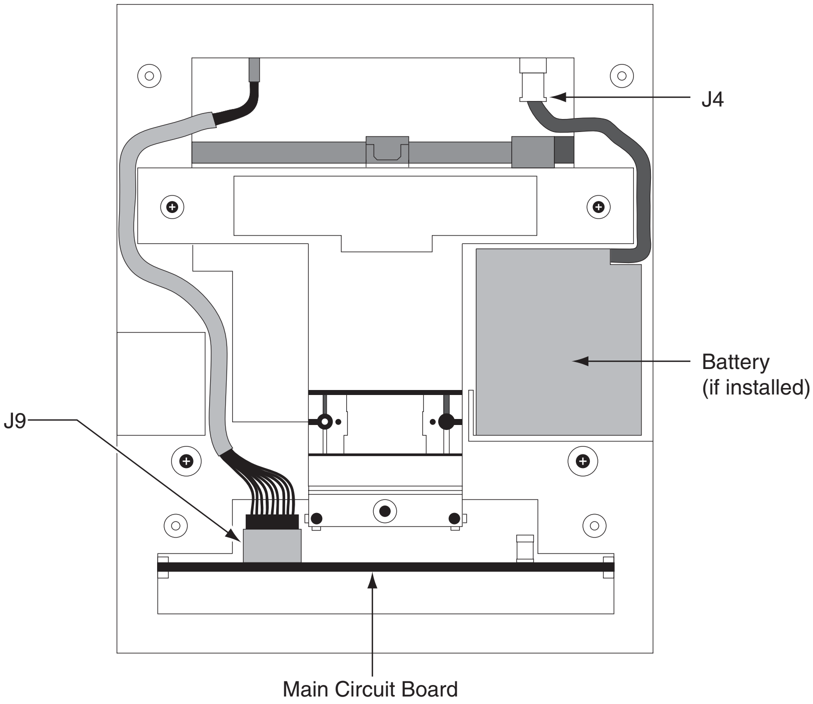


Figure 8

15. Slide the main circuit board in the rest of the way.
16. Replace the back plate. Attach the grounding screw to the main circuit board using the lower right hole on the back plate. If a ground lug is present, do not allow it to come into contact with J7. Secure the back plate with the four screws removed in step 5.
17. Line up the slots at the bottom of the reader's back with the four hinge pins at the bottom of the wall mount. Slide the reader to the left so the pins go in the slots. This fastens the reader to the wall and wall mount and forms a hinge.
18. Reconnect all external connections removed in step 3.
19. Hold down reset button and apply power. Once the reader has booted up, release the reset button.
20. Press "9" on the keypad to complete the reset when prompted.
21. Reconnect the J7 jumper (if applicable).

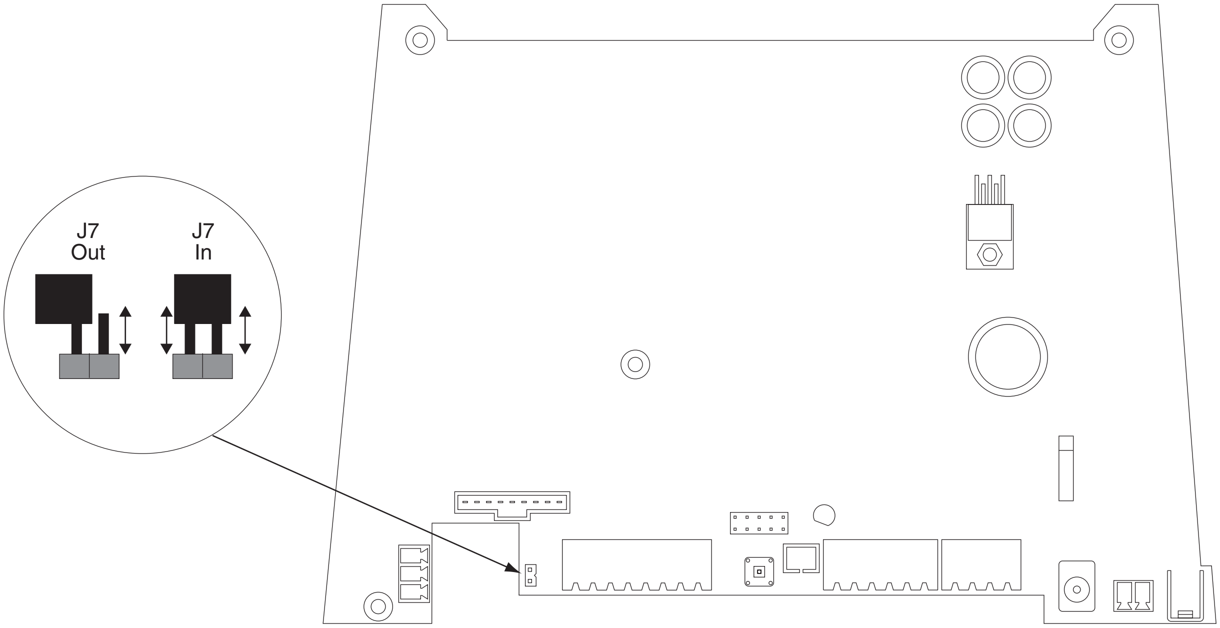


Figure 9

22. Secure the unit to wall mount with key. Upgrade is completed.

What do the LEDs on the Ethernet adapter mean?

1. Steady red or yellow LED:
   - This means the Ethernet adapter has finished booting up but has not tried to detect a network cable plugged in.
2. Red or yellow flashing:
   - This means the Ethernet cable is not plugged in or no network is detected.
3. Red or yellow and green LEDs are both flashing:
   - This means the Ethernet cable has been detected but IP address entered at the reader has not been sent to the Ethernet adapter yet. This status is normally not seen as this process happens quickly.
4. Steady green:
   - This means communication with the network has been established but the host program has not contacted the Ethernet adapter yet.
5. Green flashing:
   - This means everything is ready and messaging can occur when initiated by the host program.

(877) 671-7011
Printed in Country

70200-0014

F Series Ethernet Upgrade

Installation Instructions

Ethernet Requirements

- A TCP/IP network
- CAT 5 cable or better
- 10baseT
- Static IP address, gateway and subnet addresses (if needed)
- Port 3001 must be opened

Power Up

A reader with an Ethernet adapter installed and the network cable plugged in will automatically detect the presence of the Ethernet adapter upon power up. If the network cable is not plugged in prior to power being applied, the Ethernet adapter will not see the network and the reader will ask if the cable is plugged in. Plug in the network cable and power cycle the reader. When the reader boots up and detects the network, the LCD will display an IP address and then proceed to either the “Enter ID” or “Ready” prompt.

Address Requirements

The EN-100/200 does not support DHCP; therefore a static IP address is required and must be programmed into the reader before the adapter will communicate with the network.

Obtain all addresses that are required for the network from the system administrator of the site. If there is no need for a gateway address, set it to all zeros (i.e. 000.000.000.000). If the reader is required to communicate over a WAN, the subnet mask needs to be converted to a host bit number. If a subnet mask is not needed, set the host bit to 0. Have the system administrator set Port 3001 to allow access on all switches and routers between the EN-100/200 and host program.

To configure the Ethernet adapter, follow these steps:

1. The reader’s IP address resides in the SET SERIAL command of the SETUP menu, which is by default in the menu 2 of the reader.
2. Press # when the LCD display shows.

```
SET SERIAL
* NO  YES #
```

3. Enter the 12 digit IP address using leading zeros and press #.
4. Enter the 12 digit gateway using leading zeros or enter all zeros if no gateway is required then press #.
5. Enter the host bits if the reader will be communicating over a WAN, or leave the host bits set to 0 if not needed and then press #.
6. Press CLEAR twice to exit menu.

Subnet to Host Bits Conversions

The readers will only accept a host bit, so the subnet mask needs to be converted. The only legal subnet masks and host bits are listed below:

SUBNET MASK	HOST BITS
255.255.255.255	0
255.255.255.254	1
255.255.255.252	2
255.255.255.248	3
255.255.255.240	4
255.255.255.224	5
255.255.255.192	6
255.255.255.128	7
255.255.255.0	8
255.255.254.0	9
255.255.252.0	10
255.255.248.0	11
255.255.240.0	12
255.255.224.0	13
255.255.192.0	14
255.255.128.0	15
255.255.0.0	16
255.254.0.0	17
255.252.0.0	18
255.248.0.0	19
255.240.0.0	20
255.224.0.0	21
255.192.0.0	22
255.128.0.0	23
255.0.0.0	24

Installing the EN-200 Ethernet Adapter

➔ *The EN-100 Ethernet adapter is not field installable. Call the factory for installation.*

⚠ **CAUTION: This procedure requires a cold boot. Back up all data with the host program before proceeding.**

⚠ **CAUTION: If the reader is equipped with an optional battery backup, remove the J7 jumper before proceeding. Failure to do so could lead to risk of shock and/or main board damage, if the ground strap were to touch the main board. See figure 9.**

⚠ **CAUTION: Before removing the back plate of reader, wear a grounding wrist strap to help aid in protecting the circuit board from any ESD damage that might occur from improper handling.**

1. Unlock the reader and rotate.
2. Disconnect the power supply from the board.
3. Remove and tag all external connections to make correct re-attachment.
4. Remove HandReader from wall by sliding it to the right, away from the wall mount. See figure 1 below.

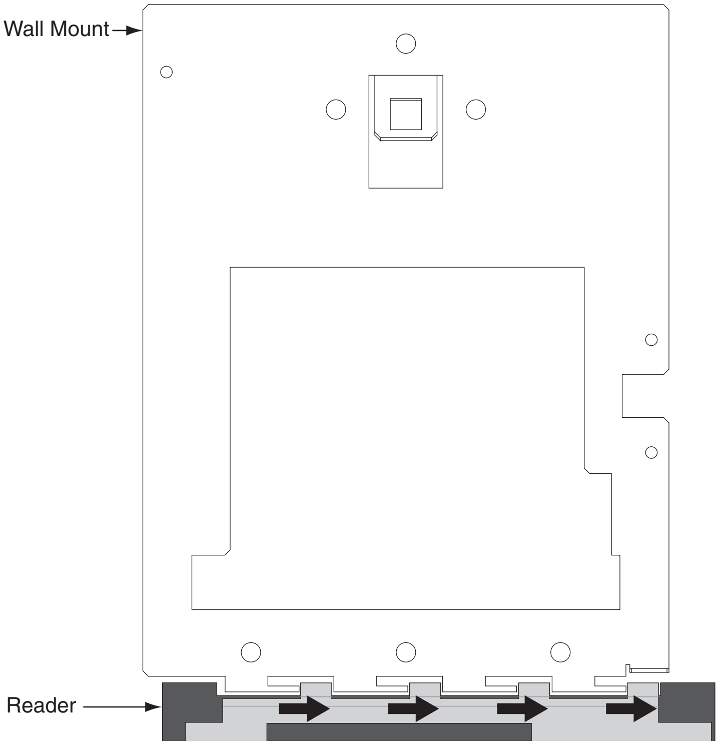


Figure 1

5. Set the reader on a firm surface such as a table. Remove the four screws that secure the back plate to the reader. Remove the grounding screw and/or ground lug (if present). See figure 2 below.

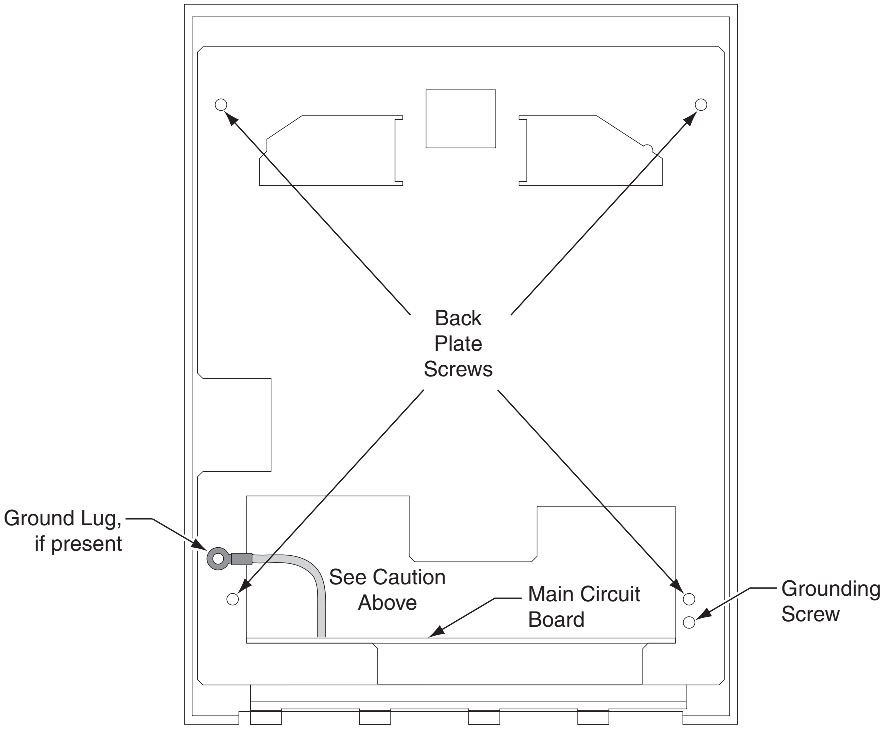


Figure 2

6. Carefully remove the back plate.

7. Locate the cable on the left side of the reader that runs from the top panel circuit board to the main circuit board. Disconnect this cable from J9 on the main circuit board. See “1” on figure 3. To remove the J9 connector from the main circuit board, depress the retaining clip on the connector and pull upwards. Take care to pull on the connector and to not pull on the cable. See figure 4 below.

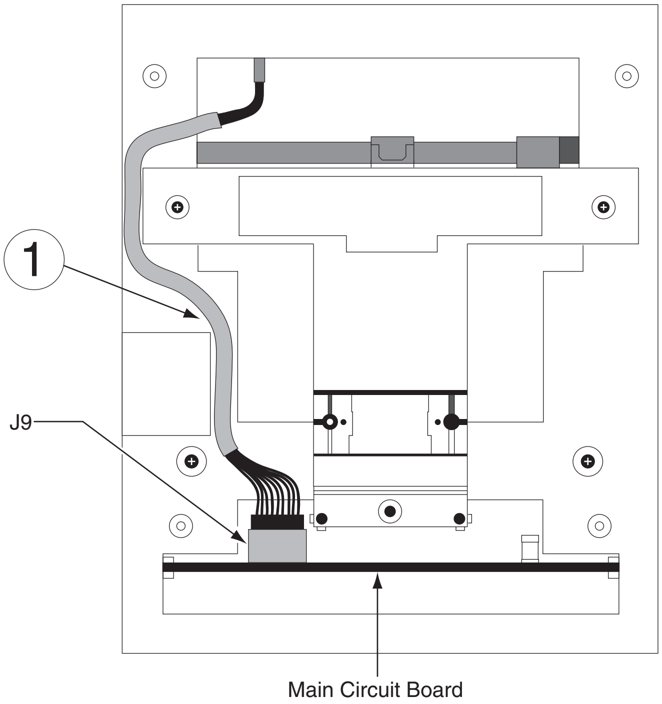


Figure 3

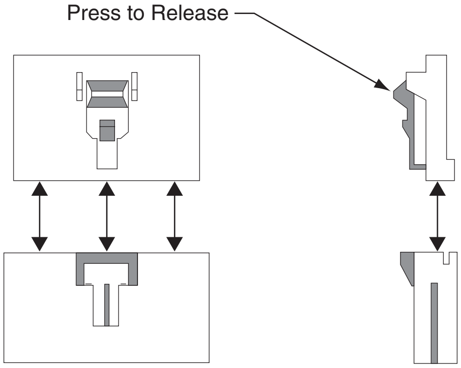


Figure 4

8. Carefully slide the main circuit board out until the ribbon cable between the camera assembly and J2 on the main circuit board is accessible. First, disconnect the J5 connector from the main board. To remove, depress the retaining clip on the J5 connector and pull upwards. See “2” on figure 5 below. Next, remove the ribbon cable from J2 by gently pulling up on this cable, being careful not to pull down as damage may occur to the camera assembly. See “3” on figure 5 below.

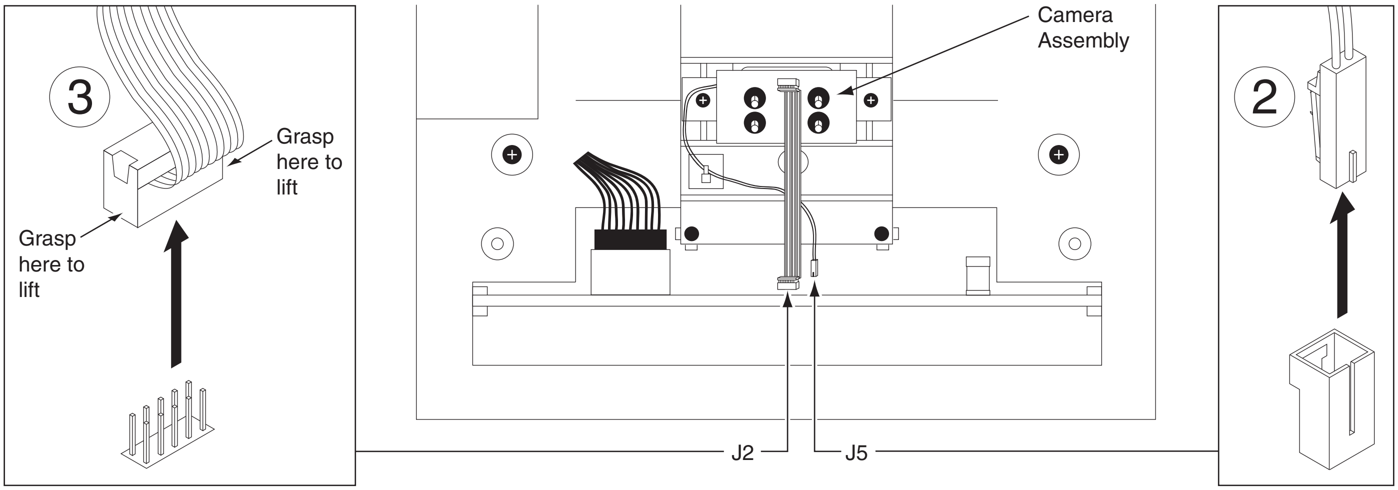


Figure 5

9. Carefully remove the main circuit board by sliding it free from the chassis.

10. Align the Ethernet adapter and carefully press the Ethernet card into place. Install the washers and nuts to secure the adapter. See figure 6 below.

⚠ CAUTION: Torque the 4-40 nuts to 4.5 – 5.5 in. lbs. (.51 - .62 Nm). Excessive torque may damage the circuit boards. After installing the Ethernet card, inspect for warped Ethernet or main PCBs.

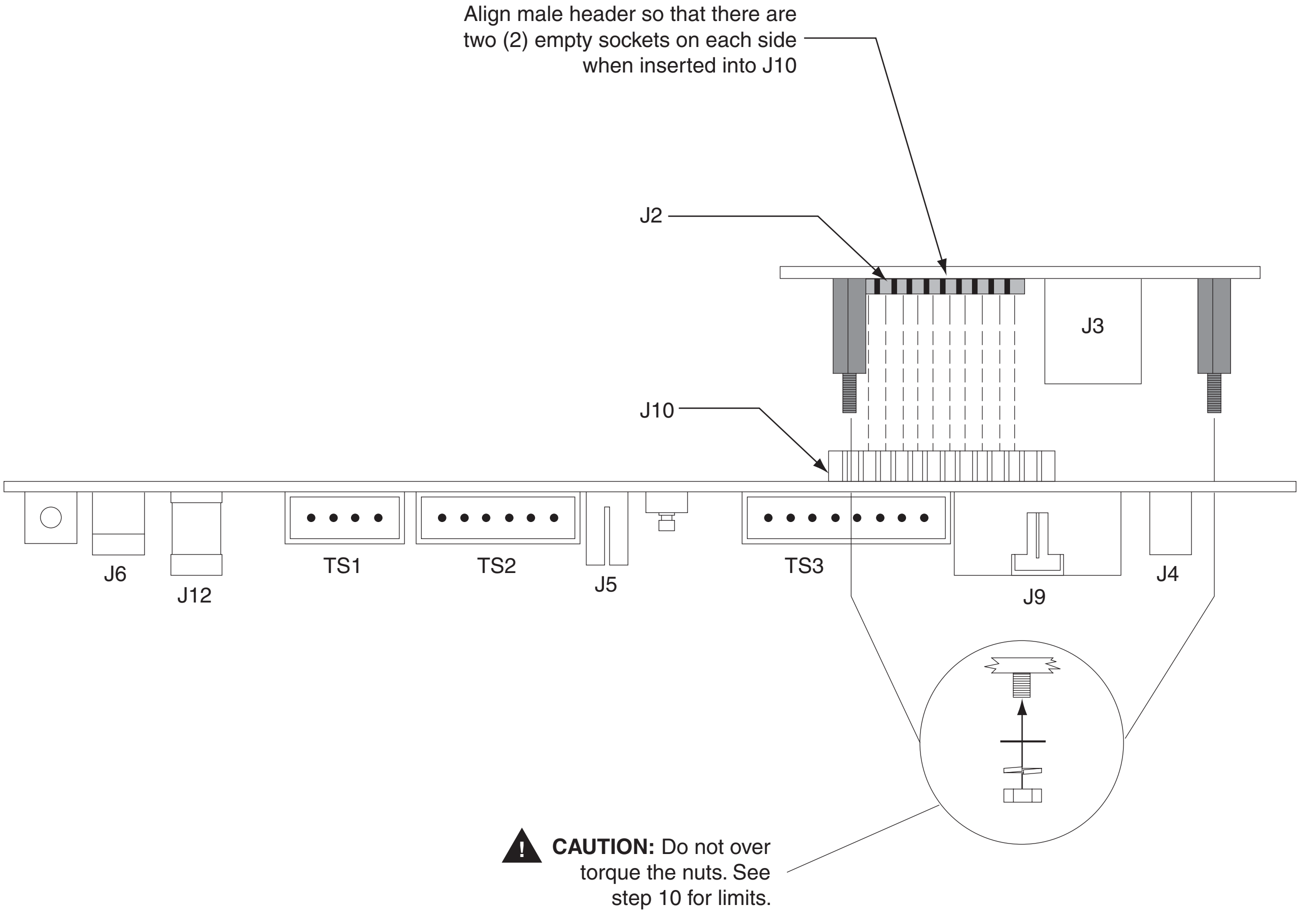

Align male header so that there are two (2) empty sockets on each side when inserted into J10
J2
J3
J10
J6
J12
TS1
TS2
J5
TS3
J9
J4
⚠ CAUTION: Do not over torque the nuts. See step 10 for limits.

Figure 6

11. Carefully slide the main circuit board back into the chassis using the guides to align the board correctly. Leave the main circuit board out about 1”.

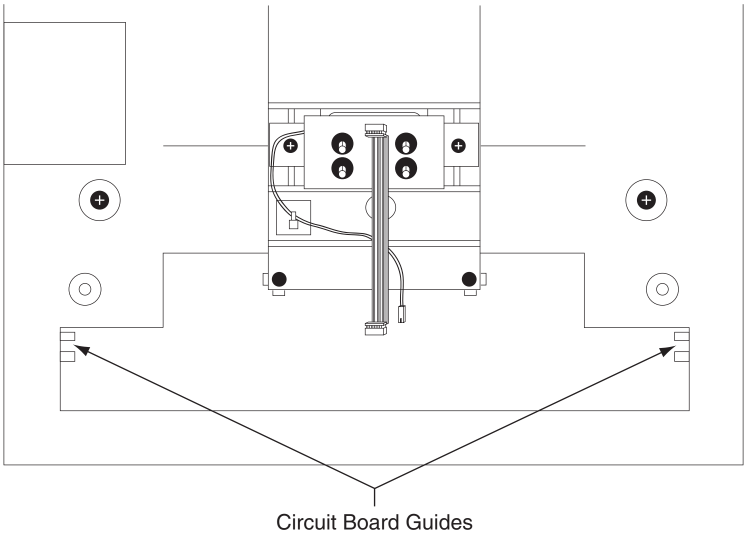


Figure 7

12. Attach the camera cable to J2 on the main circuit board. Take care to align the connector to the pins on the main circuit board and do not twist the cable, as this will damage the camera.

13. Plug in the J5 connector.

14. Locate the cable that runs from the top panel circuit board to the main circuit board. Connect this cable to J9 on the main circuit board. See figure 8 for cable routing.

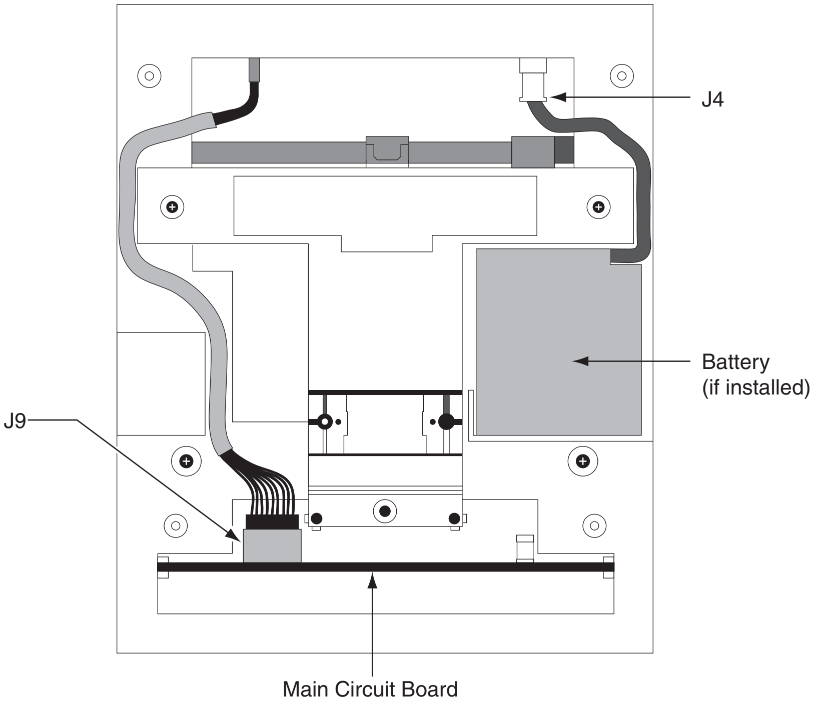


Figure 8

15. Slide the main circuit board in the rest of the way.
16. Replace the back plate. Attach the grounding screw to the main circuit board using the lower right hole on the back plate. If a ground lug is present, do not allow it to come into contact with J7. Secure the back plate with the four screws removed in step 5.
17. Line up the slots at the bottom of the reader's back with the four hinge pins at the bottom of the wall mount. Slide the reader to the left so the pins go in the slots. This fastens the reader to the wall and wall mount and forms a hinge.
18. Reconnect all external connections removed in step 3.
19. Hold down reset button and apply power. Once the reader has booted up, release the reset button.
20. Press "9" on the keypad to complete the reset when prompted.
21. Reconnect the J7 jumper (if applicable).

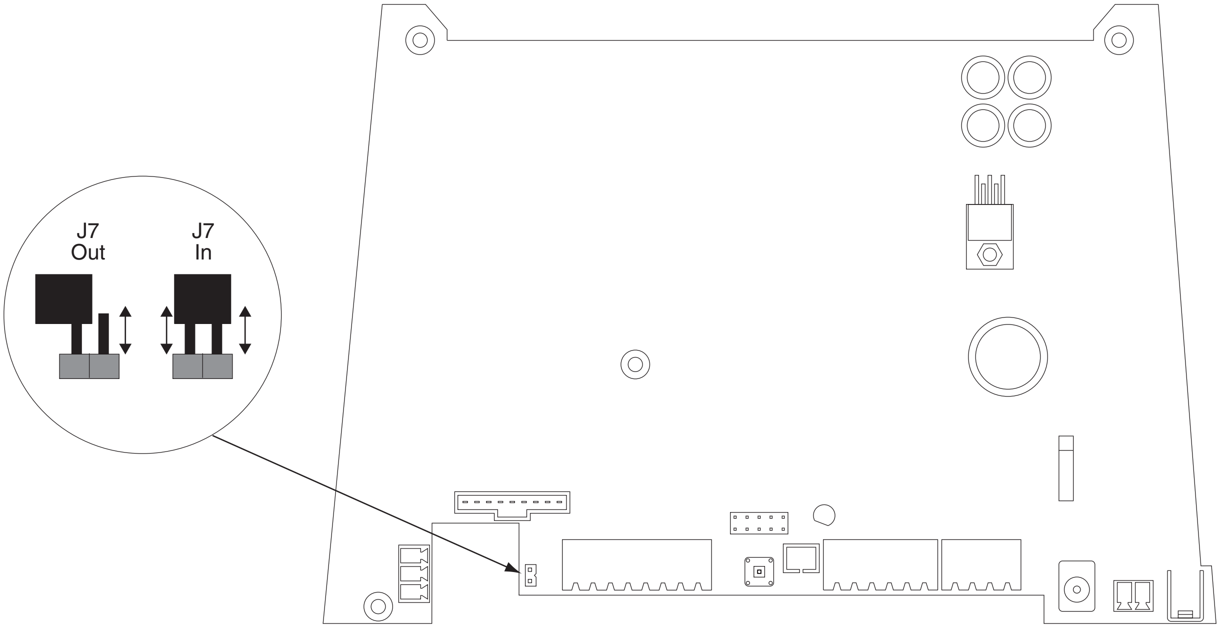


Figure 9

22. Secure the unit to wall mount with key. Upgrade is completed.

What do the LEDs on the Ethernet adapter mean?

1. Steady red or yellow LED:
   - This means the Ethernet adapter has finished booting up but has not tried to detect a network cable plugged in.
2. Red or yellow flashing:
   - This means the Ethernet cable is not plugged in or no network is detected.
3. Red or yellow and green LEDs are both flashing:
   - This means the Ethernet cable has been detected but IP address entered at the reader has not been sent to the Ethernet adapter yet. This status is normally not seen as this process happens quickly.
4. Steady green:
   - This means communication with the network has been established but the host program has not contacted the Ethernet adapter yet.
5. Green flashing:
   - This means everything is ready and messaging can occur when initiated by the host program.

70100-6101

Outdoor Reader

Installation Instructions

TABLE OF CONTENTS

OUTDOOR READER INSTALLATION

About the Outdoor Reader

The outdoor reader unit has two separate components:

- The case (called the *weather shield*) protects the reader from bad weather.
- The *HandReader* is able to function in much colder weather than regular readers when ordered with an internal heater (INT-HTR).

How the HandReader and internal heater work

In cold weather, when one places a hand on the HandReader, a mist forms around the hand. This distorts the image so the reader doesn't recognize the hand. To prevent this problem, the HandReader can be ordered with an internal heater. To accommodate the heater in the platen, the HandReader uses a 24 VDC, 2 amp power supply; this is different from the power supply for indoor readers.

UL Disclaimer

The reader is UL approved for indoor use only.

INSTALLATION INSTRUCTIONS

Before you start the installation

Before you start installing the reader and weather shield, pick an appropriate location for the reader. (See the reader manual for more information about where to locate the reader in relation to the door.)

Also make sure that you are familiar with local building codes that affect this installation and that you have the appropriate tools and fasteners.

Tools you will need for the installation

a. To install the reader, you need:

- A level
- A measuring tape
- A Phillips screwdriver
- A drill with ¼ and ½ inch bits

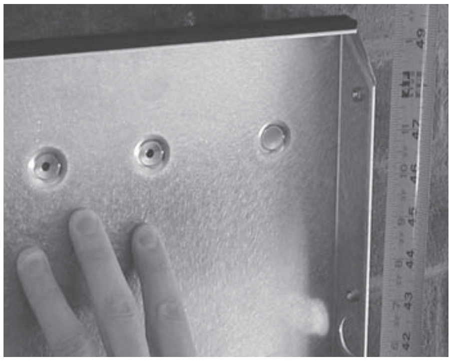
b. Materials you must provide

- wiring raceways approved by local code
- the appropriate fasteners to secure the reader to the wall

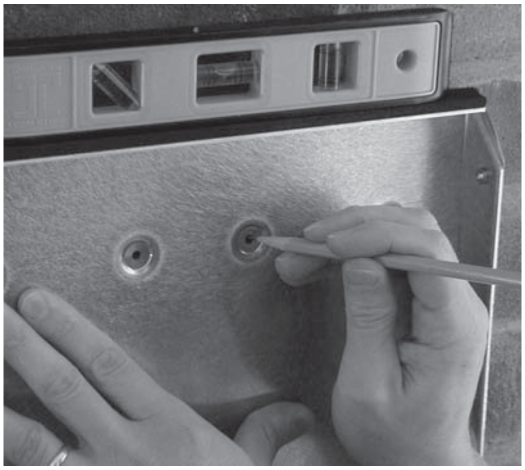
Installing the weather shield's back panel and wall mount

1. Hold the weather shield's back panel against the wall so the top of it is 49.5 inches (126 cm) from the floor or ground.

   When the installation is done, this will put the reader platen 40 inches (roughly 102 cm) from the ground.



2. Make sure the top of the back panel is level.
3. Mark the location of the five screw holes (two on the top and three on the bottom). Also mark the location of the wiring hole if you plan to run the wiring straight through the wall.

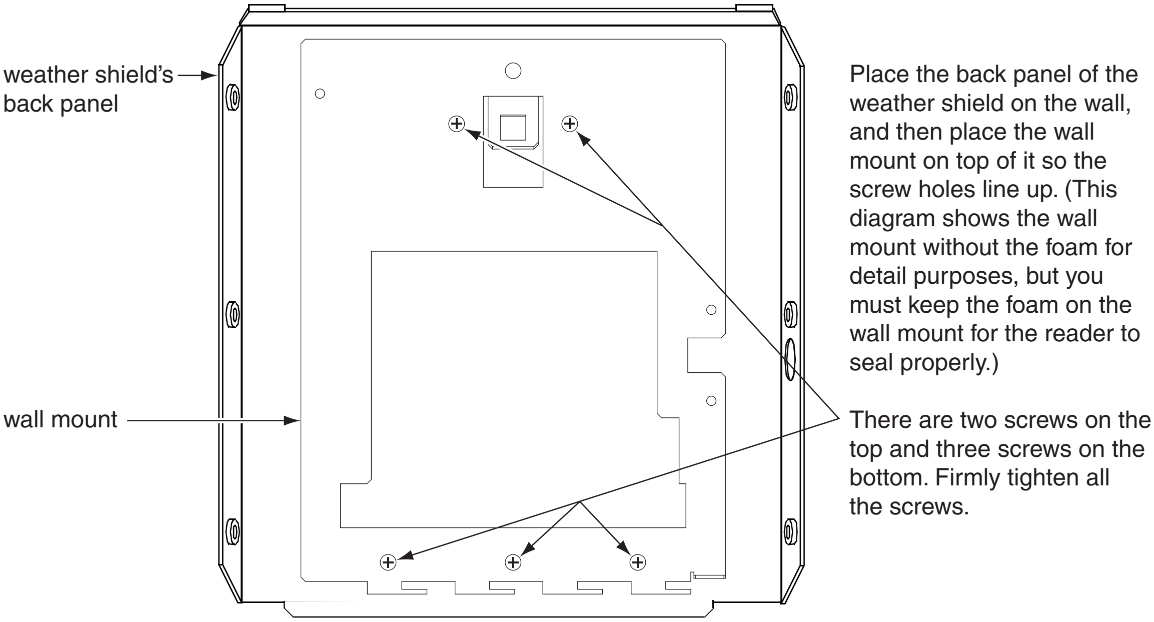


4. If needed, drill holes for each of the holes that you marked.

The size of the holes and the method you use to fasten the weather shield's back panel and wall mount to the wall depends on the type of wall, on the fasteners you have, and on any local building code requirements.

- **For wooden walls:** You may need to drill pilot holes for your screws so you don't split the wood.
- **For hollow walls:** You will probably want to use toggle bolts or some similar type of fastener designed for hollow walls. The size of the holes you need depends on the fastener.
- **For a solid wall (e.g., brick or masonry):** It's most common to use ¼ inch expansion anchors. Drill ¼ inch diameter holes that are ¼ inch deeper than the anchors.

5. Screw the weather shield's back panel and the wall mount to the wall.



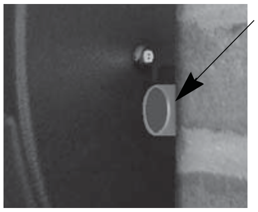
Place the back panel of the weather shield on the wall, and then place the wall mount on top of it so the screw holes line up. (This diagram shows the wall mount without the foam for detail purposes, but you must keep the foam on the wall mount for the reader to seal properly.)

There are two screws on the top and three screws on the bottom. Firmly tighten all the screws.

6. If you will use surface conduit to bring the wiring to the reader, notch the side of the weather shield and reader at the appropriate places. (Skip this step if your wiring will come straight through the wall.)

   To find the location for the hole in the weather shield, put the case on the back panel and mark the location of the conduit hole on the right side of the weather shield's back panel.

   The location for the hole is already marked on the reader (on the left side if you are looking at it from the back).



Make a notch in the side of the case so it lines up with the hole for the conduit in the side of the weather shield's back panel.

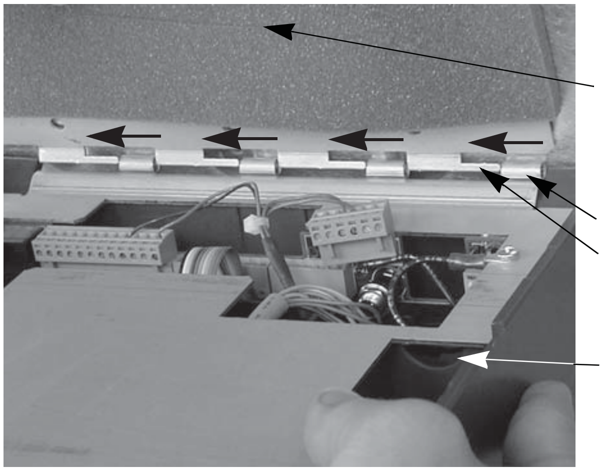
Running the wiring

7. Run the wiring for the reader, but don't connect the wires to the green terminal connectors yet.

- Make sure that you follow all local electrical codes in bringing the wiring to the reader.
- See the reader manual for wiring instructions.
- See step 9 before you connect the green terminal connectors.
- Make sure that you use an appropriate power supply. The HandReader with heated platen uses a 24 VDC, 2 amp power supply rather than the 12± volt power supply that regular readers use.

Mounting the reader

8. Line up the slots at the bottom of the reader's back with the four hinge pins at the bottom of the wall mount. Slide the reader to the left so the pins go in the slots. This fastens the reader to the wall and wall mount and forms a hinge.



Wiring that comes through the wall passes through this slit.

These slots slide over these pins, fastening the reader to the wall mount and forming a hinge.

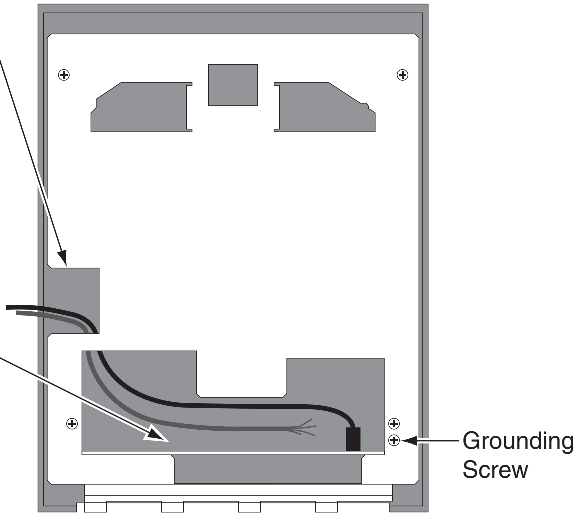
If using surface conduit, all wiring must pass through this hole (see step 9).

9. Connect the wiring and power to the reader.

   If you are using surface conduit: *Make sure all the wires pass through this hole in the reader before you connect the wires to the green terminal connectors. The green terminal connectors won't fit through this hole, and the wires must pass through this hole so they don't get pinched when you close the case.*

   If the wiring will come through the back of the reader: *The wires enter directly into the wiring area through the slit in the black foam. This is the easiest way to do the wiring.*

   See the reader manual for instructions on which wires must connect to which terminal pins.



10. Put the key in the lock on the side of the reader, turn the key clockwise, close the reader, and then turn the key counterclockwise to lock the reader.

    Don't try to shut the reader without using the key; this will bend the locking mechanism.

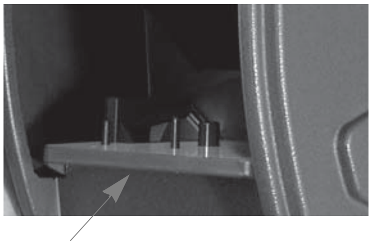
11. Test the reader to make sure it is wired and communicating correctly.

    Do this prior to installing the weather shield; you can't open the reader back up to adjust wiring or connections with the weather shield in place.

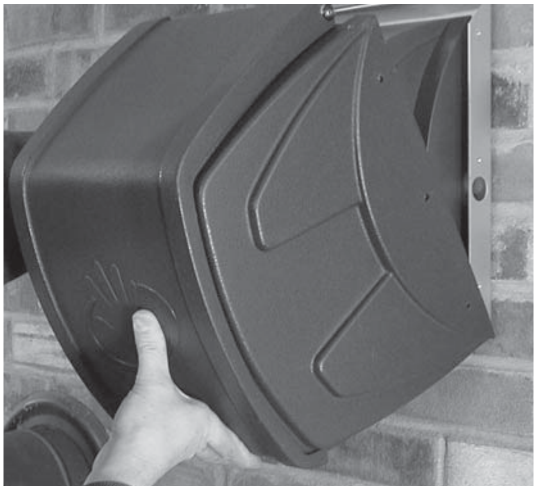
Mounting the weather shield over the reader

12. Place the weather shield over the reader. You must place the bottom of the case on first and then push in the top.

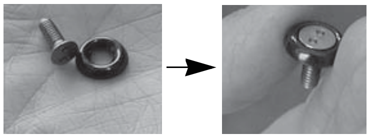
    The bottom of the case must go on first so the lip at the bottom of the opening slips under the platen rather than sliding in front of it.



Make sure the lip at the bottom of the opening in the weather shield slips under the platen.

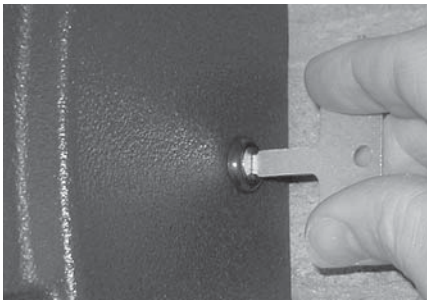


13. Put a washer on each of the six screws.



14. Use the tool with two small prongs on the end to insert the screws that hold the weather shield onto the weather shield’s back plate.

    This tool provided with the reader may be slightly different than the key shown in this picture.



15. If needed, use the RTV sealant we provided to seal any places on the top or sides where water might get behind the weather shield.

    The black pad on the back side of the weather shield’s back panel adequately seals the back on a flat wall, but on brick, clapboards, or other surfaces that aren’t flat, use the sealant to fill any gaps.

    Do NOT caulk the bottom of the case! In cool damp weather, moisture can condense inside the weather shield. Leaving the bottom uncaulked lets any water droplets that form run out instead of collecting inside the case.

Ingersoll Rand
Security Technologies

(877) 671-7011
Printed in Country

70200-0028

F Series HandPunch Top Panel Assembly Replacement

Installation Instructions

The following instructions apply to all F Series HandReader versions.

⚠ **CAUTION:** **The circuit boards within the HandReader are ESD sensitive. Observe proper ESD precautions when handling the unit.**

⚠ **CAUTION:** **This procedure requires erasing the existing hand templates. Save the existing hand templates before proceeding.**

1. Unlock the HandReader and rotate. See figure 6 on the last page of this instruction.

⚠ **CAUTION:** **If the unit is equipped with the optional battery backup, remove the J7 jumper before proceeding. See figure 2 on the next page for location of J7.**

2. Disconnect the power supply from the board.
3. Remove and tag all external connections to make correct re-attachment.

4. Remove HandReader from wall by sliding it to the right, away from the wall mount. See figure 1 below.

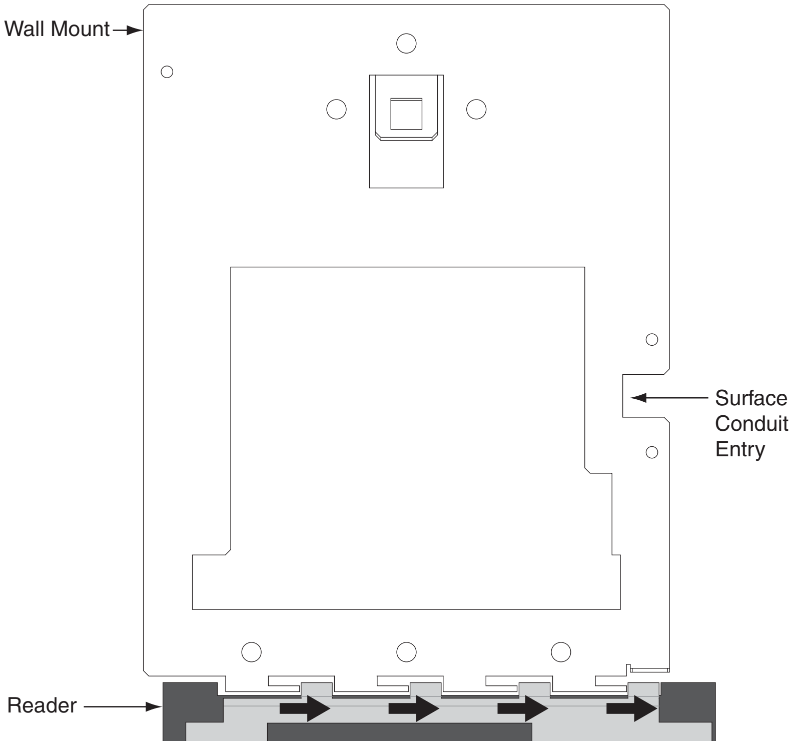


Figure 1

⚠ CAUTION: Before removing back plate of reader, wear a grounding wrist strap to help aid in protecting the circuit board from any ESD damage that might occur from improper handling.

5. Set the reader on a firm surface such as a table. Remove the four screws that secure the back plate to the HandReader. Remove the grounding screw and/or ground lug (if present). See figure 2 below.

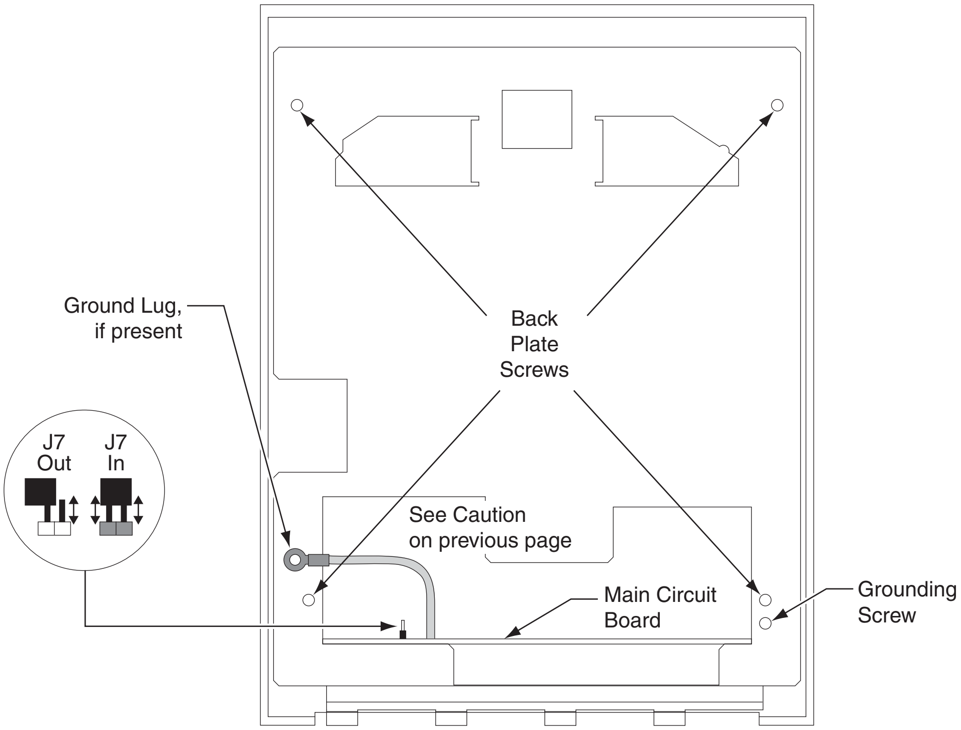


Figure 2

6. Locate the cable that runs from the top panel PCB to the main circuit board. Disconnect this cable from J3 on the top panel PCB. To remove the J3 connector on the top panel PCB, depress the retaining clip on the connector and pull downwards. If the optional battery backup is installed, disconnect the battery cable from J4 on the top panel PCB. See figures 3 and 4 below.

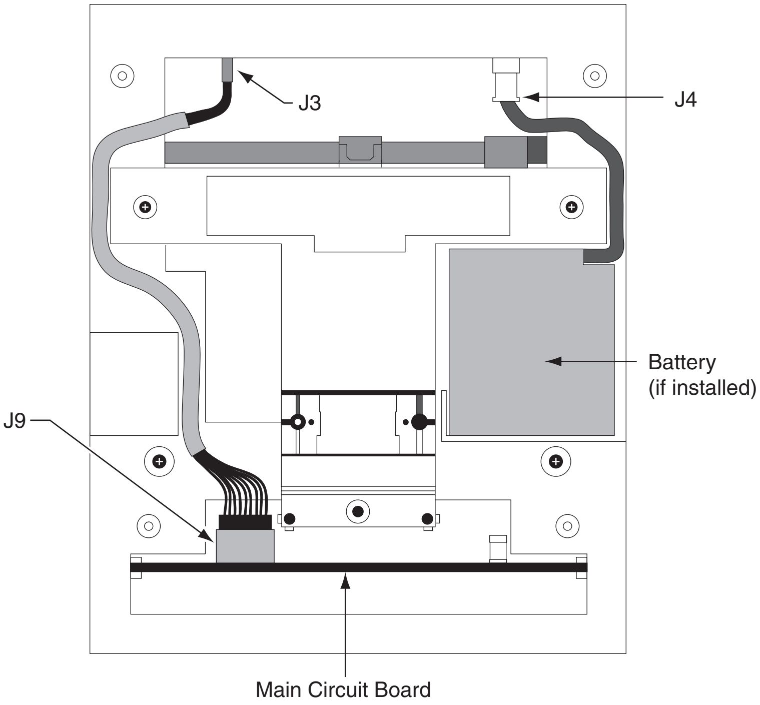


Figure 3

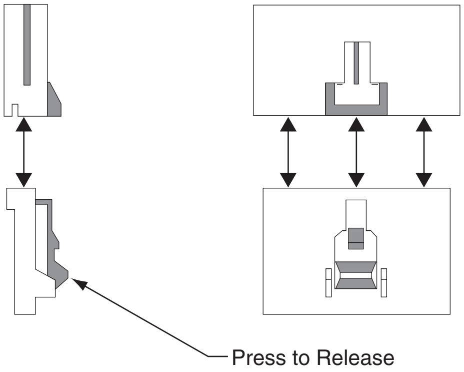


Figure 4

7. Remove the two screws that hold the top panel assembly to the front case. Carefully slide the top panel out from the front case. See figure 5 below.

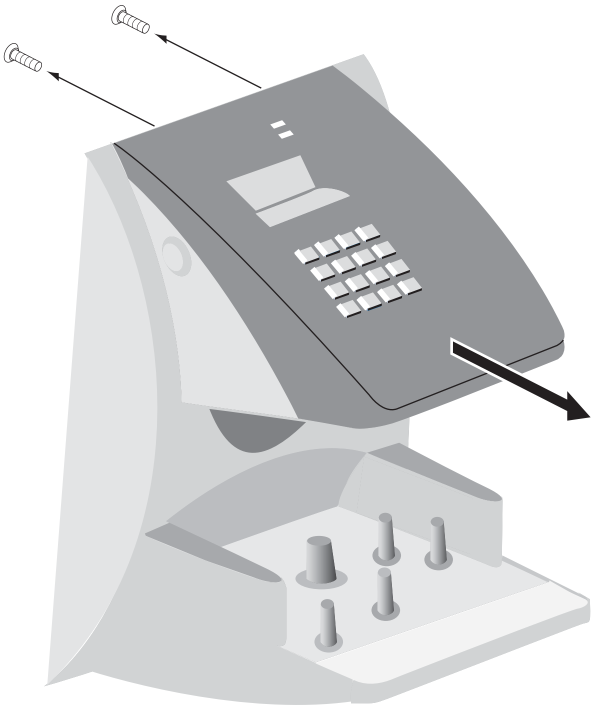


Figure 5

8. Carefully align and install the new top panel assembly. Secure with the two screws removed in step 7 above.

⚠ CAUTION: Torque the top panel screws to 3.8 – 4.4 in. lbs. (.43 - .49 Nm). Excessive torque may damage the screw bosses in the top panel.

9. Locate the cable that runs from the main circuit board to the top panel PCB. Route the cable as shown in figure 3. Re-insert the connector into J3 on the top panel PCB. Make sure the connector snaps into J3.

⚠ **CAUTION: If the battery backup option is installed, replace the J7 jumper. Be sure that both pins of J7 are shorted by the jumper. See figure 2. Re-connect the battery cable to J4 on the top panel PCB. See figures 3 and 4.**

10. Replace the back plate. Attach the grounding screw to the main circuit board using the lower right hole on the back plate. If a ground lug is present, do not allow it to come into contact with J7. Secure the back plate with the four screws removed in step 5.

⚠ **CAUTION: Torque the back plate screws to 3.8 – 4.4 in. lbs. (.43 - .49 Nm). Excessive torque may damage the screw bosses on the front case.**

11. To re-install the HandReader, reverse steps 1 – 4.

⚠ **CAUTION: Do not force the HandReader onto the wall mount when the latch is in the locked position.**

12. With the key in the unlocked position, rotate the HandReader back upright. Turn the key counter-clockwise to lock the HandReader into place. See figure 6 below.

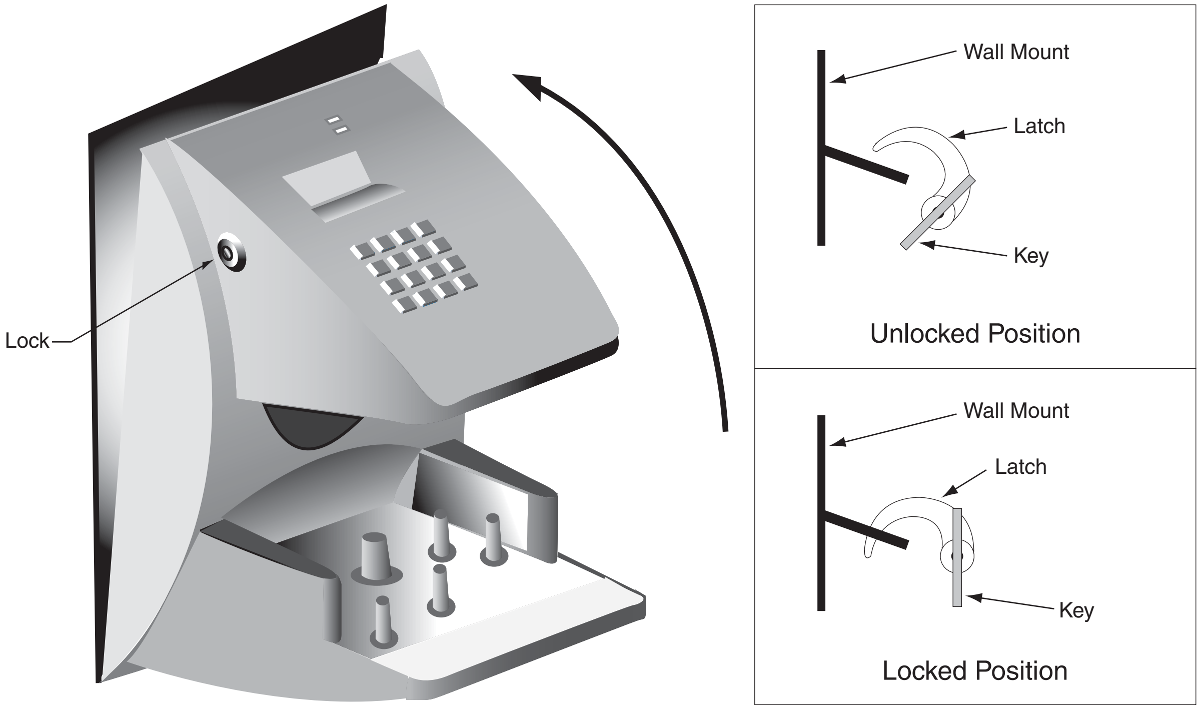


Figure 6

Ingersoll Rand
Security Technologies

70200-0093

S-BB-BAT
Spare Backup Battery

Installation Instructions

SCHLAGE

The F Series family of readers uses an internal switching regulator to obtain internal operational power via an internal lead acid battery and a power fail protection PCB or onboard circuitry. With the latter in use, switchover to battery power is automatic and occurs when the main input voltage falls to approximately 10.5 volts. At that state, the internal battery charger is disabled to save power and uninterrupted operation continues on battery power. When input power is restored, the unit switches off of battery operation and the battery charger is re-enabled to recharge the battery. A fully discharged battery requires approximately 12 hours of charge to fully recover. Additional options installed and specific configurations within the unit make it difficult to predict precisely how long battery support will last, but in general two hours of battery operation is not unreasonable. While operating on battery backup, the reader will shut down when the battery voltage reaches approximately 9.5 volts. This is done to prevent full exhaustion of the battery. A yellow indicator on the top panel illuminates to indicate that the unit is running off of battery power. This indicator extinguishes when main input power is restored.

Placement of the shunt/jumper on J7 on the main logic board enables or disables battery operation on those units equipped with an optional battery backup. To fully power down a unit equipped with battery backup, remove or reposition shunt J7 so that the two pins protruding up from the main logic board are not connected to each other. Main input power can then be removed and the unit will fully shut down. If shunt/jumper on J7 is not properly installed, the internal backup battery will not be charged, and in the event of a main input power loss, the unit will shut down.

⚠ **CAUTION: This procedure requires erasing the existing hand templates. Save the existing hand templates before proceeding.**

1. Unlock the reader and rotate.
2. Disconnect the power supply from the board.
3. Remove and tag all external connections to make correct re-attachment.
4. Remove HandReader from wall by sliding it to the right, away from the wall mount. See figure 1 below.

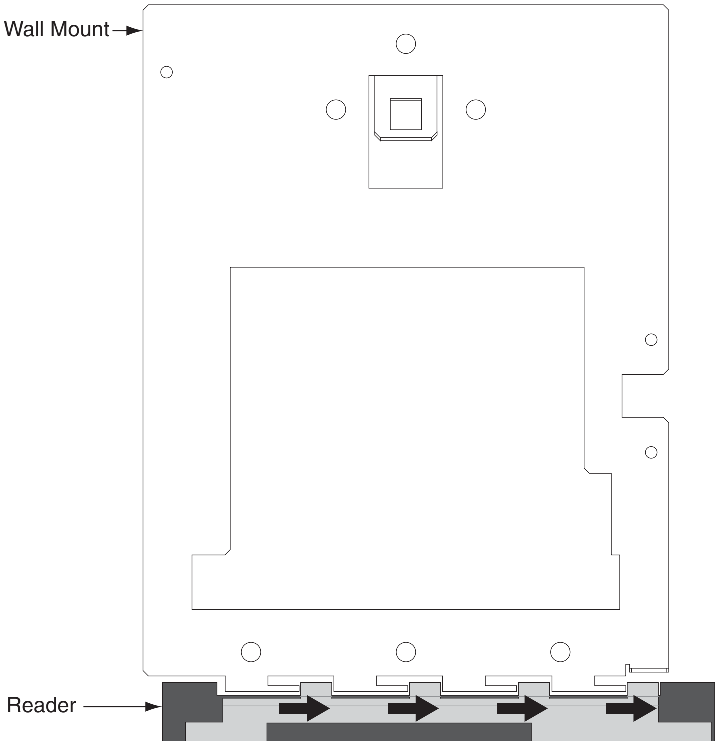


Figure 1

⚠ **CAUTION: Before removing back plate of reader, wear a grounding wrist strap to help aid in protecting the circuit board from any ESD damage that might occur from improper handling.**

5. Set the reader on a firm surface such as a table. Remove the four screws that secure the back plate to the HandReader. Remove the grounding screw and/or ground lug (if present). See figure 2 below.

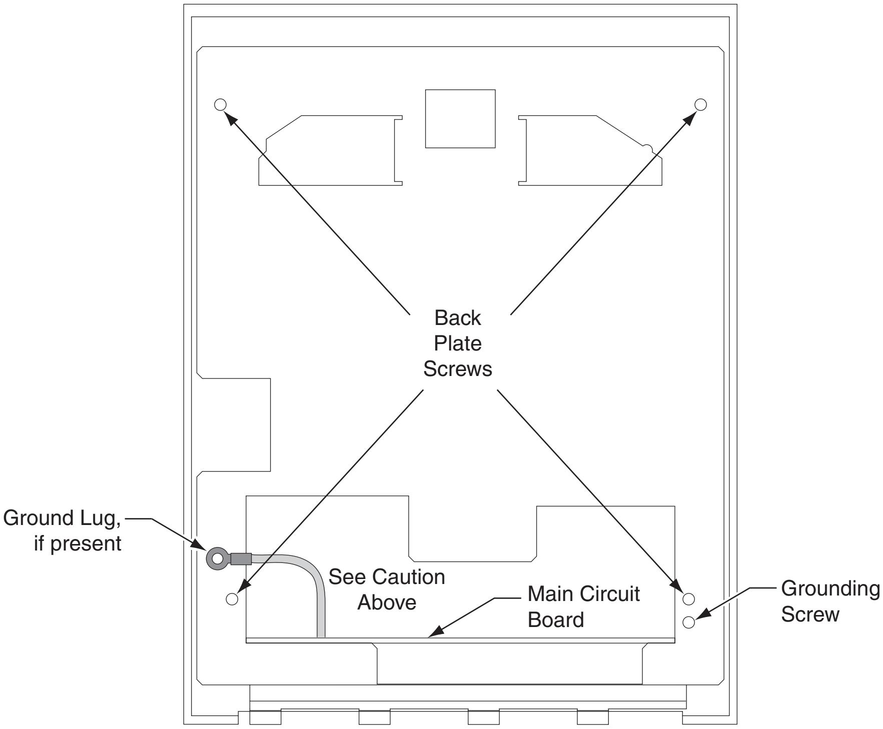


Figure 2

6. Remove the back plate.
7. Install the battery into the chassis. Route the cable as shown and attach to J4 on the top panel PCB as shown in figure 3 below.

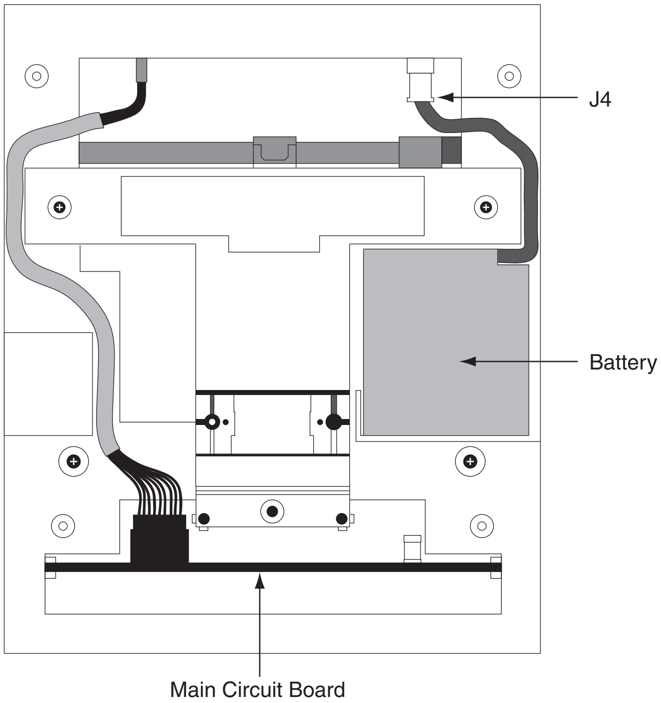


Figure 3

8. Reinstall the back plate onto the chassis. Reinstall grounding screw and/or ground lug (if present). Do not allow ground lug to come into contact with J7. Secure the back plate with the four screws removed in step 5.
9. Line up the slots at the bottom of the reader's back with the four hinge pins at the bottom of the wall mount. Slide the reader to the left so the pins go in the slots. This fastens the reader to the wall and back plate and forms a hinge.
10. Reconnect cables removed in step 3.

11. If not already installed, install the J7 jumper (if applicable). See figure 4 below.

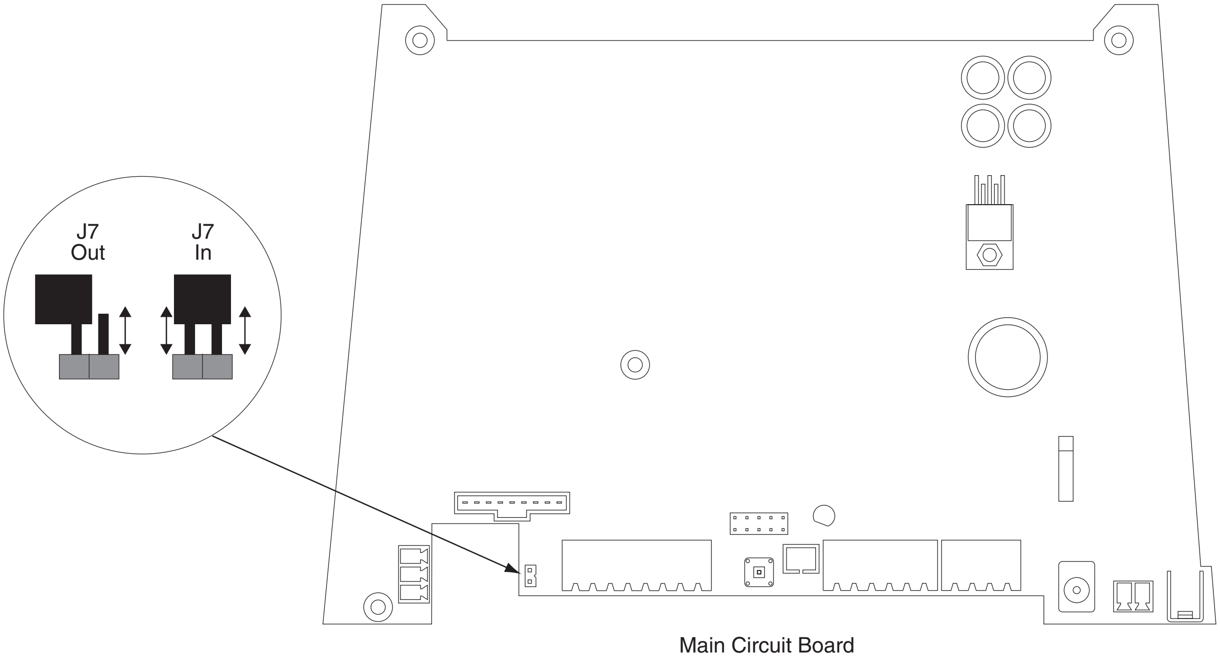


Figure 4

12. Power up the unit.

13. Secure the unit to wall mount with key. Upgrade is completed.

(877) 671-7011
Printed in Country

Wi-Fi 3rd Party Use: F-Series & G-Series

This document stands to act as a procedural guide for when using a 3rd party Wi-Fi adapter with the HandReaders, both F-Series & G-Series[1]. Schlage has performed testing to confirm that when using a Wi-Fi adapter[2], the HandReader will operate normally; so long as connections and addresses are properly set. Please use the following instructions as a guideline for initial set up of the Wi-Fi adapter.

Setup Summary of the Wireless Router and Bridge:

Host --> Switch --> Primary Wireless Router --> Wireless Router (Repeater/Bridge) --> HandReader[3]

Repeater/Bridge Setup

1. Configure the wireless router with LAN connection from the computer
   a. Set the computer to static IP mode
      i. i.e. Set the wireless router address to 192.168.0.1
      ii. i.e. Set the computer IP address to 192.168.0.100
2. Set the wireless router to repeater/bridge mode
   a. Need to make sure the primary wireless router address is different from repeater/bridge router
      i. i.e. Set the primary wireless router to 192.168.1.1
      ii. i.e. Set the repeater/bridge router to 192.168.1.10
3. Ensure that the DHCP server is disabled on the repeater/bridge router
4. Set the repeater/bridge router to connect to the primary wireless router by using security password
5. Connect a HandReader to the repeater/bridge router LAN port
   a. The GT-400 can be set either DHCP or static IP
   b. The F-Series HandReaders can be set as static IP

[1] F-Series models include: all HandPunch & HandKey models that have Ethernet enables. G-Series includes the GT-400.
[2] Wireless N150 Router: Encore 3G Mobile Broadband Wireless N150 Router plus Repeater, ENHWI-3GN3
[3] Note that the Host and the HandReaders are on the same network.

70200-0029

F Series Wall Mount Replacement

Installation Instructions

The following instructions apply to all F Series HandReader versions.

1. Unlock the reader and rotate.
2. Disconnect the power supply from the board.
3. Remove and tag all external connections.
4. Remove HandReader from wall by sliding it to the right, away from the wall mount. See figure 1 below.

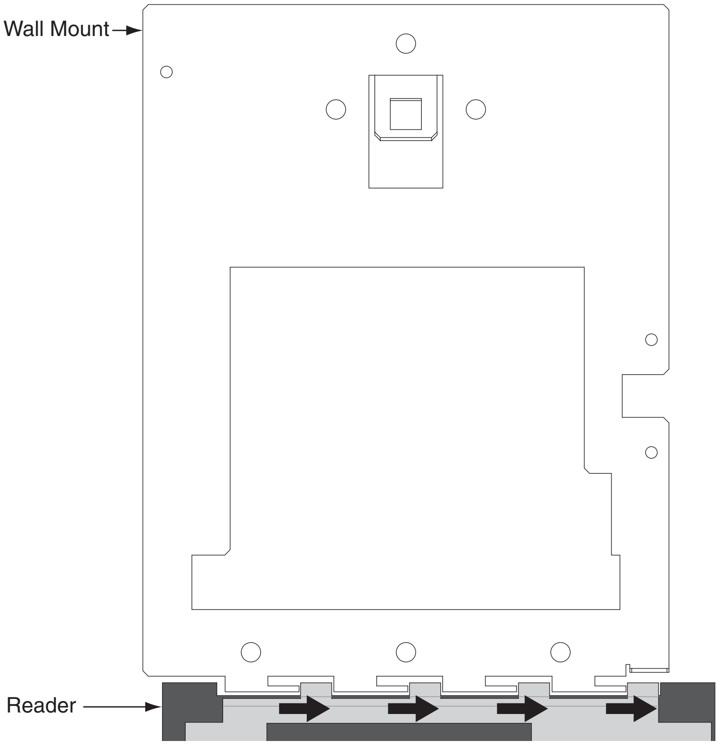


Figure 1

5. Remove the five screws that hold the wall mount in place. See figure 2 below.
6. Either hang the new wall mount or the paper template at the same height as the original wall mount. The wall mount must hang 48½" from the floor as measured from the top center hole on the panel. Ensure that the bottom line of the new wall mount/template is horizontal to the floor. Mark the locations of the five new screw holes.

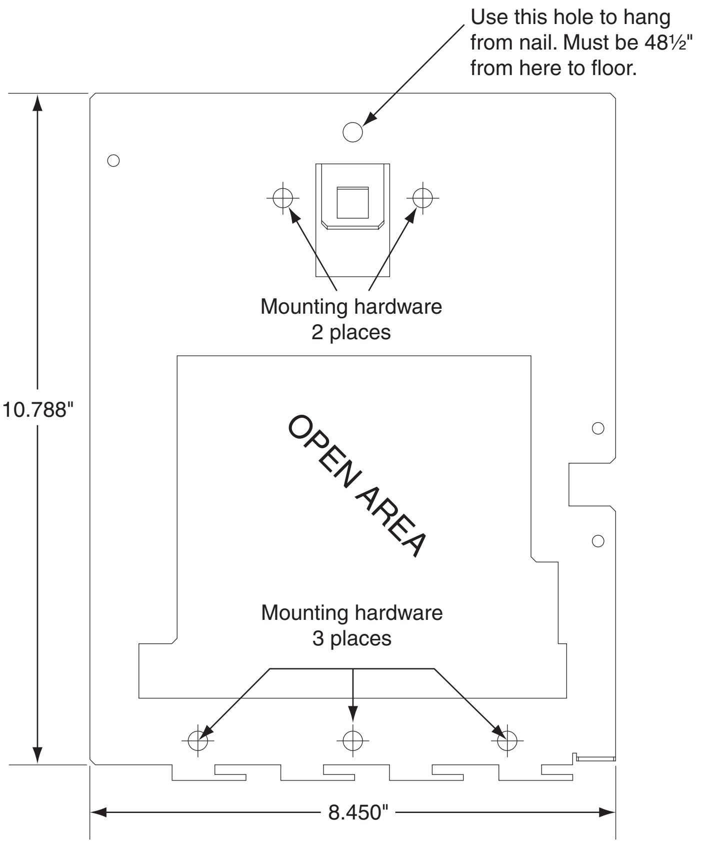


Figure 2

7. Install the new mounting hardware to the wall. Place the new wall mount panel against the wall, and install the panel.
8. Line up the slots at the bottom of the reader's back with the four hinge pins at the bottom of the wall mount. Slide the reader to the left so the pins go in the slots. This fastens the reader to the wall and wall mount and forms a hinge. See figure 3 below.

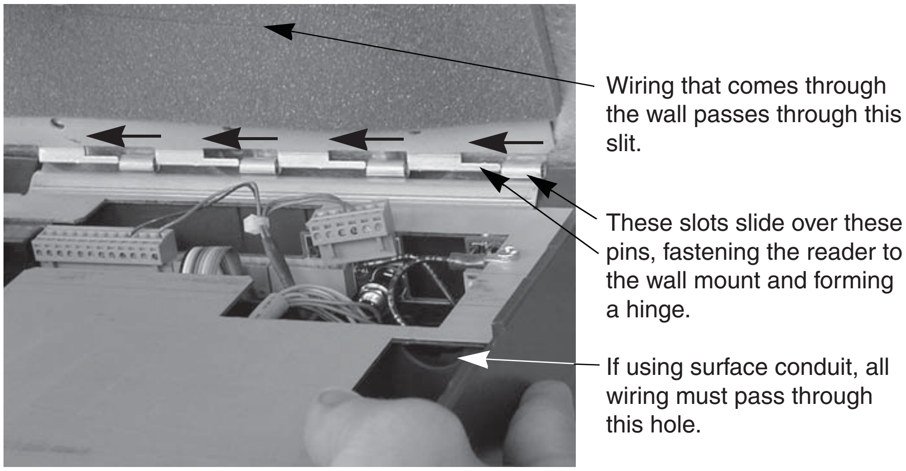

Wiring that comes through the wall passes through this slit.
These slots slide over these pins, fastening the reader to the wall mount and forming a hinge.
If using surface conduit, all wiring must pass through this hole.

Figure 3

9. Reconnect all cables removed in step 3 above.
10. Rotate the HandReader back towards the wall, and lock the unit into place with key.

SCHLAGE

ALLEGION

3rd Party Biometric Testing on the HandReader

The HandReader has existed for over 20 years and has seen consistent and superior biometric performance. However, some error rates seen at a particular site are very dependent on several factors, most notably:

- population
- training and habituation
- threshold setting

Due to the variability of factors involved at individual sites, Allegion does not quote static performance rates. However, we often refer customers to two well-respected tests run by independent third-parties. The attached documents describe test methodology and state the corresponding performance metrics. Customers with similar use case environments can reasonably expect similar results.

In brief summary, the attached reports will show the following 3-try results:

a.	Type I error rate (false rejection rate) -		
	as low as	<0.1% (Sandia)	0.25% (CESG)
b.	Type II error rate (false acceptance rate) -		
	as low as	0% (Sandia)	0.001% (CESG)
c.	Crossover error rate (CER) -		
	as low as	0.1% (Sandia)	0.5% (CESG)

The two reports are attached for your reference.

CESG Biometric Product Testing Final Report
Sandia Report

CESG contract X92A/4009309

Biometric Product Testing Final Report

Issue 1.0
19 March 2001

Tony Mansfield
Gavin Kelly
David Chandler
Jan Kane

Centre for Mathematics and Scientific Computing
National Physical Laboratory
Queen’s Road
Teddington
Middlesex
TW11 0LW

Tel: 020 8943 7029
Fax: 020 8977 7091

EXECUTIVE SUMMARY

This is a report of a performance evaluation of seven biometric systems conducted by NPL over the period May to December 2000. The test programme was sponsored by the Communications Electronics Security Group (CESG) as part of their Biometrics Work Programme in support of the "Modernising Government" and other initiatives.

The objectives of the test programme were:
- To show the level of performance attainable by a selection of biometric systems;
- To determine the feasibility of demonstrating satisfactory performance through testing;
- To encourage more testing to be sponsored, and to promote methodologies contributing to the improvement of biometric testing.

Face, Fingerprint, Hand Geometry, Iris, Vein and Voice recognition systems were tested for a scenario of positive identification in a normal office environment, with cooperative non-habituated users. The evaluation was conducted in accordance with the "Best Practices in Testing and Reporting Performance of Biometric Devices" produced by the UK Government Biometrics Working Group, and used 200 volunteers over a three-month period.

Results presented include:
- Failure to Enrol and Failure to Acquire Rates;
- The trade-off between matching errors (False Match Rate vs. False Non Match Rate) and between decision errors (False Acceptance Rate vs False Rejection Rate) over a range of decision criteria;
- Throughput rates of users in the live application, and of the matching algorithm in off-line processing;
- Sensitivity of the systems' performance to environmental conditions, and the differences in performance over different classes of users.

Biometric system performance is dependent on the application, environment and population. Therefore the performance results presented here should not be expected to hold for all other applications, or in all environmental conditions. In particular caution should be exercised when comparing these results with those of other systems tested under different conditions.

CONTENTS

FIGURES

TABLES

1 INTRODUCTION

1. This is a report of a performance evaluation of seven biometric systems conducted by NPL over the period May to December 2000. The test programme was sponsored by the Communications Electronics Security Group (CESG) as part of their Biometrics Work Programme in support of the "Modernising Government" and other initiatives.

2. The test programme had three main objectives:
   a. To show the level of performance attainable by a selection of biometric systems;
   b. To determine the feasibility of demonstrating satisfactory performance through testing;
   c. To encourage more testing to be sponsored, and to promote methodologies contributing to improvement of biometric testing.

3. The tests provide factual, vendor-independent data on the performance of biometric devices. This will inform CESG on the general capability of biometric technology, and will help in the development of policy on the use of biometrics in Government. It will also assist members of the UK Government Biometrics Working Group (BWG) in the assessment of the applicability of biometric technology to their potential applications.

4. The tests will implement and validate the BWG proposed methodology for biometric testing. The outcome will support the further development of this methodology for use with Common Criteria evaluations of biometric products and systems.

5. It is also hoped that this initial evaluation will, by example:
   a. Promote the methodology to a wider audience and contribute to the improvement of biometric testing by other organisations; and
   b. Encourage further testing to be sponsored.

To allow wider dissemination of the results (given that open publication of results was not a requirement for vendors participating in the trials), the report has been organised into two parts with different restrictive markings. The intention is that Part I excludes any commercially sensitive information and can be made publicly accessible, while Part II contains full details for CESG and Government Departments.

2 SELECTION OF SYSTEMS

6. The Test Programme was announced on the Biometrics Consortium list server, and some thirty companies responded to the call for submission of devices for testing. Because of overlap in terms of devices proposed, about twenty different systems were considered for inclusion in the test programme.

7. The criteria for selection of systems to test were agreed by CESG and the Biometrics Working Group.
   a. Fingerprint, hand and iris technologies must be included. Other systems tested should use different technologies, except for fingerprint where two systems might be tested.
   b. Within a technology, selection should be on the basis of wide availability and commonality of use.
   c. Systems should be capable of meeting basic CESG performance requirements.
   d. Systems should be testable under the agreed methodology (and, implicitly, the system performance should not be adversely affected by the proposed test protocol).
   e. The vendor should be able to support the trials within the required timescales.

8. Using these criteria, seven systems were selected for testing, using face, fingerprint, hand geometry, iris, vein pattern, and voice and recognition. There were two fingerprint systems: one using optical fingerprint capture, the other a chip sensor. Table 1 gives brief details of the tested systems. Systems have been named where vendors are happy for their results to be publicly available. (Full details of all systems are given in Part II of this report, which has a more restricted circulation.).

Short name	Brief description
Face Face (2)	Visionics – FaceIt Verification Demo Alternative enrolment and matching algorithms for this system
FP-chip FP-chip (2)	VeriTouch – vr-3(U) Alternative enrolment and matching algorithms provided by Infineon
FP-optical	*Fingerprint recognition system.*
Hand	Recognition Systems – HandKey II
Iris	Iridian Technologies – IriScan system 2200
Vein	Neusciences-Biometrics – Veincheck development prototype
Voice	OTG – SecurPBX Demonstration System

Table 1. Brief details of systems tested

9. As there is just one device per technology, it should be noted that the performance results presented are not necessarily fully representative of all systems of the same type. Indeed, even relatively minor modifications to the systems tested can give considerably different performance.

3 TEST SCENARIO

10. The test scenario was one of positive verification in a "normal office environment", with co-operative non-habituated users. The tests were conducted with 200 volunteers, over a three-month period. The typical separation between enrolment and a verification transaction was one to two months.

3.1 Volunteer crew

11. To obtain participants, a call for volunteers was issued by e-mail and in the NPL in-house newsletter. A small payment offered as an incentive for participation (and adherence to the trial "rules"). All those responding were invited to participate, though some withdrew when they could not attend an appointment for enrolment. A limited further call was issued to some staff of the other laboratories on site (NWML and LGC) to achieve slightly over 200 participants. The volunteer crew were thus self-selecting, consisting mostly of staff working on the NPL site. The age and gender profile is shown in Figure 1. This approximates that of the workforce on site.

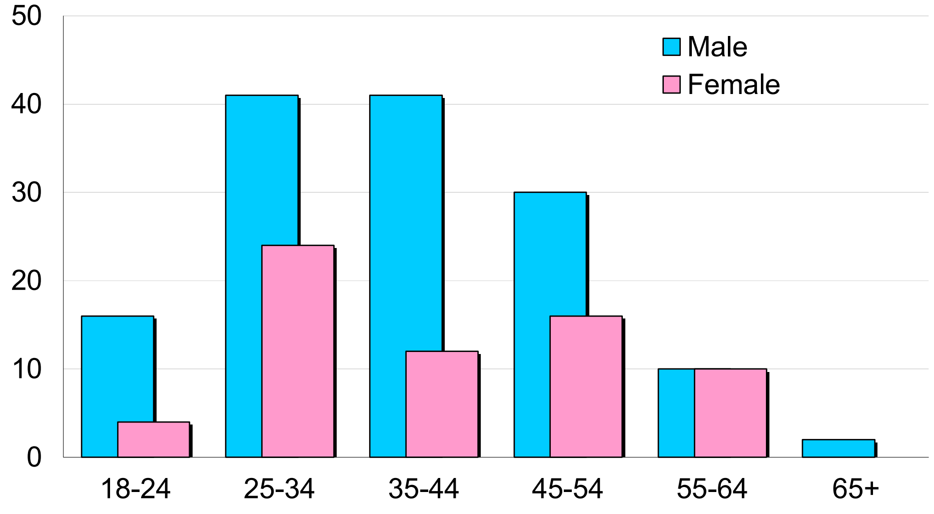


Figure 1: Age and gender of volunteer crew

12. This volunteer crew is not fully representative of the general UK adult population. Women and those older than 45 are under-represented, also the balance between different ethnic

groups is probably incorrect (ethnic origin of volunteers was not recorded). Moreover, as the volunteer crew are used to working in a scientific environment, they are more accepting of technology than the population at large. Potentially this might reduce errors due to the behavioural element in biometric system use.

3.2 Environment.

13. The tests were conducted in a room previously in normal office use.

14. Lighting levels were controlled. The room's fluorescent lighting was always on, and the window blinds kept down to reduce effects of daylight variations. The devices were sited in accordance with recommendations of the product suppliers, and those most sensitive to changes in illumination were positioned away from the window. Similarly one device whose use was sensitive to background noise was located in a quieter area off the main test laboratory. These adjustments are documented with the test results for each device.

15. The temperature and humidity of the test laboratory were not controlled. Figure 2 indicates how outdoor temperature[1] and humidity[2] varied between the days of the trials

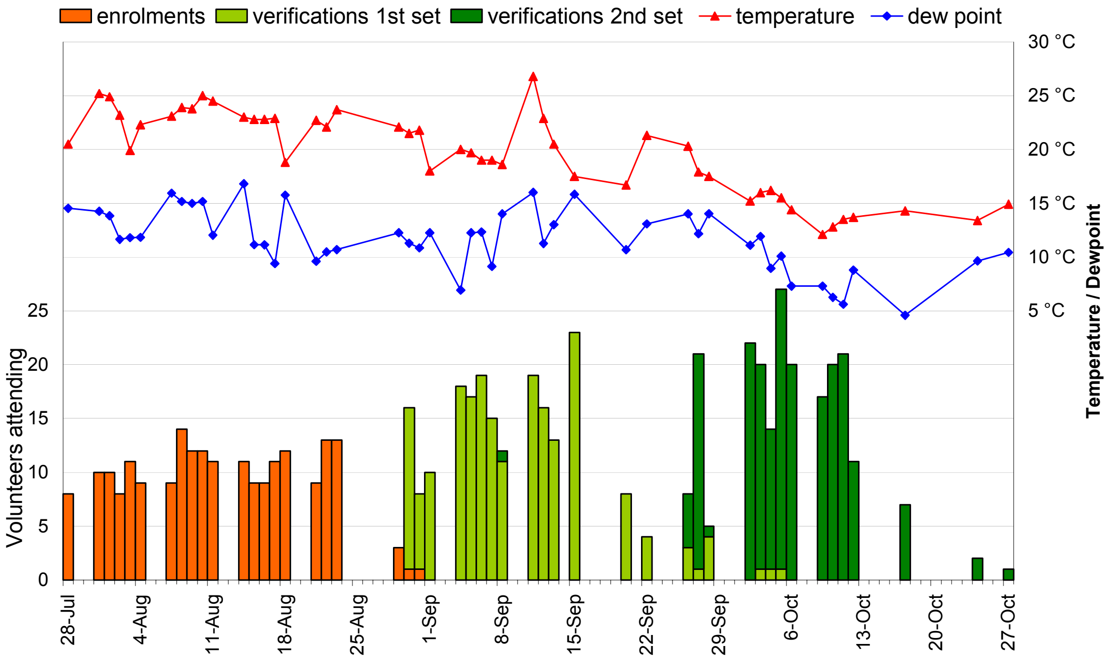


Figure 2. Environmental conditions during the trials

3.3 Enrolments & verifications

16. Figure 2 also shows the daily distribution of enrolment and verification transactions. On average the first set of verifications was made 29 days after enrolment, and the second set of verifications, 55 days after enrolment.

3.3.1 Order effects

17. The order in which the devices were used could potentially affect performance.

[1] Figures based on readings from local weather station.

[2] Dew point is plotted instead of relative humidity. This removes the strong (inverse) correlation with temperature, and to allows the same °C scale to be used.

a. On arriving at the test laboratory, volunteers could be out of breath (if they have hurried to make their appointment) or have cold hands/fingers (when cold outside), recovering to a more normal state after a few minutes.

b. The illumination for the face recognition system increased the amount of iris visible (i.e. reduces pupil size) with a potential effect on iris recognition when this occurs shortly after.

c. Feedback from one fingerprint device might affect user behaviour (e.g. finger pressure) on the other.

18. Other than volunteers attempting speaker verification when out of breath, these order effects did not appear significant. Further order effects may also exist, but are also believed to be insignificant. In view of this, a complex fully randomised sampling plan was not adopted.

a. Transactions on the Voice system were not conducted until the volunteer had regained their breath.

b. The order in which the devices were used alternated between a clockwise order around the room, and anti-clockwise. However, this ordering was often modified to avoid queuing at any system. There were no order correlations between visits.

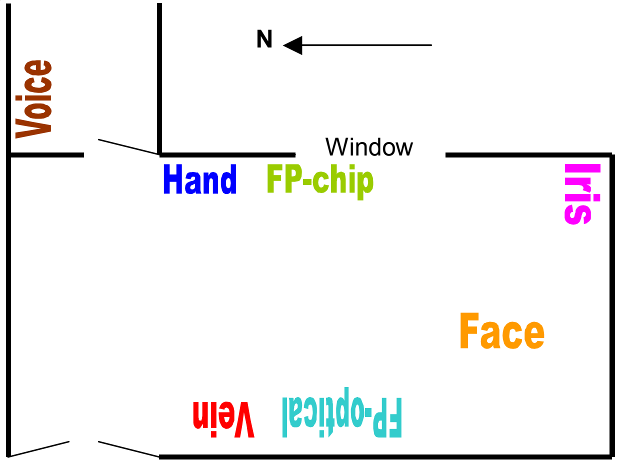


Figure 3. Positioning of systems in test laboratory

4 TEST METHODOLOGY

19. The performance trials were conducted in accordance with

Best Practices in Testing and Reporting Performance of Biometric Devices[3]

produced by UK Government Biometrics Working Group. The test protocol followed is described in

A test protocol for the Technical Performance Evaluation of Biometric Devices

For completeness this Test Protocol is included in Appendix A.

20. Modifications and enhancements to the general test protocol are discussed below.

4.1 Dealing with enrolment failures

21. Observations during preliminary testing showed:

a. Often more than two attempts would be required to obtain an enrolment. This seemed to be particularly the case with the Voice and both Fingerprint systems, where obtaining a good quality “image” is more dependent on user behaviour and familiarity.

b. For some systems, the enrolment software did not provide for re-enrolment. In such cases, problem enrolments needed to be deleted, using the underlying operating system, before re-enrolment was possible. For data-integrity reasons, we were reluctant to do this

[3] Available at http://www.cesg.gov.uk/biometrics/

while under the pressure of processing volunteers, and as a result re-enrolments had to occur on a subsequent visit.

c. Some systems did not automatically record every enrolment attempt failure.

22. The protocol for dealing with enrolment failures was therefore modified. Where practical, immediate re-enrolment was attempted, (as previously). However, at subsequent visits, whenever a volunteer had failed to enrol on one of the devices, they were asked to try re-enrolling regardless of the number of previous enrolment attempts.

4.2 Avoiding data collection errors

23. Additional procedures were put in place to help avoid data collection errors:

a. Errors due to the use of the wrong hand, finger, etc.

b. Errors due to attributing the attempt to the wrong identity.

4.2.1 Avoiding use of wrong hand, finger, etc.

24. Users were asked to always use their right index finger, eye or hand as appropriate. Without this consistency, it would be difficult for supervisors to observe and prevent use of the wrong finger, hand or eye at enrolment or verification. The saved images allow further checks that the correct iris, hand or finger was used, though this is easier for iris and hand images than for fingerprint images.

4.2.2 Avoiding attribution of attempt to wrong identity.

25. Each user was allocated a PIN for the trials, which was shown on the named data sheet collected by the user at each session (see e.g. Appendix C). The following possibilities for attributing attempts to the wrong identity must be addressed by checking procedures.

a. The user picks up the wrong data sheet[4].

b. The user mistypes their PIN, producing another valid PIN[5].

c. The user forgets to enter their PIN on a system where the PIN is not cleared between attempts. As a result the attempt is made against the previous user's identity[6].

These were addressed as follows.

26. **Feedback on claimed identity**
The Voice, Face and Iris systems provided feedback on the claimed identity. This would show the individual and supervisor that failures were due to the wrong PIN being used.

27. **Error detecting PINs**
The PINs used to claim an identity were chosen to minimise the chance that mistyping would produce another valid identity. This was done using the ISBN error-detection scheme (though avoiding use of "X" as the check digit). The 4-digit PINs `abcd` have the property that `4a+3b+2c+d` is exactly divisible by eleven. This detects all single digit errors and transpositions. From the available PINs, the set used was as widely spaced as possible, in the range 1000 – 9999, giving robustness against more complex typing errors.

28. **User makes at least 3 attempts per device per session**
If a PIN not being entered causes attempts to be recorded against the previous user's identity, these will be the 4th or subsequent attempts. However, these will be ignored as only the first 3 attempts per user per session are analysed.

29. Any incorrect attempts were recorded on the user's data sheet, allowing for annotation of the logged data and exclusion from analysis. Where possible, prior to conducting analyses, the

[4] This happened twice (of a possible 412 occasions), where the volunteers had very similar names.

[5] One of the systems recorded when incorrect PINs were entered. Of some 2000 entered PINs, 5 were entered incorrectly. Two single digit errors, one transposition, and two 2-digit errors.

[6] This could happen on three of the systems tested, occurring twice, once, and no times (of a possible approx 400 occasions).

data saved for verification failures were checked further, to determine if the cause of failure was a mis-acquisition or a mis-labelling.

5 RESULTS OVERVIEW

5.1 Failure to enrol

30. The “failure to enrol” rate measures the proportion of individuals for whom the system is unable to generate repeatable templates. This includes those unable to present the required biometric feature (for example the Iris system failed to enrol the iris of a blind eye), those unable to produce an image of sufficient quality at enrolment, as well as those unable to reproduce their biometric feature consistently. Enrolment failure rates for the systems tested are shown in Table 2. Note that, in cases of difficulty, several attempts were allowed to achieve an enrolment. If necessary, these further enrolment attempts were made at subsequent visits by the volunteer.

System	Failure to enrol rate
Face	0.0%
Fingerprint – Chip	1.0%
Fingerprint – Optical	2.0%
Hand	0.0%
Iris	0.5%
Vein	0.0%
Voice	0.0%

Table 2. Failure to enrol rates

5.2 Failure to acquire

31. The “failure to acquire rate” measures the proportion of attempts for which the system is unable to capture or locate an image of sufficient quality. This includes cases where the user is unable to present the required biometric feature (e.g. having a plaster covering his or her fingerprint); and cases where an image is captured, but does not pass the quality checks. Failure-to-acquire rates for the systems tested are shown in Table 3. The figures exclude cases where the image was not captured due to user error (e.g. the user not positioning themselves correctly) as in these cases the attempt was simply restarted.

System	Failure to acquire rate
Fingerprint – Chip FP-chip (2)	2.8% 0.4%[7]
Face	0.0%
Fingerprint – Optical	0.8%
Hand	0.0%
Iris	0.0%
Vein	0.0%
Voice	2.5%

Table 3. Failure to acquire rates

5.3 False match rate (FMR) vs false non-match rate (FNMR)

32. The fundamental operation of a biometric system is the comparison of a captured biometric image against an enrolment template. The false match and false non-match rates measure the

[7] For verification, minimal quality checks were performed.

accuracy of this matching process. By adjusting the decision criteria there can be a trade-off between false match and false non-match errors; so the performance is best represented by plotting the relationship between these error rates in a detection error trade-off graph.

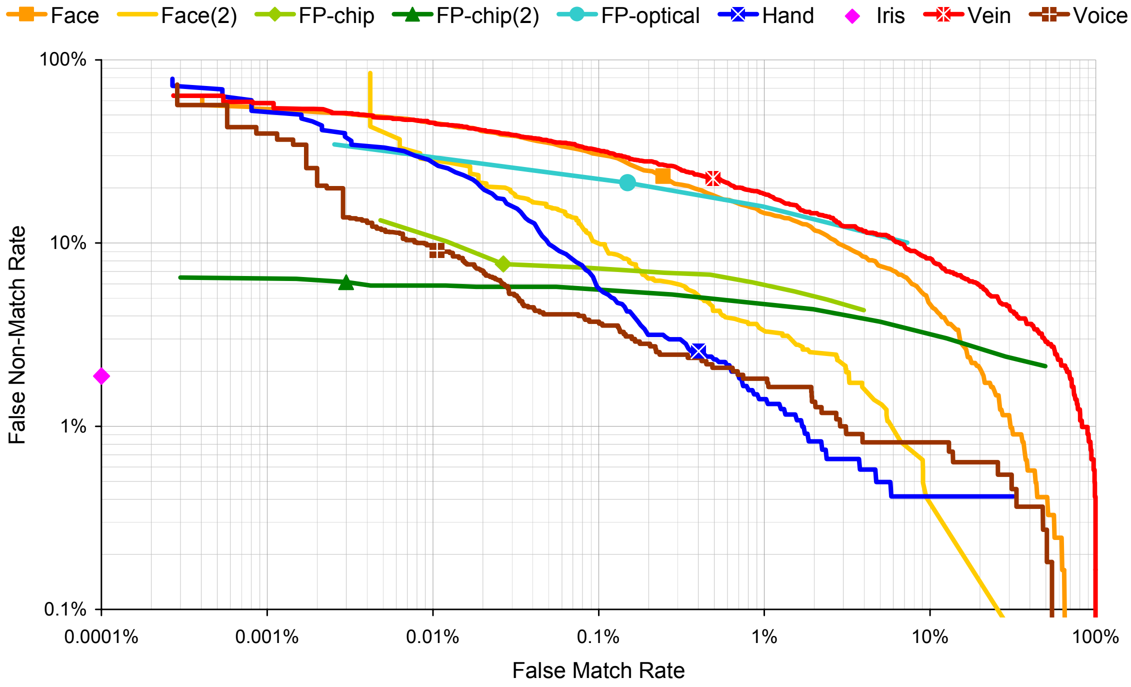


Figure 4. Detection error trade-off: FMR vs FNMR

33. Matching algorithm performance for each system, over a range of decision criteria, is shown in Figure 4. (The lower and further left on the graph, the better the performance). The node on each curve shows performance at the default decision threshold. No curve is shown for the Iris system, which operates with a pre-determined threshold. The iris system had no false matches in over 2 million cross-comparisons. For all the other systems the leftmost point on each curve represents a single false match in the total number of cross-comparisons made.

34. Observing images corresponding to false non-matches showed that some of matching failures were due to poor quality images. Systems vary in how they deal with poor quality images, some will "fail to acquire" such images, while systems will often cope with poor image quality. Therefore the matching error rates should not be considered in isolation from the failure to acquire and failure to enrol rates.

5.4 False acceptance rate (FAR) vs. false rejection rate (FRR)

35. False acceptance and rejection rates measure the decision errors for the whole system. These measures combine matching error rates, and failure to acquire rates in accordance with the system decision policy. When the verification decision is based on a single attempt:

$$\mathrm{FAR}(\tau) = (1\text{- FTA})\ \mathrm{FMR}(\tau)$$
$$\mathrm{FRR}(\tau) = (1\text{- FTA})\ \mathrm{FNMR}(\tau) + \mathrm{FTA}$$

where τ is the decision threshold, and FMR, FNMR, FTA, FAR and FRR are the false match rate, false non-match rate, failure to acquire rate, false acceptance rate and false rejection rate respectively.

36. The false acceptance false rejection trade-off curve is shown in Figure 5. The curves for the face, hand geometry, iris and vein systems are unchanged, as these systems had no failures to acquire.

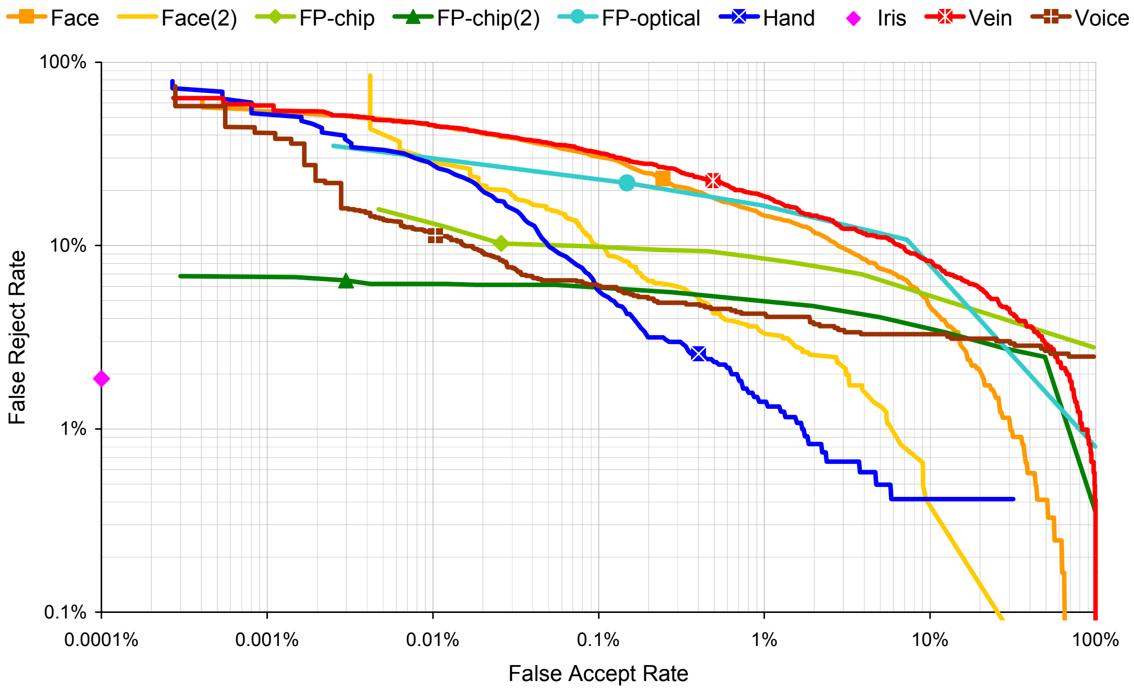


Figure 5. Detection error trade-off: FAR vs FRR

5.5 Multiple attempt error rates

37. Many systems allow multiple attempts, in their normal mode of operation. The effects on error rates of a "best-of-3" decision policy are examined in this section.

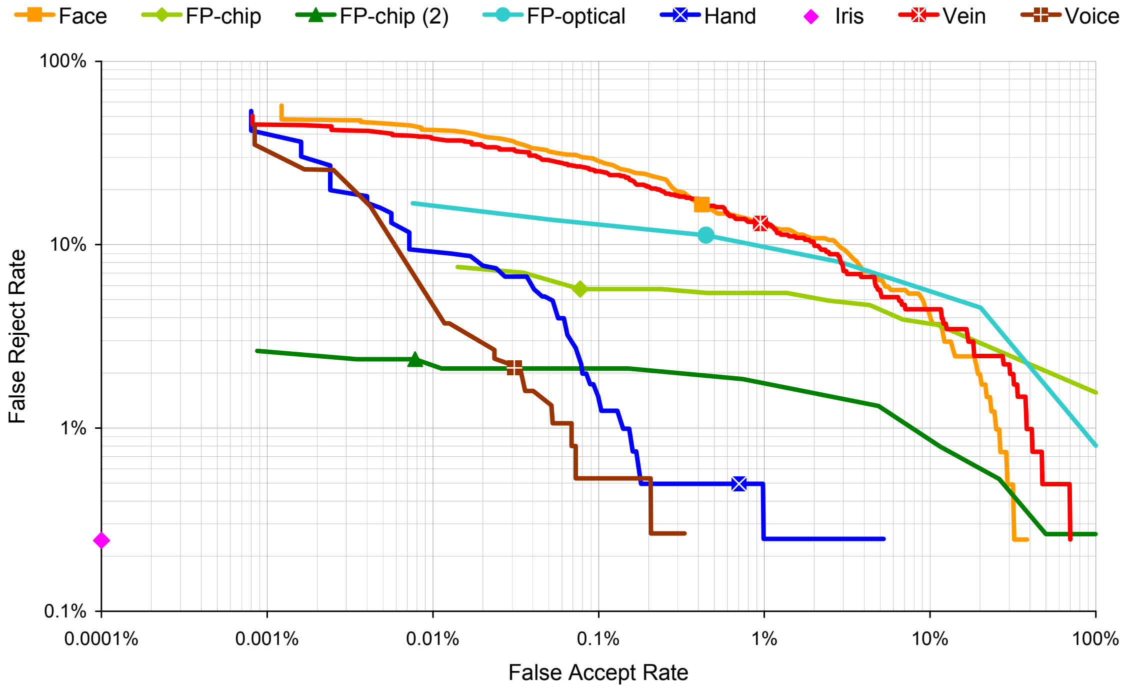


Figure 6. Detection error trade-off: Best of 3 attempts

38. The 3-attempt genuine and impostor scores are the best matching score from the 3 attempts made at the person-visit (scored against the chosen template). The resulting detection error trade-off (DET) curves are shown in Figure 6.

39. This method of obtaining the DET curve is appropriate when all attempts are constrained to use the same finger, face or hand etc. In real life, it may be possible to substitute a different finger, face, hand, etc at the second or third attempt. If so (and assuming the individual impostor attempts are fully independent) the 3-attempt false acceptance rate at any decision threshold is given by $1-(1-\alpha)^3$ where α is the false acceptance rate for a single attempt at the same threshold. Thus, two detection error trade-off curves may be shown:

a. Where all three attempts are constrained to use the same finger, hand, face, etc; and

b. Where substitutions are allowed between attempts.

In the case of the trial systems and data, the two curves follow each other closely[8], so Figure 6 shows a single curve for each system[9].

5.6 User throughput

System	Transaction Time (Seconds)			Time includes entry of PIN?
	Mean	*Median*	*Minimum*	
Face	15	14	10	Excluded
Fingerprint-Optical	9	8	2	Excluded
Fingerprint-Chip	19	15	9	Excluded
Hand	10	8	4	Included
Iris	12	10	4	Included
Vein	18	16	11	Included
Voice	12	11	10	Excluded

Table 4. User transaction times

40. The time for a user transaction has been calculated using the time differences logged between consecutive transactions (as detailed in Appendix A.6.7). Table 4 shows the mean, median and minimum transaction times to indicate the spread of results. The differences in operation of the trial systems accounts for much of the difference in timings.

a. The Face system collected a sequence of images over a 10 second period, saving the best match obtained. The transaction times would be somewhat shorter if the system stopped when the threshold was first exceeded; however, this would not have allowed us to examine performance over a range of decision thresholds.

b. The Iris system would normally work in identification mode, not requiring PIN entry. This would reduce transaction times.

c. The keypad of the Vein system could not cope with rapid entry of the PIN. The time to do this dominates the overall transaction time.

d. The transaction times for the Voice system were dominated by the time taken in giving user prompts and feedback. The prompting and speeds were chosen to be suitable for users unaccustomed to the system, rather than for maximum throughput.

5.7 Matching algorithm throughput

41. The measured throughput of the programs for batch mode running of the matching algorithms is shown in Table 5. These diagnostic programs had significant overheads, for example logging all matching attempts to a file, or handling the Windows interfaces. Therefore, the matching algorithm throughput may be significantly higher than those shown, perhaps by a factor exceeding 100. (In the case of the chip-based fingerprint system, the difference in throughput of the two diagnostic programs illustrates the improvement possible. In an

[8] The ratio FAR_b/FAR_a of the false acceptance rates derived under the different assumptions varies from 1 to 1.3 for the voice system and fingerprint systems; from 1 to 1.7 for the vein system, and from 1 to 2 for the hand and face systems.

[9] For the FP-chip, and FP-optical systems, a cross-comparison scoring of all attempts against each template was not available, and the curve shown is derived as detailed in paragraph 39. For FP-chip (2) and all the other systems, the curve was derived using a full set of genuine and impostor scores.

equivalent implementation, the basic FP-chip algorithm would be faster than the more complex alternative FP-chip(2).)

System	Matches per minute	Program interface	System, processor speed, memory, & OS			
Face	800	Windows	Pentium			Win2K
FP-chip	60	Windows	Pentium	133MHz	32Mb	Win98
FP-chip (2)	2,500	Command Line	Pentium	500MHz	64Mb	Win95
FP-optical	50	Windows	Pentium	500MHz	64Mb	Win95
Hand	80,000	Command Line	SunUltra5	270MHz	128Mb	SunOS5.8
Iris	1,500,000	Command Line	SunUltra5	270MHz	128Mb	SunOS5.8
Vein	130	Windows	Pentium	500MHz	64Mb	Win95
Voice	680	Command-Line	Pentium	500MHz	64Mb	Win95

Table 5. Diagnostic program throughput

5.8 Performance differences by user & attempt type

42. Attempts can be categorised by:
a. Whether made at enrolment visit or at the second or third visit by the volunteer;
b. The gender of the volunteer;
c. The age of the volunteer;
d. Whether the volunteer was wearing spectacles in the case of Face and Iris systems;
e. The length of the user's pass-phrase in the case of the Voice system.

Performance differences between these subsets have been analysed, and are reported for each system in Part II. The general findings are summarised in Table 6.

System	Gender	Age	Visit	Other
	Observations:		lowerFRR<higherFRR	Less significant
			lowerFRR<higherFRR	**More significant**[10]
Face	**male<female**	younger<older	**enrol<later**	without<with glasses
FP-chip	male<female	**younger<older**	**enrol<later**	
FP-chip(2)	male<female	younger<older	enrol<later	
FP-optical	male<female	**younger<older**	**enrol<later**	
Hand	male<female			
Iris				without<with glasses
Vein	**male<female**	younger<older	**enrol<later**	
Voice	female<male	younger<older	**enrol<later**	

Table 6. Summary of performance differences by user type

43. False rejection rates for attempts made immediately following enrolment were generally significantly lower than (less than half) those made at volunteer's second or third visit.

44. Generally men had a lower false rejection rate than women (the voice system being the only exception), and younger volunteers a lower false rejection rate than their older colleagues. The gender differences appeared the more significant for the Face, Hand and Vein systems, and the age differences the more significant for the Fingerprint systems.

45. As women and over 45's were under-represented in our volunteer crew, our results may be biased. For a given threshold, with equal numbers of men and women, a slightly higher false non-match rate might be expected. However since false matches are more likely within the same gender class, the equalisation would reduce the false match rate at the same threshold.

[10] The more significant observations have a χ^2 value exceeding 15. (See Appendix D for details.) The probability of such observations being due to the random nature of the sample is in the range 0.01% - 20% dependent on the degree of correlation between different attempts by the same person.

6 VALIDATION OF METHODOLOGY & FUTURE ENHANCEMENTS

46. The evaluation has implemented the BWG proposed methodology for biometric testing, validating many aspects of this methodology. For example:

a. Demonstrating the feasibility of the methodology;

b. Showing that the number of volunteers used (200) is sufficient to evaluate performance of biometric systems at their current level of accuracy;

c. The practical significance of issues described in "Best Practices" has been demonstrated:
The need for time separation between enrolments and verification attempts;
The need to minimise the chance of labelling errors;
The modified procedures to simulate unknown impostor attempts when there are dependencies between templates.

A single evaluation cannot demonstrate repeatability of the results. However, some of the devices evaluated have been tested elsewhere in similar scenarios, and the results are consistent.

47. The evaluation revealed further issues concerning the applicability of the test protocol, and enhancements to best practices. These are noted below.

6.1 The requirement for additional system functionality

48. The test protocol required systems to save data for off-line calculation of genuine and impostor matching scores. This capability is often not provided in a vendor's standard supplied system. This raises the following issues:

a. Some systems will be unable to meet this requirement for testing (for example standalone systems which store templates are stored locally, but have insufficient memory to log transaction attempts). This point was raised by some of the vendors who initially expressed an interest in participation in the trials.

b. When the required functionality is achievable with vendor support, it is important that protocols are sufficiently consistent across testing organisations. Otherwise the vendor needs to develop a different customisation for each test, and support costs can be very significant.

c. Sometimes achieving the desired functionality can affect system performance. For example the time taken in logging images may slow the system and affect user behaviour. It is also possible that implementing the required functionality at minimal cost will introduce errors into the system.

49. If all testing, including impostor tests, are conducted "live" these problems are avoided. However, this requires:

a. Data collection to be very closely supervised as all results must be logged by the supervisor;

b. Extra attempts to be made to show performance at a variety of decision thresholds; and

c. Extra attempts to be made for live impostor tests.

6.2 One attempt may involve a sequence of images

50. With many biometric systems, a sequence of images is processed in a single verification attempt. For example, with the trial system it appears that:

a. The Face system collects images over a period of 10 seconds, and gives the best match obtained;

b. The Chip-based Fingerprint system collects images until a match is obtained, or until timeout;

c. The Optical Fingerprint system scans for fingerprints until an image of sufficient quality is obtained, or the timeout is reached;

d. The Hand Geometry system occasionally requires a second hand placement, when the score is very close to the decision threshold;

e. The Iris system collects images until a match is achieved or until timeout.

51. The current version of "Best Practices" does not explicitly deal with these cases, yet this mode of operation can sometimes bias off-line calculations using the collected data. For example with the face system, in a real impostor attempt the score would be based on the image that best matches the impersonated template. A cross-comparison of stored genuine images uses the image that best matches the genuine template, and therefore may underestimate the false match rate.

52. The questions that must be addressed are:

a. Would the decision be based on a different image if comparison were against a different template?

b. If so, would live impostor attempt scores be higher/lower than off-line scoring with genuine attempt images?

In the case of the tested Optical Fingerprint, Hand Geometry and Iris systems, the image collected does not depend on the template being matched. With the Fingerprint Chip, the collected image might instead be last before timeout; and, apart from image quality, should be equivalent to the image saved from a genuine attempt.

6.3 Failure to acquire

53. As noted in Section 5.3 (paragraph 34), different systems handle poor quality input in different ways. With some systems this may result in a failure to acquire, and with others a matching failure. In this respect the FAR-FRR trade-off graph provides a better comparison of performance than the FMR-FNMR trade-off graph.

6.4 Other performance trade-offs

54. Systems may have other adjustable parameters affecting performance in addition to (or instead of) an adjustable decision threshold. These allow different performance trade-offs (which, depending on the application, may be more important than the FAR-FRR trade-off). For example, with the Face, Iris, and Chip-Fingerprint systems, which try to match collected images over a fixed time period, there is a trade-off between the time allowed and the false rejection rate.

APPENDIX A. TEST PROTOCOL

A.1 Introduction

This report describes the test protocol planned for the UK Government Biometric Test Programme. The protocol is for "scenario testing" and conforms to the guidelines in "Best Practices in Testing and Reporting Performance of Biometric Devices". The protocol is intended to be practical in terms of effort and costs, and applicable to many of today's commercially available biometric devices when operating in their intended environments.

Several systems will be tested at the same time, in a standard indoor (office) environment and using a volunteer crew similar to the general adult UK population. The trials will involve approximately 200 volunteers using each of the systems being tested. Volunteers will attend the trials on three occasions: firstly for enrolment and practice attempts; and later, one and two months after enrolment, to collect "genuine" attempts Detection Error Trade-off (ROC) analysis.

Impostor attempts will be simulated using cross-comparison of genuine attempts against enrolment templates for other enrolees. This will be carried out off-line using vendor-provided software with the collected enrolments and genuine-attempt images and data.

A.1.1 Applicability of this protocol

Biometric limitations — The protocol cannot be used if it takes much longer than a few seconds for the system to extract the required biometric features. For example we could not test a system that uses 10 minutes of typing at a keyboard to make an identity decision. The separation between enrolment and test attempts will be approximately 1 month. If we are interested in the effects of template ageing time over a timespan much greater than this, the protocol may also be inappropriate.

System functionality — We can only test complete systems. These must be able to operate in "verification" mode, matching a single attempt against a single stored template. It is also necessary for the system to log specific information about each attempt, and there must be a capability for off-line generation of matching scores

System Error Rates — We shall not be able to measure error rates to values of 1% or below with any certainty. For example, if 1% of the population have (or lack) some feature causing enrolment failure, there is a 13% chance that no-one in a 200 person sample have that peculiarity. On the other hand to measure error rates exceeding 10% we may be using more volunteers than required, and a smaller test may be more cost effective.

A.1.2 Modelled Scenario

The scenario modelled is that of a verification application in an indoor environment.

Co-operative users — It is hard to replicate the actions and motivations of an uncooperative user.

Overt system — We shall be using volunteers who will be brought to a specific location for testing, and who will test several devices. This effectively rules out covert testing.

Non-habituated users — Our volunteers will use the system a few times only, with gaps of a few weeks between each use. The level of habituation will therefore be quite low. We shall avoid using volunteers who have extensively used one of the systems under test, so that comparisons are fair. We do not propose replicating a higher level of habituation by allowing practice attempts: this would create additional complexities to be able to separate practice attempts from the real test attempts.

Supervised enrolment, lightly-attended use — Enrolment will be supervised. Subsequent attempts will be lightly attended: there will be someone on hand to sort out problems should these occur. However, it should be noted that, after enrolment, the main role of the supervisor is to ensure the integrity of the data collection process rather than to assist volunteers in their attempts.

Standard environment — The tests will be conducted indoors, in a standard office environment. It is harder, and more costly to conduct the trials in an outdoor environment, and currently relatively few devices will operate satisfactorily in an outdoor environment.

Public users (UK adults) — Volunteer user attitudes are likely to be closer to those of the general public, than that of company employee. Also, volunteers will be local to the testing laboratory, and their biometric features will reflect the UK demographics. Results may be different with other population demographics. We note that our volunteers are probably more scientifically aware (and perhaps better able to follow instruction) than the general public.

Closed system — We shall enrol and test using the same system. Note that if the system would normally used several sensors, where there are considerable variations between sensors, the proposed protocol may not be appropriate.

A.1.3 Performance Measures

The proposed tests will measure the following aspects of performance (where applicable).

- Failure to enrol rate
- Failure to acquire rate
- Detection error trade-off graph (i.e. ROC)
- System false match and false non-match rates
- Penetration rate (where appropriate)
- Binning error rate (where appropriate)
- User throughput
- Matching algorithm throughput (reported with processing system used)
- Sensitivity of performance to (potentially problematic) changes in environment, population, or usage

A.2 Device setup

We allow vendor involvement during device set-up to help ensure that the systems are correctly installed and operating optimally.

A.2.1 Install systems & familiarisation

The complete system will be installed at the test site. Account will be taken of vendor recommendations regarding positioning, illumination, and background noise etc. in so far as these are realistically achievable in a general office/indoor environment. Threshold, image quality and other settings will be set in accordance with vendor advice.

A.2.2 Test sensitivity of performance to environment, population, usage

Some pre-trial tests will be carried out to determine environmental and other factors that may cause problems. This will be a limited investigation, mainly using the testing team. The aim is to determine:

- what potential problems exist,
- if these problems are controlled by the system,
- how significant the problems appear to be,
- whether we need to impose environmental or other controls to minimise the problem during the trials,
- what additional information we need to record to identify difficult subsets of volunteers during subsequent analyses.

Some of the potential sensitivities to test, and what may be done to analyse or control any problems are shown in the following table:

Technology	Effect to test	If effects seem significant
All	age, gender, template-ageing	Compare of error rates for different subsets of volunteers/attempts
All	lighting level & direction	Control lighting levels during trial
All	dirt/smears on sensor	Set policy for cleaning devices
All	movement during attempt	Provide appropriate instructions for volunteers
All	positioning	Provide appropriate instructions for volunteers
Finger-print	Dry / cold / cracked / damp / wet fingers	Advise volunteers on improving fingerprint quality. Record temperature & humidity
Hand geometry	rings, plasters, etc.	Log attempts made with rings etc. Provide separate error rates for these cases
Iris, Face	Glasses	Record those who wear glasses/contact lenses Provide separate error rates for these cases

A.2.3 Set enrolment & transaction attempt policies

The enrolment policy will be set to deal with the problems identified, with the aim of achieving the greatest number of good enrolments.

The supervisors who will conduct enrolment will be trained and familiar with each system and its common problems.

A.2.4 Produce system information for volunteers.

For each system, a short description of how the system operates, and how it should be used will be prepared in consultation with the system vendor. This is to reduce the burden of describing full details of the systems at enrolment, and before later transaction attempts.

A.3 Volunteer crew

A call for volunteers will be issued. To encourage participation a small reward will be offered. If more than 200 people volunteer, participants will be selected at random from the volunteers.

Before enrolment participants will be informed of the purpose of the trials, what is required of them, and what information will be collected and stored. They will be asked to sign to give their consent to the collection of biometric images and information, and to confirm that they have not previously used any of the devices being tested. Age category and gender of participants will be recorded, together with any information found useful in identifying problem cases in the preliminary trials.

A.4 Enrolment

Each participant will attempt to enrol on each system under test. The order of enrolment on the devices being tested will be randomised. Only one set of equipment will be used for each system to avoid “channel” effects. Enrolment will be conducted using the enrolment functions of the supplied systems, and will supervised by a member of staff who had been trained for this purpose.

Enrolment images will be collected by the system. *(We use the word image to refer to the actual input signal; this may not strictly be an image in the case of non-optical devices. If the system is unable to record actual enrolment images, it may be possible to conduct the required analyses using the image templates.)*

Immediately after enrolment, several attempts will be made to check that the participant can be reliably verified. Advice to help users achieve successful verifications will be given if necessary. If they cannot be reliably verified this shall count as an enrolment failure.

If enrolment fails, one re-enrolment will generally be attempted. *(In some cases it may be clear that subsequent attempts must fail, for example if the volunteer does not have the required biometric feature. In such cases no re-enrolment attempt would be made. In other cases the enrolment failure may due to a clearly identifiable error which can easily be overcome, for example failures due to not following the proper enrolment process. In such cases more than two enrolment attempts might be made.)*

Some systems allow an “override” to register a poor quality image as an enrolment template in cases of difficulty; such features will not be used. Any problems with enrolment will be noted by the enrolment supervisor.

Cases where the enrolment template cannot be generated, or where all practice attempts fail, are

considered to be failed enrolments. In these cases, subsequent verification attempts are not required of the participant on the device in question. Data from failed enrolments will be removed from the enrolment database and will not be used in analysing false match or false non-match error rates.

A.5 Test data collection

Volunteers will make two sets of transactions, at approximately one and two months after enrolment. On each occasion they should make (at least) three attempts. This will allow direct calculation of "best of three attempt" rejection rates, and can also reveal whether some users are much more error prone than others.

Attempts will be largely unsupervised, but there will be a supervisor on hand to help in case of difficulty. Users may observe attempts made by others, but will not be allowed to make practice attempts (apart from those they made as part of enrolment). This is to ensure that only the genuine transactions are recorded. It is also the case that practice attempts could artificially lower the failure to acquire rate. Additional attempts (i.e. after the required 3 attempts) may be made. It is important to ensure that no attempt is made against the identity of another participant. If a volunteer is keen to see a rejection, it is permitted that they may make an attempt against a non-participating identity. Again, such attempts should not take place immediately prior to their "genuine" attempts.

The order of using the devices will be random across users, and not correlated with the order of use on other occasions. Users will be asked to try to make these attempts successful, and to refrain from making bogus attempts (e.g. using the wrong finger on fingerprint devices, or pulling faces on face recognition devices). As an incentive to obey these instructions, payment for participation is linked to making the required number of good attempts.

Attempt images will be collected by the system, and user details, date and time logged. To avoid data entry errors, user identity will be entered using a swipe card or smart card if possible.

The supervisor will note any problems that arise during the test data collection, so that non-genuine attempts are not included in the analyses. Details of such attempts should be reported.

A.6 Analysis & Reporting

A.6.1 Data collected

Collected by system

- event logs as collected automatically by each system
- images of all test attempts
- enrolment database
- enrolment images

Collected by supervisor:

- log of failed enrolments
- log of (non-genuine) attempts to be excluded
- user details, e.g. age, sex *(The relevant user information to collect will depend on the sensitivities identified in preliminary tests.)*

A.6.2 Failure to enrol rate

The proportion of volunteers failing to obtain an enrolment (of sufficient quality) will be reported along with the enrolment policy and any quality threshold settings.

A.6.3 Failure to acquire rate

The proportion of attempts resulting in a failure to acquire error, averaged across all enrolees, will be reported together with any quality settings.

A.6.4 Detection Error Trade-off plot

The following enrolments and attempts will be excluded when deriving false match and false non-match rates:

- enrolment templates associated with any failed enrolment,
- attempts made on the day of enrolment,
- attempts made by non-enrolees, non participants in the trials, or by participants not completing the trials,
- attempts noted as a non-genuine in the supervisor log book,
- attempts resulting in failure to acquire errors
- extra attempts (4th or later attempt) made by any user on any day. (This is to ensure there is no imbalance due to some users making many more attempts than others).

Distance scores for genuine transactions may have been generated "live" during data collection. Otherwise we use vendor provided software for generating these distance scores off-line from the collected images.

Some systems do not generate distance scores, but can operate at various security settings. In such cases the attempts will be analysed using off-line software at different security settings. In such cases we consider the distance measure to be the strictest security setting at which the attempt results in a match.

We use the supplied software to generate impostor attempt distance scores, by comparing each attempt against the templates for all other enrolees. In the case of non-independent templates it will be necessary to re-enrol all enrolees apart from the one who made the attempt.

The Detection Error Trade-off curve plots the proportion of genuine transaction scores exceeding the matching threshold *(we assume that low scores imply a good match and high scores a poor match)* against the proportion of impostor transaction scores below that threshold, as the threshold varies.

A.6.5 System false accept & false reject rates

In cases where the usual decision policy of the system is not based on a single attempt-template comparison, we give the false accept rate and false reject rate using the actual decision policy, at the system settings used.

A.6.6 Penetration rate & binning error rate.

If a binning algorithm is used, we need to know the "bin" for each template and each genuine attempt.

The penetration rate is the average proportion of the database that would need to be searched if the system were operating in identification mode, where the average is taken over all genuine attempts. This can be estimated if we know the number of attempts in each bin, and which bins are compared against each other. A bin error occurs when an attempt is placed in a bin which is not compared with the correct bin for the biometric entity used, and hence will fail to match.

A.6.7 User throughput & matching algorithm throughput.

User throughput measures the elapsed time of a single transaction. All attempts are to be timed at a consistent point during the transaction (e.g. the start time). The difference in times between the first and second, or second and third attempts, by an individual on one day approximates the total transaction time. This assumes that the 2nd and 3rd attempts immediately follow the first attempt.

We can time the off-line calculation of impostor distance scores and compute the number of template-attempt matches performed to obtain the matching algorithm throughput. As the time is hardware dependent, the system used should be specified with the resulting throughput rate.

A.6.8 Sensitivity to population & environment

Where there appear to be differences in performance due to population, environment or usage changes (see section A.2.2), in some cases we will be able to assess the affects on performance by analysing subsets of the attempts. For example we can compare the error rates for different age categories, for people with glasses against those without glasses etc. We can also compare the error rates for attempts one month after enrolment with those two months after enrolment (and with error rates immediately after enrolment) to see the effects of template ageing. Comparing the error rates for the first attempt with those for the second and third attempt made on any occasion may show possible improvement in performance due to habituation.

APPENDIX B. CONSENT FORM & ENROLLMENT DATA SHEET

Name

Laboratory

Phone

Email

TRIAL ID

□ Male □ Female

Age:

□ 18-24 □ 25-34 □ 35-44
□ 45-54 □ 55-64 □ 65+

Other

□ Glasses
□ Contact Lenses

I am happy to participate in these trials. I consent to my biometric data being collected during the trial and stored electronically.

I permit use of this data for the purposes of evaluating performance of biometric devices, by the National Physical Laboratory, the Government Biometrics Working Group, and by the manufacturers of the devices under test. *[Data made available outside NPL will consist of only the collected biometric data, and the personal details in the box above.]*

Signed:

System	Enrolled OK	Problems / Notes
Face		
Iris		
Vein		
Hand Geometry		
Voice		
Fingerprint Optical Reader		
Fingerprint Chip Reader		

Return for recognition attempts on:

APPENDIX C. VERIFICATION DATA SHEET

«FirstName» «LastName»

TRIAL ID **«PIN»**

Please make **3** attempts on each system

Try your best to be correctly recognised - Do **NOT** try and trick the systems

System & Brief Instructions		Comments
VEIN		
1. Place **RIGHT** hand on pad	□	
2. Click button under your fingers to take image	□	
3. Enter **«PIN»** on keypad, check on screen, then press *	□	
FINGERPRINT – OPTICAL SENSOR		
Enter **«PIN»** in ID box – Check this before proceeding	□	
1. Press VERIFY to make a verification	□	
2. Use **RIGHT INDEX** finger	□	
FACE		
Enter **«PIN»** and check your image displayed	□	
1. Press START VERIFICATION	□	
2. Stand on marked spot and face camera	□	
IRIS		
1. If needed click START or 🔍 *to show ID entry box*	□	
2. Enter **«PIN»** and click OK	□	
3. Use **RIGHT** eye	□	
FINGERPRINT – CHIP SENSOR		
Enter **«PIN»** in ID box – Check this before proceeding	□	
1. Press START to commence verification	□	
2. Use **RIGHT INDEX** finger	□	
HAND GEOMETRY		
1. Enter **«PIN»** and press "#YES" key	□	
2. Use **RIGHT** hand	□	
	□	
VOICE		
Dial 6901 and follow instructions	□	
	□	
	□	
For impersonation attempts use ID **«PIN-impostor»**	□	
	□	
	□	

Options for payment

□ (NPLML Staff) Please make payment with my November salary
My staff number is:

□ (non NPLML staff) Please send a cheque to:

□ Please donate my payment to the NPL Sports Club Pavilion Rebuild Fund

□ Please donate my payment to Save the Children

□ I wish to waive payment

Signed:

APPENDIX D. SIGNIFICANCE OF USER & ATTEMPT VARIATIONS

55. Attempts can be categorised by:

a. Whether made at the enrolment visit or at the second or third visit by a volunteer;

b. The gender of the volunteer;

c. The age of the volunteer;

d. Whether the volunteer was wearing spectacles in the case of Face and Iris systems;

e. The length of the user's pass-phrase in the case of the Voice system.

Performance differences between these subsets have been analysed, and are reported for each system in Part II.

56. To determine the statistical significance of any observed differences (i.e. the probability of the difference being attributable to sampling error) a simple χ^2 test was used.

a. The number of correct and failed verifications at the default threshold were counted for each class. E.g.

Observed	Under 35	Over 34	Combined
FRR	3.9%	11.5%	8.3%
Rejected	29	116	145
Verified	710	893	1603
Total	739	1009	1748

b. If there were no difference between classes the combined error rate would apply to both classes.

Expected	Under 35	Over 34	Combined
FRR	8.3%	8.3%	8.3%
Rejected	61.3	83.7	145
Verified	677.7	925.3	1603
Total	739	1009	1748

Observed-Expected		
	-32.3	32.3
	32.3	-32.3

c. The test statistic used is

$$\sum \frac{(Obs.\ -\ Exp.)^2}{Exp.} = (32.3 - ½)^2 \left(\frac{1}{61.3} + \frac{1}{83.7} + \frac{1}{677.7} + \frac{1}{925.3} \right) = 31.17$$

(The subtraction of ½ represents the correction for continuity; and is used because the observed values can only take integer values.)

d. If all attempt results are statistically independent, the test statistic would follow a χ^2 distribution (with 1 degree of freedom). In the example case χ^2 exceeds 31.17 with probability less than 0.01%. However, this overstates the significance since there are dependencies between each attempt made by the same user.

e. If all *N* attempts by any user had the same result (the maximum correlation possible), while attempts by different users are independent, then the test statistic divided by *N* follows a χ^2 distribution (with 1 degree of freedom). In the example case, if there are 9 attempts per user, the probability of χ^2 exceeding $\frac{31.17}{9} = 3.46$ is 6.28%. This understates the significance, since user attempts are not correlated to such an extent.

f. Both results are shown, the true significance lies between these values.

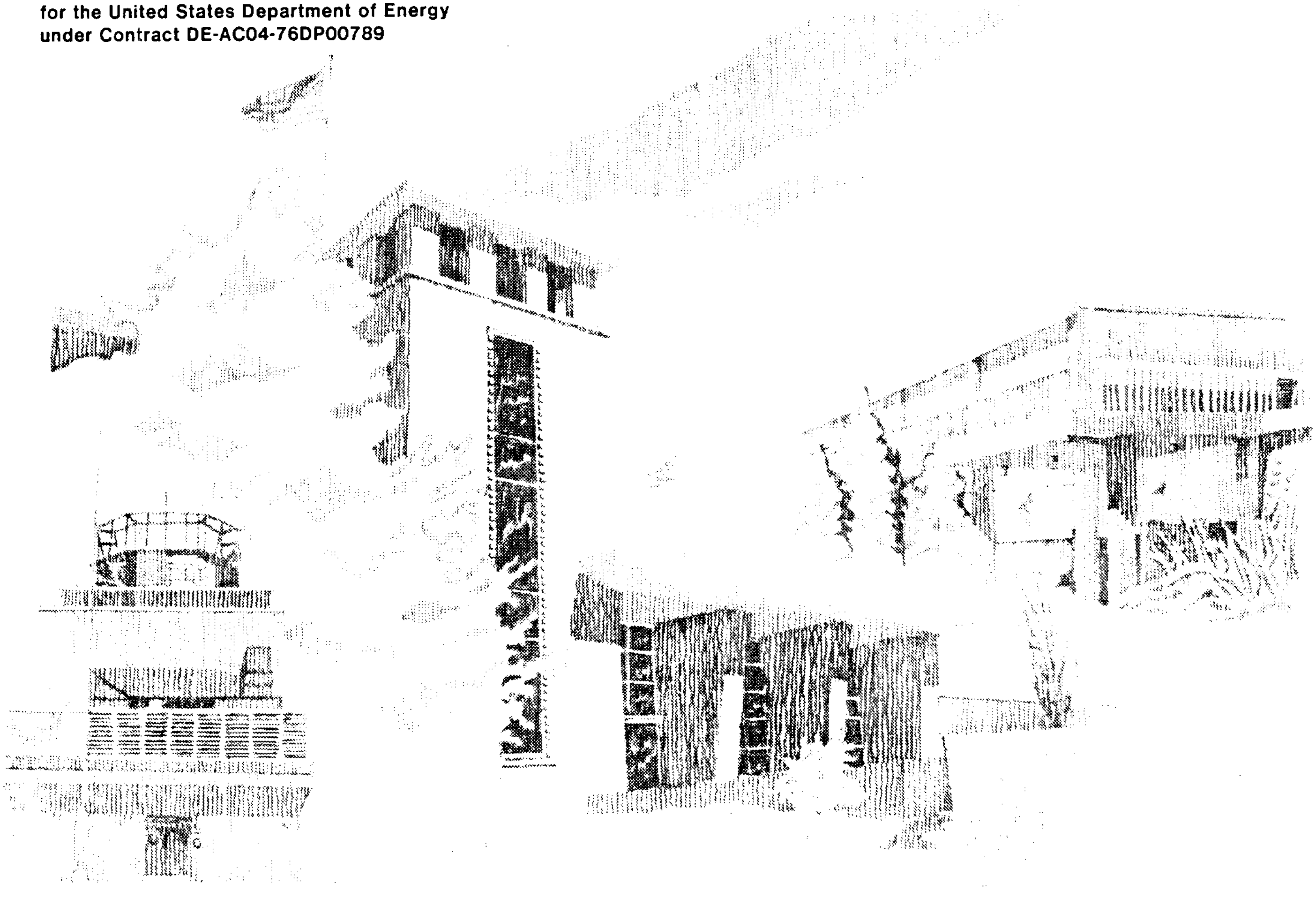
SANDIA REPORT

SAND91–0276 • UC–906
Unlimited Release
Printed June 1991

A Performance Evaluation of Biometric Identification Devices

James P. Holmes, Larry J. Wright, Russell L. Maxwell

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550
for the United States Department of Energy
under Contract DE-AC04-76DP00789



Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

Printed in the United States of America. This report has been reproduced directly from the best available copy.

Available to DOE and DOE contractors from
Office of Scientific and Technical Information
PO Box 62
Oak Ridge, TN 37831

Prices available from (615) 576-8401, FTS 626-8401

Available to the public from
National Technical Information Service
US Department of Commerce
5285 Port Royal Rd
Springfield, VA 22161

NTIS price codes
Printed copy: A03
Microfiche copy: A01

SAND91–0276
Unlimited Release
Printed June 1991

Distribution
Category UC–906

A Performance Evaluation of Biometric Identification Devices

James P. Holmes and Larry J. Wright
Facility Systems Engineering Division

Russell L. Maxwell
Systems Engineering Division
Sandia National Laboratories
Albuquerque, NM 87185

Abstract

When an individual requests access to a restricted area, his identity must be verified. This identity verification process has traditionally been performed manually by a person responsible for maintaining the security of the restricted area. In the last few years, biometric identification devices have been built that automatically perform this identity verification. A biometric identification device automatically verifies a person's identity from measuring a physical feature or repeatable action of the individual. A reference measurement of the biometric is obtained when the individual is enrolled on the device. Subsequent verifications are made by comparing the submitted biometric feature against the reference sample. Sandia National Laboratories has been evaluating the relative performance of several biometric identification devices by using volunteer test subjects. Sandia testing methods and results are discussed.

Contents

Figures

A Performance Evaluation of Biometric Identification Devices

Introduction

In many applications, the current generation of biometric identification devices offers cost and performance advantages over manual security procedures. Some of these applications are: physical access control at portals, computer access control at terminals, and telephone access control at central switching locations. An installation may have a single, standalone verifier which controls a single access point, or it may have a large networked system which consists of many verifiers, monitored and controlled by one or more central security sites.

Establishing how well a biometric identification device operates should be an important consideration in any security application. Performance data, however, is neither easy to obtain nor to interpret. Because there are no test standards yet to test against, test methods must be well documented. To measure its theoretical performance limit, a verifier could be tested in an ideal environment with robotic simulation of biometric data. The results of such a test would probably differ greatly from its real-world performance. The human element greatly affects the performance of any identity verifier. Environmental factors such as noise, light, electromagnetic radiation, moisture, dust, and temperature could also affect the verifier's performance.

Sandia began its latest verifier test series in November, 1989. Nearly 100 volunteers attempted many verifications on each machine. Environmental conditions were nominal, as the tests were all performed in a laboratory room for the convenience of the test volunteers. The biometric features used by the suppliers of the latest generation of verifiers in the Sandia tests include:

1. Fingerprint by Identix, Inc.[1]
2. Hand geometry by Recognition Systems, Inc.[2]
3. Signature dynamics by Capital Security Systems, Inc. Sign/On Operations.[3] (Formerly Autosig Systems, Inc.)
4. Retinal vascular pattern by EyeDentify, Inc.[4]
5. Voice by Alpha Microsystems, Inc.[5]
6. Voice by International Electronics, Inc.[6] (Formerly ECCO, Inc.)

General Test Description

Statistics have been compiled on false-rejection error rates and false-acceptance error rates for each verifier. The error rates are described as a percentage of occurrence per verification attempt. "Attempt" is used in this report to describe one cycle of an individual using a verifier as proof of being a validly enrolled user (enrollee). Most verifiers allow more than one try per attempt. "Try" describes a single presentation of an individual's biometric sample to the verifier for measurement. "False-rejection" is the rejection of an enrollee who makes an honest attempt to be verified. A false-rejection error is also called a Type I error. "False-acceptance" is the acceptance of an imposter as an enrollee. A false-acceptance error is also called a Type II error. False-acceptance attempts are passive; these are cases where the imposter submits his own natural biometric, rather than a simulated or reproduced biometric of the enrollee whose identity is claimed. To sum up:

false-rejection error = Type I error = rejection of an enrollee
false-acceptance error = Type II error = acceptance of an imposter.

Each verifier in the test is a commercially available unit. Because of the differences in these units and because we needed an equitable basis of comparison, we attempted to modify some of the units. One goal was to have each verifier report a final decision score for every verification try. Although the manufacturers were generally cooperative, it was not possible to achieve all our goals within the time and budget constraints of the testing. The Identix fingerprint verifier did not generate score data at all. The Capital Security signature verifier scores were not directly related to the accept or reject decision because of some additional decision making after the scores were generated. If a biometric testing standard ever becomes a reality, it should include a section on score data generation and reporting.

Software and/or firmware modifications were made by the manufacturer on some units to allow Sandia to collect the desired test data. All verifiers and specified modifications were purchased by Sandia. Where possible, each verifier was set up in accordance with the manufacturer's recommendations. In most cases, a representative from each manufacturer visited the testing laboratory to verify that his device was properly set up. Where problems were pointed out, attempts were made to rectify them. Some attempts were more successful than others within the limits of our test facility resources.

Testing and Training

The verifier tests at Sandia were conducted in an office-like environment; volunteers were Sandia employees and contractors. A single laboratory room contained all of the verifiers. Each volunteer user was enrolled and trained on all verifiers. There were both male and female volunteers and the efforts of both were valuable to this study. However, for the purpose of simplifying the text, we will use the term "his" rather than "his/her."

There is a learning curve for the proper use of a biometric identification device. As a user becomes more familiar with a verifier, his false-rejection rate decreases. This curve differs for individual users and verifiers. This learning effect was minimized for the Sandia testing by training the individuals before the test, by monitoring their performance, and by eliminating the first few weeks of test data in the results. A number of users were reenrolled on verifiers where there was indication of below-average performance. The transactions prior to the reenrollment were not included in the test results. Some manufacturers recommend that the users be reenrolled as many times as necessary to produce the best enrollment scores. We tended to limit reenrollments to known problem cases due to the relatively short duration of our test, and also to give the verifiers more nearly equal treatment. Verifiers on which it is more difficult to enroll would therefore tend to give somewhat less than optimum performance in our test. This effect is less significant for verifiers which modify the stored reference template by averaging in the biometric samples from successful verification attempts. The EyeDentify and the Identix units are the two tested verifiers that do not modify the reference template.

Other known errors were identified for removal by instructing the users to note on a real-time hardcopy printout any transaction where he made a mistake, or was "experimenting" and did not feel that the verification attempt was valid. A similar method was used to identify invalid transactions on the false-acceptance test. Many hours were devoted to identifying and removing invalid transactions from the data files. There is no doubt, however, that a small number of unrecognized errors remain in the data.

The problem of selecting a representative test user group is most vexing when testing biometric identification devices. While the differences in physiological and behavioral properties of humans are the bases for the devices, these same differences can bias test results between test user groups. The best solution to this problem seems to be to use many users and to make numerous attempts. The larger the numbers, the more likely the results will represent true performance values. Relative performance must be measured against absolute performance. A verifier's relative performance within a user group is generally easier to defend than is the absolute performance.

No extraordinary incentives were offered the volunteer users who performed the tests. Treats in the test room were used to tempt users to remain active. A drawing for a free lunch was offered to the regular users. About 80 of the 100 enrolled users remained fairly active in the tests. Work and travel schedules accounted for the loss of some users. Others simply became disinterested.

First Test Series: False-Rejection Testing

- users attempted verification on each machine many times
- test period was three months long
- users were allowed up to three tries per verification attempt.

Second Test Series:
Passive False-Acceptance Testing

- user submitted the personal identification number (PIN) of other users
- user then submitted his own natural biometric
- users were allowed up to three tries per verification attempt.

Data Processing

The first step in the data processing was to remove the invalid transactions that were noted on the printed data logs generated at each verifier. The data files were then processed to remove incomplete records and to convert the data to a common format. The data was sorted into individual user groups. Records from users making less than six transactions were deleted. User data obtained prior to user group reenrollment on a verifier was also deleted.

A verifier can usually be configured to accept up to three "tries" on a verification attempt. A "try" is one cycle of the user presenting his biometric to the verifier for measurement. To simulate verifier performance on one-, two-, and three-try attempt configurations, our users were instructed to try a third time if verification was not successful on the first or second try. Recorded time- of-day information allowed each score to be identified as either a first, second, or third try.

Up to three tries in a five-minute time interval were considered one verification attempt. Additional tries within this interval were ignored. Tries beyond the five-minute interval were considered another verification attempt. At any given threshold value, a score will produce either an accept or a reject. An accept on the first try is counted as an accept for one-, two-, and three-try configurations. An accept on the second try is counted as a reject on a one-try configuration and an accept on a two and three-try configuration. An accept on the third try is counted as a reject on a one and two-try configuration and an accept on a three-try configuration. Three rejects are counted as a reject on all three configurations. To sum up:

	Configuration Test Result		
Verification Action	one-try	two-try	three-try
Accept on first try	accept	accept	accept
Accept on second try	reject	accept	accept
Accept on third try	reject	reject	accept
No accepts with three tries	reject	reject	reject
No accepts with less than three tries	only actual rejects counted		

The false-reject error rate is the ratio of false-rejects to total attempts at verification. A false reject will be represented as "FR" and is reported in this document as a percentage value. Where transaction score data was available, the FR was calculated for each user for one-try, two-try, and three-try verifier configurations over a range of possible thresholds. The scores were used to find the number of errors that would have occurred had the verifier test threshold been set at each of the possible thresholds.

The false-accept error-rate is the ratio of false-acceptances to total imposter attempts. It will be represented as "FA" and was calculated for each user over the range of possible thresholds and presented as a percentage value.

The FR and FA for each verifier was calculated by averaging the user-percent error rates at each threshold value selected. The FA and FR error-rate curves are shown in the next section, entitled "Results of the Testing." Where possible, error-rate curves are shown for one-try, two-try, and three-try verification attempts. These curves exhibit two general characteristics. One characteristic is the non-zero value of the crossover point of the FA and FR curves. A second characteristic is the trend toward a lower rejection rate as the number of tries at verification increases. Both these characteristics force some tradeoffs in using these verifiers.

The non-zero error value at the crossover point means that there is no threshold setting where both the FA and FR error-rates are zero. The user must choose a threshold setting to fit the application. As the threshold is moved toward tighter security (higher rejection error rates), both imposters and valid users face higher rejection rates. Both are rejected less often when the threshold is moved toward lower security. The point at which the FA and FR curves cross over is referred to as the equal-error setting. This single-value error rate has been accepted as a convenient value to describe the performance of a verifier in the Federal Information Processing Standards Publication (FIPS PUB) 83. This and other single-value criteria have been used to characterize verifier performance, but no single value can provide much insight into the true performance capability of any verifier. The FA and FR error-rate curves provide much more insight into performance and should be examined for suitability in any security application.

Multiple-try attempts at verification can improve the performance of some biometric verifiers. The rejection rate for valid users generally decreases faster than the rejection rate for imposters, as more verification tries are allowed. Valid users are generally rejected because of inconsistent presentations of their biometric input. Additional tries allow the valid user to correct the inconsistencies and to generate an acceptable input that matches the reference template. Imposters are generally rejected because their biometric is not close enough to the reference to be accepted. Additional tries increase the chances of imposter acceptance if the biometric differences are small enough to be masked by the inconsistent user inputs and by tolerant threshold settings.

The Identix fingerprint verifier we tested did not have a customer adjustable system threshold. While individual thresholds could be adjusted, we did not get any test data at other than the factory-set threshold. The other verifiers tested did provide test score data, but the Capital Security signature verifier scores could not be used to generate error-rate curves because of a second calculation that it uses to make the accept or reject decision.

Our transaction time results were obtained by timing the users from when they touched the verifier until the verification attempt verdict was given. The users were not told that they were being timed. We feel that the results reflect verification times that would be typical in an actual installation. These times are substantially longer than the minimum times of a skilled user in a hurry.

Results of the Testing

Alpha Microsystems Results

Alpha Microsystems of Santa Ana, California bought out Voxtron and is now selling an updated system called Ver-A-Tel. This voice verification system makes use of a personal computer (PC), which contains the speech board hardware and the software programs. User terminals are touch-tone telephones. The Ver-A-Tel system is offered in two similar versions: the telephone intercept system (TIS) and the remote-access system (RACS). We tested the public TIS version, but not the direct-line RACS version.

The software supplied with the system provides the necessary management functions to enroll and delete users, to configure the system parameters, to display activities and alarms and to generate reports. Because this password-protected software is menu driven, it allows the security manager to select options from the screen and to fill in the blanks to configure the system. A supplied user's guide provides any additional information that might be needed.

Users were enrolled on the same touch-tone telephone that was later used to access the system. Prior

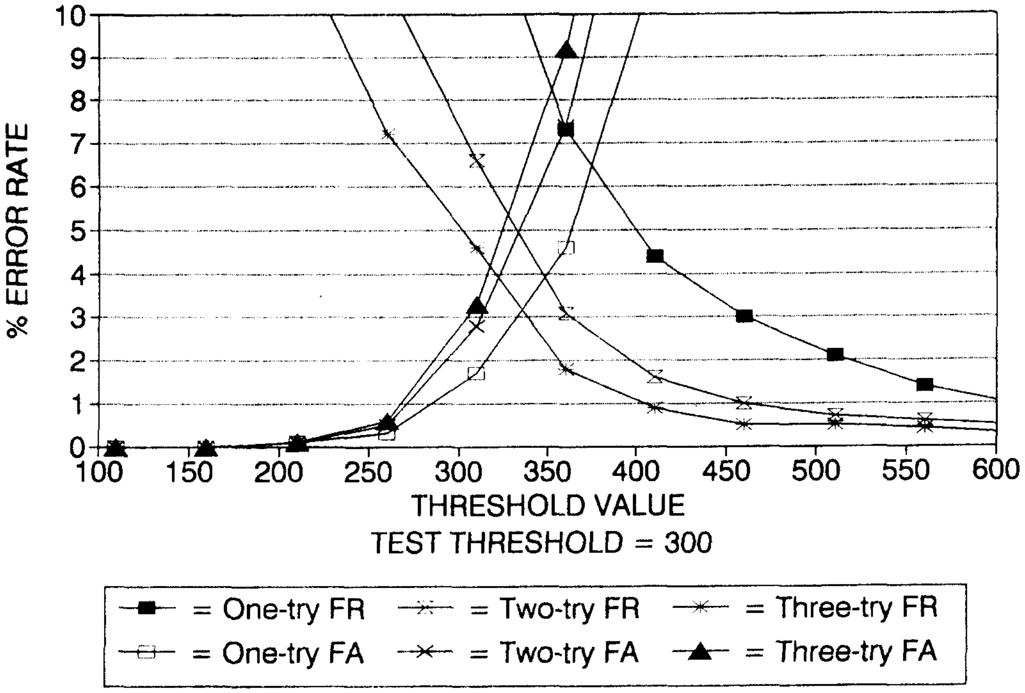


Figure 1. Alpha Microsystems Voice Verifer

Capital Security Systems, Inc. Results

Capital Security Systems, Inc. of Columbia, MD purchased the signature dynamics verifier line from Autosig Systems, Inc. This verifier consists of a user interface tablet and a controller which is designed to integrate into a host-computer access control system. The Capital security system offers products for both physical entry control and data access control. The user interface is similar for both applications. A variety of hardware and software options allow the system to function in applications from stand-alone protection of a single entrance to networked, host-based systems.

The user interface is a desk top tablet (~9 3/8 by 11 inches) that incorporates a digitizer tablet, a magnetic stripe card reader, and a tethered pen. The digitizer tablet (~2 1/2 by 5 inches) is the area where the user actually signs his name with the tethered pen. The system measures the dynamics of the user's signature to form the biometric template for enrollment and verification.

The controller can function as a stand-alone device with the user interface and door interface hardware, but must be connected to a computer for programming and user enrollment. An IBM PC or a higher class, compatible computer with a serial port and a floppy disk drive can be used. The computer class must match the controller interface requirement.

Software is provided to allow the security manager to configure the system and to enroll users. A menu-driven program provides the manager with the necessary options. Before a user can be enrolled, a user data record must be generated in the user data file. The manager selects the options and fills in the blanks to generate the record. For the model tested, a magnetic stripe card was required for ID entry. It was coded with the user's PIN and provided to the user for verifiers in this test series.

To enroll, the user must follow the illuminated prompts on the interface tablet. First the user PIN is entered with a swipe of his magnetic stripe card through the card reader. Next, the user is prompted to alternately sign on and wait while the system generates a template. Finally, the user is prompted when the sequence is complete. It normally takes two signatures and one verification signature to enroll. The signature must be within the marked digitizer pad area, using the tethered pen. The system can be used with a regular ball-point pen tip and a stick-on paper sheet over the pad, or with an inert, inkless pen tip system directly on the digitizer pad.

Verification is similar to enrollment. The user PIN is entered with the magnetic card and the user signs his name on the digitizer pad with the tethered

to enrollment, the security manager created a record for each user and each was assigned a unique PIN. An optional secret enrollment passcode, to prevent an imposter from enrolling in place of the authorized user, was not tested.

A phrase is required for enrollment and subsequent verification. The security manager can select from a number of standard phrases on the menu display; from this selection, he can allow the user to make up his own phrase. There are some restrictions on user-selected phrases, such as the minimum and maximum length and the optimum number of syllables. These options are discusssed in the User's Guide which is supplied with the system.

Voice verifier manufacturers are quick to point out that security is enhanced if each user has a secret phrase. These manufacturers, however, do not address the problem of how to keep a phrase secret that must be uttered into a microphone. On the other hand, it is certainly less likely that an imposter would be accepted if he does not know the proper phrase. It is even plausible that a valid user could have a lower false-reject error rate with a chosen phrase that was more natural or familiar to him. The objective of our test was to measure the ability of the system to verify users based solely on their biometric properties. Thus, we assigned the same phrase to all users.

To enroll, a user calls the verifier telephone number. The system answers and instructs the user to enter his PIN on the touch-tone keypad. If the system finds that the PIN belongs to someone who is not yet enrolled, it tells the user what he must do to enroll. This may include an instruction to enter the proper enrollment passcode on the keypad. The user is instructed to say the verification phrase a number of times. The system performs checks on each response and may prompt the user to be more consistent and to repeat the phrase again. When the system parameters for a successful enrollment are met, the system so informs the user. A user template is generated from the enrollment data and is stored for future verification of the user's identity. The system may tell the user that the enrollment was better than most. This indicates that the enrollment phrases were very consistent. It is also possible for the user to fail. In this case, the user is told to practice and try again. The security manager can also check the enrollment scores to get a measure of the enrollment performance. Individual accept or reject thresholds can be set by the security manager to compensate for differences in user performance. This adjustment is made (plus or minus) to the system threshold setting.

On verification attempts, an enrolled user's PIN is recognized by the system and is used to retrieve the proper template from the enrollment database for verification. The user is then prompted to say the phrase for verification. Optionally, the new phrase data may be averaged into the stored template to update the template each time the verification is successful. In time, if the user becomes more consistent and the verification scores improve, the security manager may opt to adjust the user threshold value to a more secure value. Experienced users generally skip the voice prompts because a preceding tone signals the user that he can go ahead without further delay if he does not need the voice instruction.

The time information given for the Alpha Microsystems voice verifier is different from other verifiers because it includes dialing a 5-digit telephone number and waiting for the verifier to answer. We included this scenario because the telephone access method was also used in our test verifier. Other access methods may result in different transaction times. The minimum time of ~13 seconds was necessary to perform the following steps:

- lift the phone and dial a 5-digit extension
- wait for the voice system to answer and generate the tone prompts (without waiting for the subsequent voice prompts)
- enter a 4-digit PIN on the phone keypad
- say "yankee doodle dandy"
- be verified.

The average user in our test took ~19.5 seconds for a complete verification. This average includes multiple-try attempts when this was required by the system.

The crossover point where the one-try false-reject and the one-try false-accept curves are equal has an error rate of 6.5% at a threshold value of ~375. At the test threshold setting of 300, the three-try, false-reject error rate was 5.1% and the three-try, false-accept error rate was 2.8%.

There were 5434 transactions in the false-reject test and 2990 transactions in the false-accept test. The results of these tests are shown in Figure 1.

pen. A prompt then tells the user whether the verification was successful or if another signature try is necessary. Two tries are usually allowed. Each successful verification is averaged into the reference template to allow the system to accommodate long-term changes in the user signature. This averaging can be inhibited by the security manager.

Imposter testing consisted of each imposter entering PINs by using the magnetic stripe badges of all other users. The imposter knew the real user's name from the badge, but did not have a sample of the user's signature. The imposter was free to try to sign the actual user's name. As a matter of interest, we attempted some verifications by tracing over valid signatures. The scores were generally much worse than other imposter attempts because of the importance of the signature dynamics in verification. None of the tracing attempts were included in our test results.

The time to perform a verification depends in part on how long a user takes to sign his name. Our users averaged ~15 seconds to verify on the Capital Security system; this time includes PIN entry via a swipe card reader and some multiple-try attempts as required by the system. The minimum time observed was ~12 seconds.

Error-rate curves are not shown because the Capital Security accept or reject decision process is more than just a function of the transaction score. A second decision calculation is performed on all tries that produce a score between 16,000 and the verifier threshold setting. The threshold was set at 21,000 for our test.

All false-accept and false-reject error rates obtained were from a count of the errors at the operational threshold:

False-Reject Error Rate	Percentage
three-try	2.06%
two-try	2.10%
one-try	9.10%

False-Accept Error Rate	Percentage
three-try	0.70%
two-try	0.58%
one-try	0.43%

The Capital Security is usually set up for two tries.

There were 3106 transactions in the false-reject test and 6727 transactions in the false-accept test. The Capital Security system error-rates are shown in Figure 2.

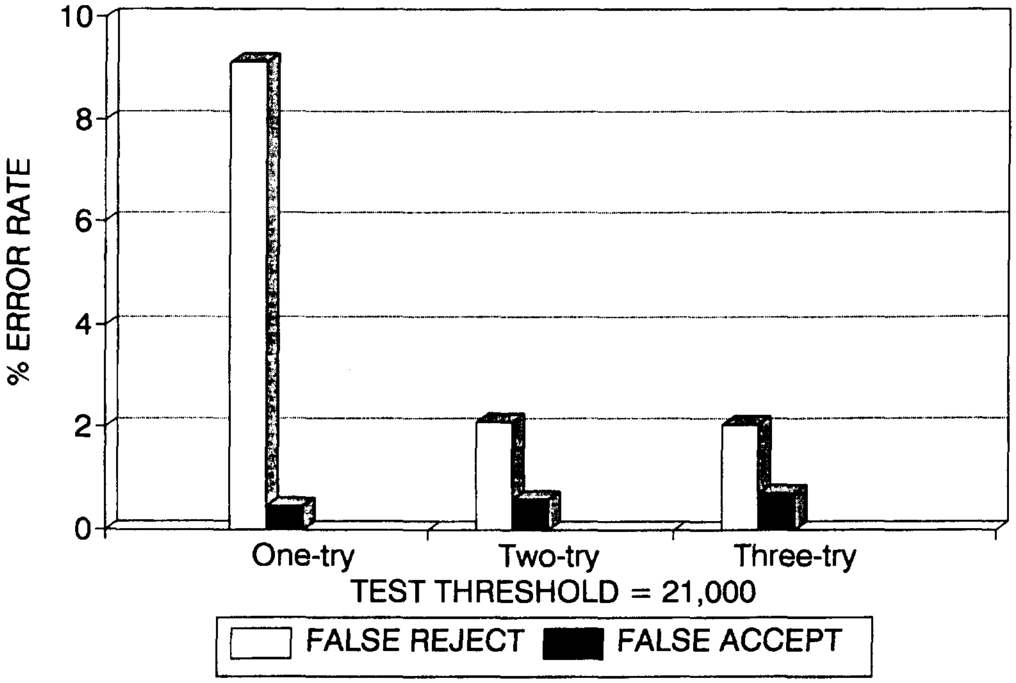


Figure 2. Capital Security Signature Dynamics

International Electronics (ECCO VoiceKey) Results

International Electronics, Inc. of Needham Heights, MA purchased ECCO Industries, Inc. of Danvers, MA and now markets the ECCO VoiceKey. The VoiceKey is a self-contained, wall-mounted user interface that communicates with a controller over a copper wire cable. The user interface contains an alphanumeric display, keypad, a microphone, an audible beeper, and indicator lights. Keys, displays, etc. allow all necessary functions to be performed at the user interface. Some of these functions are user enrollment and system management.

The user interface and controller can operate in a stand-alone mode to provide security at a single entry point, or can be networked through a network controller to other units in a security system. A VoiceKey network has a master voice reader and slave voice readers. The master voice reader is normally used for all enrollments and programming, which are then downloaded to the slave readers. Enrollment and programming can be performed at any slave, but it cannot be downloaded to any other reader. A printing capability allows audit information to be output to a printer connected to the controller of the master reader.

User enrollment is normally performed at the master voice reader by a security manager who is authorized to enter the programming mode. This authorization must be verified by voice before the programming mode can be entered. Programming is accomplished by keypad key inputs. Message displays and lights provide feedback to the programmer as the program steps are entered. A supplied programming manual provides complete information on the programming procedures. A user program allows new users to be added. This option requires the security manager to enter a unique PIN to access zone data and to enter the user authorization level for the new user. The reader then displays a series of message and colored-light prompts for the new user to initiate the sequence and to say his password several times. A red/green light display at the end of the enrollment sequence informs the new user of failure/success in enrolling. (This frustrates color-blind users who cannot distinguish between the red and green colors.) If successful, the new user can practice using his password as desired. Each successful verification causes the user's template to be modified by the new input.

Verification can be accomplished in ~5 seconds. Users averaged ~6.6 seconds per one-try attempt; in this time, they were able to enter a 4-digit PIN on the keypad and to utter the single password.

The crossover point where the one-try, false-reject curve and the one-try, false-accept curve are equal has an error-rate of 8.2% at a threshold value of 100. Only one-try, false-accept data was obtained for the VoiceKey verifier. There are three user thresholds available for the VoiceKey verifier. Security level 1 is a threshold of 75, level 2 is a threshold of 65 and level 3 is a threshold of 55. At the test threshold setting of 75, the three-try, false-reject error rate is ~4.3%, and the one-try false-accept error-rate is ~0.9%.

Voice verifier manufacturers are quick to point out that security is enhanced if each user has a secret phrase. These manufacturers, however, do not address the problem of how to keep a phrase secret that must be uttered into a microphone. On the other hand, it is certainly less likely that an imposter would be accepted if he does not know the proper phrase. It is even plausible that a valid user could have a lower false-reject error rate with a chosen phrase that was more natural or familiar to him. The objective of our test was to measure the ability of the system to verify users based solely on their biometric properties. Thus, we assigned the same phrase to all users.

We experienced high, false-rejection error rates with the assigned password. The manufacturer's representative suggested that each user be allowed to choose a password familiar or comfortable to him. We gave additional training and reenrolled ~15% of the users that were experiencing the most trouble with verification. On reenrollment, the users could choose from several suggested words. Some were allowed to select a word of their choice. This effort did produce better verification scores for many of the individuals after they were reenrolled. We were unable to correlate the effect of reenrollment on the long-term, false-rejection error rates. Several variables remain in the verification process. As the user becomes more familiar with a password, he would be expected to get more consistent in its use. The user's reference template is also modified for each successful verification, and thus should improve the verification scores of consistent users. An analysis of entire user group performance before and after reenrollment, however, did not show a significant improvement over time.

There were 4871 transactions in the false-reject test and 3270 transactions in the false-accept test. The graphical results of these tests are shown in Figure 3.

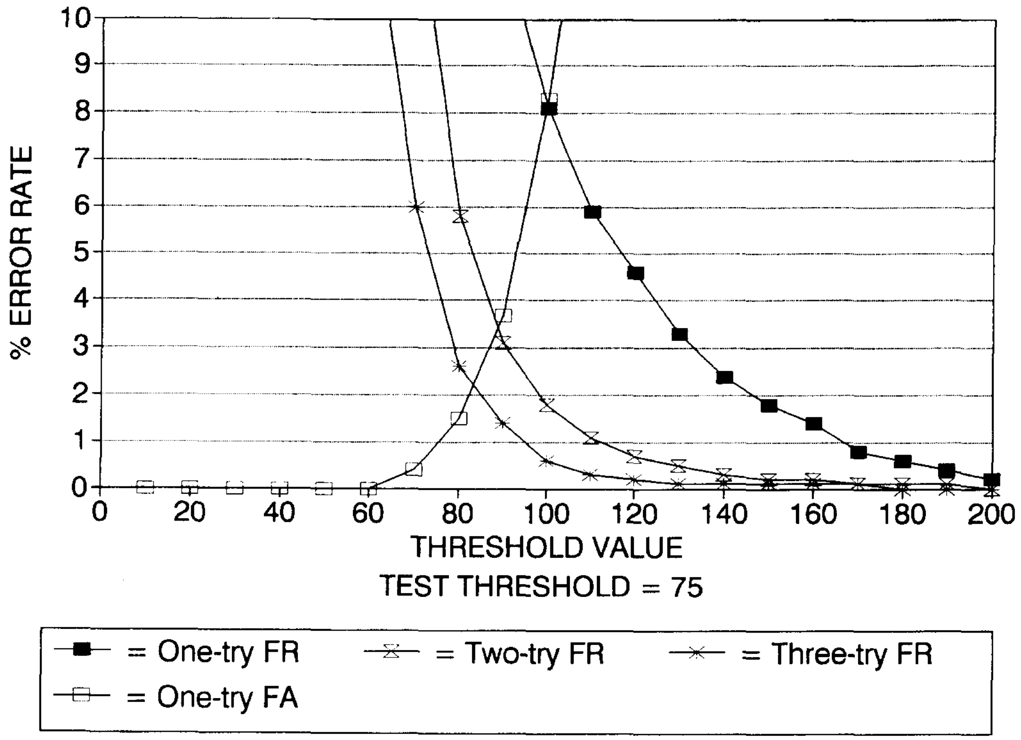


Figure 3. International Electronics Voice Verifier

EyeDentify Verify Mode Results

The retinal pattern verifier in this test series was Model 8.5, manufactured by EyeDentify, Inc. of Portland, Oregon. The verifier includes a reader and a controller. The reader contains an aperture where the user looks to align his eye with an optical target, which appears as a series of circles. As the user moves his eye around, the circles become more or less concentric. Proper alignment is achieved when the circles appear concentric and the user is looking at the center of the circles. The reader also contains a display, a keypad, and an insertion reader for magnetic stripe cards. A copper cable connects the reader to a controller box that contains processing and interface electronics.

The controller can function as a stand-alone device with the user interface and door interface hardware, but must be connected to a computer for programming and user enrollment.

Two readers were tested. Reader 1 was set up to operate in the verify mode using a PIN entered via an insertion card. Reader 2 was set up to operate in the "hands-free" recognize mode. The results for Reader 1 are discussed in this section, and the results for Reader 2 are discussed in the following section entitled: "EyeDentify Recognize Mode Results."

The software allows the security manager to configure the system and to enroll users. A menu-driven program provides the manager with necessary options. Before a user can be enrolled, a user data record must be generated in the user data file. The manager selects the options and fills in the blanks to generate the record. Once the record generation in the enrollment sequence is completed, a message instructs the user to enroll. The new user then aligns the optical target in the viewing aperture and presses the "ENTER" key on the keypad to initiate the eye-scan sequence. Each subsequent scan generates a score on the computer display and allows the security manager to accept or reject it. The user template is generated from an average of the accepted scans on enrollment. This template is not modified by subsequent verifications, so it is important to take some care during enrollment and not to accept scores below the mid 70s. It is not difficult for most properly instructed users to score above 80.

The user's PIN must be entered for verification. The EyeDentify 8.5 allows either manual entry on the keypad or automatic entry by using the card reader. Our tests used the card entry option. The average time for our users to perform the verification process was ~7 seconds. This time included some multiple-try attempts and the removal of glasses by some users after inserting their card. The quickest times were around 4.5 seconds.

The false-reject error rates for EyeDentify Model 8.5 in this test are significantly less than for the Model 7.5 we tested in 1987. There are two differences between the models we tested that could account for the decrease in these errors:

1. Improved data acquisition software for Model 8.5 now tests for eye fixation before accepting a scan. This feature reduces the chance of a rejection due to eye movement.
2. The Model 7.5 we tested used only keypad PIN entry, while the Model 8.5 we tested used magnetic card PIN entry.

The verify mode crossover point, where the one-try, false-reject error rate and one-try, false-accept error rate are equal, was ~1.5% at a threshold of ~45 for Model 8.5. At the test threshold setting of 70, the three-try, false-reject error rate was 0.4%. No false-accepts were recorded at this threshold value. There were 5134 transactions in the false-reject test and 4196 transactions in the imposter test. The test results for Reader 1 are shown in Figure 4.

EyeDentify Recognize Mode Results

A unique option of the Model 8.5 verifier is the "hands-free" mode of operation. While the verifier is operating in this mode, the user merely peers into the viewing aperture and aligns an optical target by positioning his head. The verifier senses the user's presence, takes a scan, and decides whether or not the scan data is from an eye. If a digital pattern is generated from an eye, the verifier searches the template data base for a match. If a match is found, the verifier recognizes the user as valid. Otherwise, the user is requested to "REPEAT" up to two more tries until a valid match is found. The user is rejected if a match is not found in three tries.

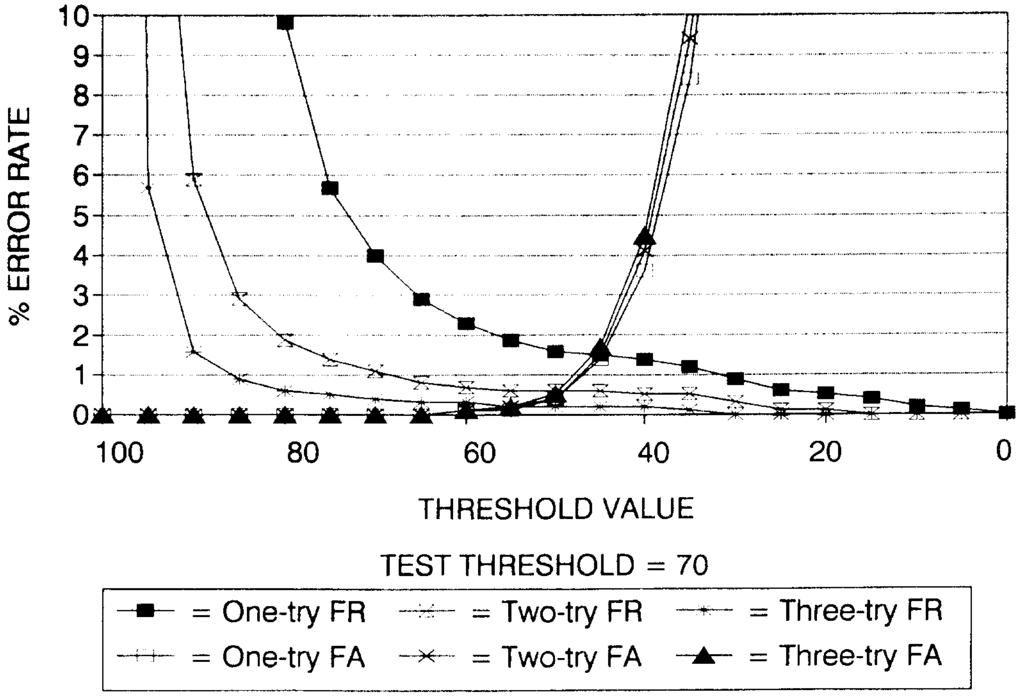


Figure 4. EyeDentify Eye Retinal Pattern

No timing information was taken for the recognize-mode operation because there is no precise point that can be observed when the user initiates the sequence. The user peers into the aperture, aligns the target, and waits for the target to turn off at the end of the scan. The auto-scan feature eliminates the need to insert the magnetic card and press the START button, cutting ~2 to 3 seconds from the verify-mode transaction time. We had a user database of ~100 users that had to be searched to find a matching template for each transaction. This searching did not add a noticeable time delay to the transaction. Larger databases will add more search time to each transaction.

The threshold was set to 75 for the recognize mode of operation. This means that any scan that produces a score of 75 or less is rejected as not being a member of the enrolled user base. A score of greater than 75 causes an accept, and the name of the identified user is displayed on the reader.

There were 5072 transactions recorded on the recognize-mode reader. A transaction is defined as any scan the machine decides meets the minimum criteria to be an eye. None of these scans resulted in a false accept. This result is especially significant because the 100 user database multiplies the possible matches to over half a million!

False-reject information cannot be reported on the "hands-free" recognize reader because there is no PIN associated with a reject that can tie it to a user. No doubt the false-reject rate is significantly higher in the recognize mode because the user does not control the start of the scan. In many attempts, the scan started before the user had the target properly aligned. With practice, most users learned to use the recognize mode to their satisfaction. EyeDentify has now modified their acquisition software to allow users more time to align the target. This change should lower the false-reject error rate.

Identix Results

The fingerprint verifier evaluated in this test was the TouchLock, manufactured by Identix, Inc. in Sunnyvale, California.

The user interface to the Identix system is a sensor module that contains the finger platen/scanner hardware, a display, a keypad and communications electronics. This module is ~8.2 inches wide, 4.4 inches tall, and 3.9 inches deep. The sensor module communicates with a remote processor module over a copper wire cable. The remote module contains the processor, memory, input/output hardware, and communications hardware to support stand-alone operation at a single entry point or in a network environment. Our test verifier was connected to a host computer with the Identix TouchNet software support system. It also was connected to a magnetic-stripe, swipe-card reader via its built-in card reader interface. The card reader was used to enter user PIN information for verification attempts.

The Identix supplied software is a password-protected, menu-driven program for IBM PC and compatibles. It provides the capability to configure the system, to set up user records, and to generate reports.

User enrollment is performed at the sensor module. A security manager must first be verified by a fingerprint scan before the enrollment mode can be entered. Messages on the sensor module display provide user prompts and status information. A unique PIN must be entered for the new user, followed by a number of finger scans that allow the system to generate a template. If the enrollment is successful, a quality rating is displayed. The manager can accept or reject the enrollment at this point. The manufacturer recommends that only "A" or "B" quality ratings be accepted. A "C" rating is the least desirable. If the enrollment is unsuccessful, the system informs the user, who is invited to try again. The templates are not modified by subsequent verifications, so if problems appear, the user should be enrolled again.

We accepted some "C" enrollments for our test. We retrained and reenrolled users that experienced the most problems with verification. The reenrollment did not always result in a higher quality rating. A number of our users appear to have poor quality fingerprints that would not produce good results, even when other fingers were tried. Another problem was caused by low humidity during our test period. User's skin would dry out to the point where the system could not verify the user. Lotion or skin moisturizer often solved the dryness problem.

Our users all had the factory-default verification threshold of 125. The host system software allows the security manager to change individual threshold values, but we did not exercise this option. Our test results do not include the error-rate curves because this verifier did not generate verification score information. Only the percentages of false-reject errors and the false-accept errors at the factory-default threshold can be reported.

The lack of score data hampered our attempts to quantify the Identix verifier. Enrollment quality ratings were generated from groups of finger scans. Individual scan quality was not available. Some clues were available from prompts to position the finger further up or down on the platen, but we could not correlate the finger positioning to scan quality. Our

false-rejection error rates were significantly worse than the estimated error rates published in the Identix TouchNet User's Guide, supplied by Identix with the TouchNet system. Identix indicates an estimated single-try, false-rejection error rate of ~3% for an enrollment threshold setting of 125. We experienced over 9% false-rejections for three-try attempts with the 125 threshold setting. The cold, dry weather effect on skin conditions in Albuquerque could account for some of this difference. Individual score data might have given us more insight into the problem.

Our users averaged ~6.6 seconds for a card PIN entry verification, including multiple-try attempts. The fastest users verified in under 5 seconds.

Two identical readers were used in this test. The two readers tested were set up for a maximum three-try attempt and only reported a single accept or reject transaction result for each attempt. If a user was accepted on either the first, second, or third verification try, the attempt was recorded as an accept. If a user was rejected on all three tries, the attempt was recorded as a reject. Individual-try data was not available from the monitoring program.

Reader 1 logged 2248 verification attempts with a false-reject error rate of 9.4% and no false accepts. Reader 2 logged 2316 attempts with a false-reject error rate of 9.5% and no false accepts. The number of false-accept attempts was 3424. The false-reject error rate equals the percentage of the three-try false-rejects that occurred in the verification attempts.

Recognition Systems, Inc. Results

The Model ID3D-U hand-profile verifier manufactured by Recognition Systems, Inc. (RSI) of San Jose, California was evaluated in this test. The verifier houses the hand geometry reader and all the electronics in one enclosure. Both the wall mount or the desk top models are available. The reader has a platen with guide pins to aid in proper hand placement; an optical imaging system acquires the hand geometry data. Displayed messages prompt the user and provide status information. A keypad and an insertion magnetic-stripe card reader record user data input. This verifier can be configured for stand-alone operation or for use with a host processor. Our test verifiers were configured for use with a host processor. The host management software we used included some custom features not required for normal system operation.

User enrollment takes place at the verifier reader. In actual security system applications, each user is assigned an authority level and, if required, a password for entering the security management command mode. A new user can only be enrolled by a security manager with the proper authority level and password to enter the enrollment sequence. The manager must first be verified on the hand geometry reader, and then he must enter the proper password within a time limit to initiate the enrollment sequence. Our test software did not require a password or manager verification for user enrollment. It provided the necessary functions with a menu-driven program that allowed the test conductors to fill in the blanks and to initiate the enrollment sequence.

User Enrollment Sequence

1. A valid PIN is entered by the new user.
2. A ** PLACE HAND ** message then appears on the reader display.
3. The user must then place his hand on the platen and against the guide pins.
4. When the imaging system determines that the hand is properly positioned within the time limit, the hand geometry data is acquired and a ** REMOVE HAND ** message is displayed.
5. The message display prompts are repeated at least two more times, and the user reference template is then generated from an average of the three inputs.

User Verification Sequence

1. Enter the user PIN by keypad or card reader.
2. Follow the ** PLACE HAND ** and ** REMOVE HAND ** instructions on the display.

The average verification time for our users was ~5 seconds, with card PIN entry. (Times as low as ~2.9 seconds were observed.)

The false-reject error rates for Model ID3D-U in this test were less than the rates were in 1987 when we tested the Model ID3D-ST. PIN entry by magnetic card rather than by keypad is the most likely reason for the lower error rates.

The crossover point, where the one-try, false-reject error rate and the one-try, false-accept error rate are equal, was ~0.2% at a threshold of ~100 for Model ID3D-U. At the test threshold value of 75, the three-try, false-reject error rate was less than 0.1% and the one-try, false-accept error rate was ~0.1%. Three-try, false-accept error rate data was not obtained in this test. The test results were very similar on both readers; thus, only Reader 0 results are plotted.

Reader 0 logged 5303 transactions in the false-reject test and 5248 transactions in the imposter test. Reader 1 logged 5285 transactions in the false-reject test and 3839 transactions in the imposter test. The results of this test are shown in Figure 5.

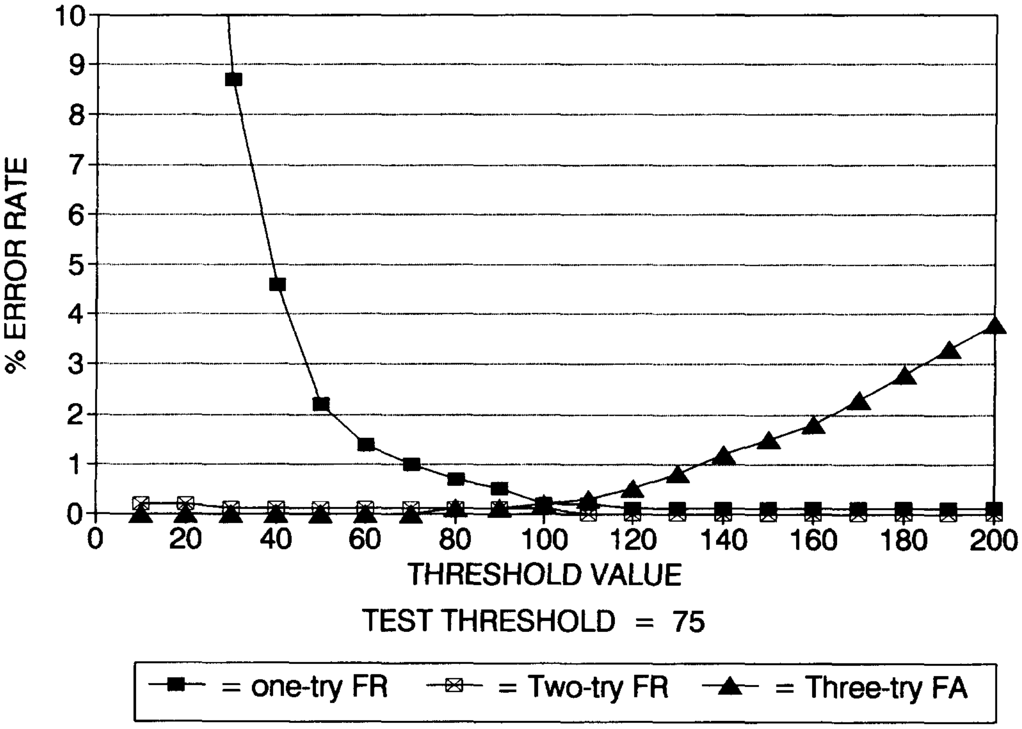


Figure 5. Recognition Systems Hand Geometry

Summary

The relative performance of the tested verifiers can be deduced from the test results. These results include the user variables in the operation of the machines and are therefore representative of the performance that can be expected with average users; at the same time, they are not a true measure of the machines absolute performance limits. The degree to which our results differ from the performance limits is an indication of the complexity of the user interface. As an interface becomes more complex, more user variables are introduced that could shift the test results away from the performance limit.

From a test viewpoint, it is desirable to have a final score value reported for each verification try. This report is not possible, however, because some verifiers do not provide the score data necessary for us to calculate error-rate curves. Verifier results in this case are given only for the one threshold value tested. It would have been possible to repeat the performance tests at a number of different threshold values to obtain points on the error-rate curves, but we did not have the resources for such an extensive test. This is only one of several roadblocks for developing biometric verifier testing standards.

A user survey was taken late in the test. The summary results are given in the appendix. Users generally preferred the verifiers that produced the fewest false-rejects and which took the least time to use. User frustration grew rapidly with high, false-rejection rates; these rates proved to be a bigger problem for them than did the slow transaction times. The RSI hand geometry was overall the user favorite.

The verification timegraph (see Figure 6) shows the average transaction times for:

- entering the PIN
- presenting the biometric feature
- verification or rejection.

The Alpha Microsystems time also includes the time necessary:

- to dial a five-digit number on a touch-tone telephone
- wait for an answer from the system.

This data was obtained by timing the users without their knowledge. These times are representative of actual-use transactions; they are not intended to indicate the minimum times possible.

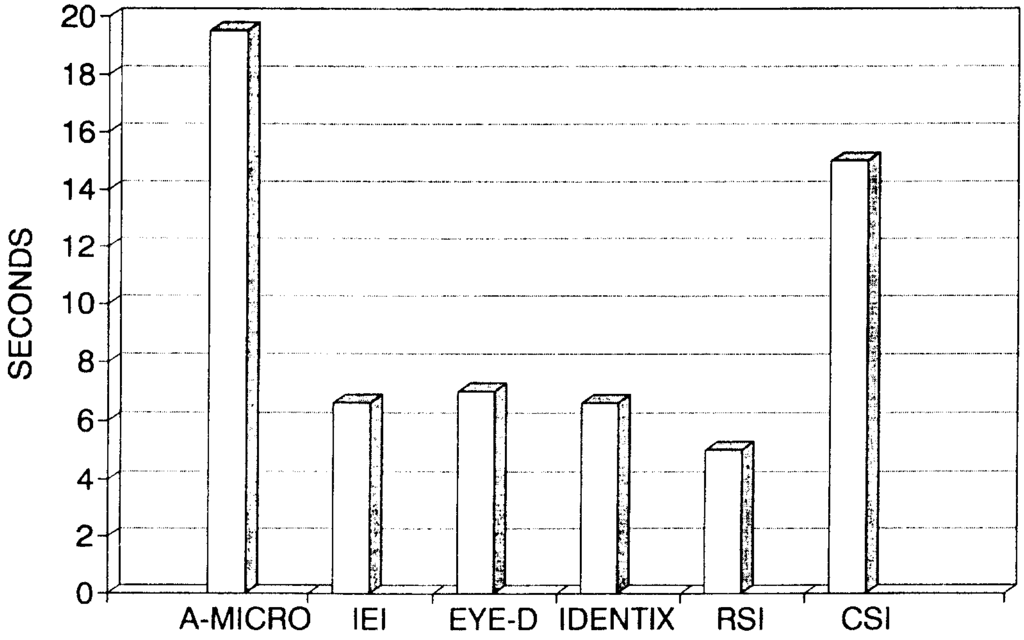


Figure 6. Average Verification Time in Seconds

Conclusions

Performance is a very important issue, but it is not the only factor in choosing a biometric identification device. The device must also be suitable for the facility in which it is installed. The present generation of biometric identification devices provides reliable and cost-effective protection of assets. Available computer interfaces and software provide effective security management with real-time control, transaction logging, and audit-tracking capabilities. The current need in the biometric identification field is to have the market make greater use of what already exists. While new biometric devices are still emerging, it is unlikely that any of them will turn the market around with a price or performance breakthrough.

The error-rate curves contain much more information about the performance of the verifiers than was included in our individual discussions. Manufacturers can provide additional information about how to apply their devices to specific requirements. Finally, it is important to keep the error rates in perspective to the real world. A 3% false accept means that there is a 97% probability that an imposter will be detected.

References

[1]Identix, Inc., 510 N. Pastoria Ave., Sunnyvale, CA 94086, (408) 739-2000

[2]Recognition Systems, Inc., 1589 Provencetown Drive, San Jose, CA 95129, (408) 257-2477

[3]Capital Securities Systems, Inc., Capital Security Operations, 9050 Red Branch Road, Columbia, MD 21045, (301) 730-8250

[4]EyeDentify, Inc., PO Box 3827, Portland, OR 97208, (503) 645-6666

[5]Alpha Microsystems, 3501 Sunflower, Santa Ana, CA 92704, (714) 957-8500

[6]International Electronics, Inc., (ECCO) VoiceKey, 32 Wexford St., PO Box 584, Needham Heights, MA 02194, (617) 449-6646.

APPENDIX

User Survey Results

	ALPHA		EYEDENTIFY			RECOGNITION	AUTOSIG	
Which machine do you feel:	MICRO	ECCO	VERIFY	RECOGNIZE	IDENTIX	SYSTEMS	SIGNON	NONE
1. is the easiest to use?	0	4	2	22	15	35	1	0
2. is the fastest?	1	4	1	28	8	35	0	0
3. is the slowest?	38	5	1	2	9	0	24	1
4. rejects you most often?	11	36	2	5	17	1	6	0
5. rejects you least often?	11	6	10	11	12	42	9	0
6. requires most concentration?	10	25	12	23	6	1	4	0
7. requires most proficiency?	11	23	9	15	11	1	9	4
8. requires least proficiency?	5	6	4	9	12	38	6	1
9. is most frustrating to use?	10	34	2	12	12	0	5	3
10. is most friendly/fun?	5	2	6	17	13	31	6	1
11. gives health/safety concerns?	1	0	23	21	1	5	0	47
12. gives invasion of privacy concerns?	0	1	2	2	3	1	16	56
13. was most difficult to enroll on?	17	21	1	1	15	2	3	18
14. was most intimidating to use?	5	16	4	6	4	0	2	41
15. best to secure a computer terminal?	7	4	12	10	22	18	7	9
16. best for door security?	3	7	18	19	13	27	3	4
17. best for bank/POS use?	1	0	13	8	21	11	23	6
18. best for large population?	2	2	5	14	16	38	3	8

19. Did you like card or pin best? Card: 56 Pin: 17 None: 3

NOTES:
1. Number of respondents: 76
2. Respondents were allowed to make multiple responses to each question.

DISTRIBUTION:

1 Edward J. McCallum, Director
Office of Safeguards and Security
US DOE
SA-10
Washington, DC 20545

1 William L. Barker, Acting
Dep. Asst. Secy. for Security Affairs
US DOE
SA-1
Washington, DC 20545

1 David A. Jones, Acting Director
Policy, Standards and Analysis Division
Office of Safeguards and Security
US DOE
SA-12
Washington, DC 20545

1 William J. Desmond, Chief
Physical Security Branch
Office of Safeguards and Security
US DOE
SA-121
Washington, DC 20545

1 Larry D. Wilcher, Chief
Technical and Operations Security Branch
Office of Safeguards and Security
US DOE
SA-123
Washington, DC 20545

1 Jerry C. Howell, Deputy Director
Field Operations Division
Office of Safeguards and Security
US DOE
SA-13
Washington, DC 20545

1 Donald C. Tubbs
Assessment and Integration Branch
Office of Safeguards and Security
US DOE
SA-131
Washington, DC 20545

1 Ernest E. Wagner, Chief
Weapons Safeguards and Security Operations
Branch
Office of Safeguards and Security
US DOE
SA-132
Washington, DC 20545

1 A. J. Heysel, Chief
Production/Energy Safeguards/
Security Operations Branch
Office of Safeguards and Security
US DOE
SA-133
Washington, DC 20545

1 G Dan Smith, Chief
Planning and Technology Development Branch
Office of Safeguards and Security
US DOE
SA-134
Washington, DC 20545

1 Carl A. Pocratsky
US DOE
SA-134
Washington, DC 20545

1 Marshall O. Combs, Deputy Director
Headquarters Operations Division
Office of Safeguards and Security
US DOE
SA-14
Washington, DC 20545

1 David A. Gurule, Acting Director
Security and Nuclear Safeguards Division
US DOE/AL
PO Box 5400
Albuquerque, NM 87115

1 Donald J. Cook, Director
Attn: Stan Laktosic, Tom Golder
Central Training Academy
US DOE/AL
PO Box 5400
Albuquerque, NM 87115

DISTRIBUTION (Continued):

1 Donald Jewell, Assistant Director
Central Training Academy
US DOE/AL
PO Box 5400
Albuquerque, NM 87115

1 Ronald Perry
Argonne National Laboratory
Bldg. 222 Electronics
Argonne National Laboratory
9700 South Cass Avenue
Argonne, IL 60439

1 Roger L. Black
W. Patrick Keeney
Argonne National Laboratory
Bldg. 752/MS 6000
PO Box 2528
Idaho Falls, ID 83403

1 Larry Runge and George Schoener
Safeguards and Security Division
Bldg. 50
2400 Upton Road
Upton, NY 11973

1 Kris Dahms
Safeguards and Security Division
Bldg. 703
2400 Upton Road
Upton, NY 11973

1 Robert L. Windus, Security Officer
US DOE/BP
PO Box 3621
Portland, OR 87208

1 Harold W. Kelley, Director
Safeguards and Security Division
US DOE/CH
9800 South Cass Avenue
Argonne, IL 60439

1 Rudy Dorner
Fermi National Accelerator Laboratory
MS 102
Batavia, IL 60150

1 H. R. Martin, Acting Director
Safeguards and Security Division
US DOE/ID
785 DOE Place
Idaho, Falls, ID 83402

1 Timothy L. Mitchell, L 024
Lawrence Livermore National Laboratory
PO Box 808
Livermore, CA 94550

1 Darryl B. Smith
James W. Tape
N-DO/MS E550
Los Alamos National Laboratory
PO Box 1663
Los Alamos, NM 87545

1 Jack England, Division Leader
OS-DO, MS G729
Los Alamos National Laboratory
PO Box 1663
Los Alamos, NM 87545

1 E. Wayne Adams, Director
Safeguards and Security Division
US DOE/NV
PO Box 98518
Las Vegas, NV 89193-8518

1 William G. Phelps, Director
Safeguards and Security Division
US DOE/OR
PO Box 2001
Oak Ridge, TN 37831-8570

1 J. A. Bullian, Director
Safeguards and Security Division
US DOE/PNR
PO Box 109
West Mifflin, PA 15122

2 Joseph W. Wiley, Director
Safeguards and Security Div
US DOE/RL
PO Box 550
Richland, WA 99352

DISTRIBUTION (Continued):

1 Michael Hooper, Acting Director
Safeguards and Security Division
US DOE/SF
Lawrence Livermore Laboratories
L-556
PO Box 808
Livermore, CA 94550

1 Gerorge G. Stefani, Jr., Director
Security and Safeguards Division
Schenectady Naval Reactors Office
US DOE
PO Box 1069
Schenectady, NY 12301

1 Donald J. Ornick, Director
Security Division
US DOE/OR
900 Commerce Road East
New Orleans, LA 70123

1 H. B. Gnann, Chief
Safeguards Engineering and Projects Branch
US DOE/SR
PO Box A
Aiken, SC 29808

1 Joan Christopher, Security Officer
Western Area Power Administration
US DOE
PO Box 3402
Golden, CO 80401

1 Larry Cameron
Allied Signal, Inc., Kansas City Division
2000 E. 95th Street
Kansas City, KS 64131-3095

1 Edward C. McGurren, Manager
Security Operations
Allied Signal, Inc., Kansas City Division
2000 E. 95th Street
Kansas City, KS 64131-3095

1 Harley Toy, Manager
Nuclear Services
Battelle Memorial Institute
505 King Avenue
Columbus, OH 43201

1 Boeing Petroleum Services
Attn: Security Department
850 South Clearview
New Orleans, LA 70123

1 John W. Jones, Manager
Safeguards and Security
EG&G Idaho
1955 Fremont
Idaho Falls, ID 83402-3126

1 Daniel Baker, Manager
Security
EG&G Mound
Bldg. 99
PO Box 3000
Miamisburg, OH 45432

1 K. N. Gardner
Technical Security
Bldg. 99
EG&G Mound
PO Box 3000
Miamisburg, OH 45432

1 Ron Mahan, Manager
Security Administration
EG&G Mound
Bldg. 99
PO Box 3000
Miamisburg, OH 45432

1 Vince Hanson, Manager
Protective Force
Bldg. 47
EG&G Mound
PO Box 3000
Miamisburg, OH 45342

1 Curtis L. Fellers
Technologies Department
Bldg. OSE-211
EG&G Mound
PO Box 3000
Miamisburg, OH 45342

DISTRIBUTION (Continued):

1 Roy E. Gmitter, Manager
Plant Security
General Electric Neutron Division
PO Box 2908
Largo, FL 34649

1 Holmes and Narver, Inc.
Attn: Electronics Department
PO Box 93838
Las Vegas, NV 89193-3838

1 Clifford A. Druit, Manager
Y-12 Safeguards and Security
Martin Marietta Energy Systems
Bldg. 9706-1, MS 8213
PO Box 2009
Oak Ridge, TN 37831-8213

1 James Hallihan
Mason and Hanger-Silas Mason, Co., Inc.
Pantex Plant
PO Box 30020
Amarillo, TX 79177

1 James Long
Protection Technologies of Idaho
785 DOE Place
Idaho Falls, ID 83402

1 Jeffrey Jay, Team Manager
Inspection and Technical Assessment Branch
Science Applications International Company
c/o DOE/Savannah River Operations Office
PO Box A
Aiken, SC 29802

1 Wackenhut Services, Inc.
800 West Commerce Rd., Suite 100
New Orleans, Louisiana 70123

1 Walk, Haydel, and Associates
600 Carondelet
New Orleans, LA 70130

1 Edward R. Saxon, Chief
Hanford Patrol
Westinghouse Hanford Company
SO-46
PO Box 1970
Richland, WA 99352

1 E. L. Goldman
Westinghouse Idaho Nuclear Company, Inc.
PO Box 4000
Idaho Falls, ID 83403

1 Ronald D. Klingler, Manager
Safeguards and Security
Westinghouser Idaho Nuclear Co., Inc.
MS 5102
PO Box 4000
Idaho Falls, ID 83403

1 Larry Schenk, Manager
Technical Security
Westinghouse Idaho Nuclear Company, Inc.
PO Box 4000
MS 5102
Idaho Falls, ID 83403

1 James M. Miller, Manager
Safeguards and Security
Westinghouse Materials Company of Ohio
PO Box 398704
Cincinnati, OH 45239

1 W. W. Arra
Westinghouse Savannah River Co., WSRS
703-57A, Rm. 7
PO Box 616
Aiken, SC 29802

1 M. Brinton
Westinghouse Savannah River Co., WSRS
703-45A, Rm. 110
PO Box 616
Aiken, SC 29802

1 C. J. O. Cox
Westinghouse Savannah River Co., WSRS
703-45A, Rm. 150
PO Box 616
Aiken, SC 29802

1 J. W. Maloney, Manager
Safeguards and Security
Westinghouse Savannah River Co., WSRS
PO Box 616
Aiken, SC 29802

DISTRIBUTION (Concluded):

1 S. C. Nashatker
Westinghouse Savannah River Co., WSRS
703-45A, Rm. 151
PO Box 616
Aiken, SC 29802

1 W. W. Rajczar
Westinghouse Savannah River Co., WSRS
703-42A, Rm. 115
PO Box 616
Aiken, SC 29802

1 John M. Samuels, Managers
Safeguards and Security Department
Westinghouse Savannah River Co., WSRS
PO Box 616
Aiken, SC 29802

1	3430	R. P. Kelly
1	3431	J. A. Kaiser
1	3432	D. E. Kerome
1	3433	R. M. Workhoven
1	3437	R. G. Baca
1	5200	J. Jacobs
1	5210	C. C. Hartwigsen
1	5211	S. H. Scott
1	5219	R. W. Moya
1	5220	J. W. Kane
1	5230	H. M. Witek
1	5231	D. J. Gangel
1	5233	D. C. Hanson
1	5234	J. C. Mitchell
1	5238	R. F. Davis
1	5240	D. S. Miyoshi
10	5240A	M. W. Green
1	5245	I. G. Waddoups
20	5245	J. P. Holmes
1	5245	L. S. Wright
1	5248	R. P. Syler
5	5248	R. L. Maxwell
1	5249	B. J. Steele
1	5260	J. R. Kelsey
1	5268	S. J. Weissman
1	8530	M. A. Pound
1	8531	D. R. Charlesworth
1	8536	C. L. Knapp
1	8523	R. C. Christman
5	3141	S. A. Landenberger
8	3145	Document Processing For DOE/OSTI
3	3151	G. C. Claycomb

3rd Party PoE Adapter Use: F-Series & G-Series

This document stands to act as a procedural guide for when using a 3rd party PoE adapter with the HandReaders, both F-Series & G-Series[1]. Schlage has performed testing to confirm that when using a PoE adapter[2], the HandReader will operate normally; so long as the minimum power requirements are met. Please use the following instructions as a guideline for initial set up of the Wi-Fi adapter.

Setup Summary of the PoE Injector and PoE Splitter (One-on-One)

Host --> Switch --> PoE Injector --> PoE Splitter --> HandReader

1. Connect from a host PC to a network switch via an Ethernet cable
2. Connect another Ethernet cable from the network switch to "LAN IN" on the PoE Injector
3. Connect between "Power/Data Out" of PoE Injector and "Power/Data In" of PoE Splitter by using Ethernet cable
    a. It is important to note the distance between the PoE Injector and PoE Splitter. PoE supported distances may vary depending on the manufacturer[3].
        i. Power degradation could occur if lengths are exceeded, which could have undesirable effects in the performance of the HandReader.
4. Connect power cable to the PoE Injector
5. Connect "LAN OUT" from PoE Splitter to HandReader Ethernet port
6. Connect "DC OUT" from PoE Splitter to HandReader power port
    a. It is important to ensure that the outputting power is at least 12V at 1A.
    b. It is important to ensure that the power (barrel) connector is compatible with HandReader.
        i. Power degradation could occur when inadequate power is outputted from the splitter, which could have

[1] F-Series models include: all HandPunch & HandKey models that have Ethernet enables. G-Series includes the GT-400.
[2] PoE Device Detail: Model Name & Number; TP-LINK PoE Adapter Kit: TL-POE200
[3] The TL-POE 200 maximum transfer length is 100 meters (330 ft)

Technical Note

Product	GT-400
Date	May 23, 2014
Subject	Lithium Battery Replacement

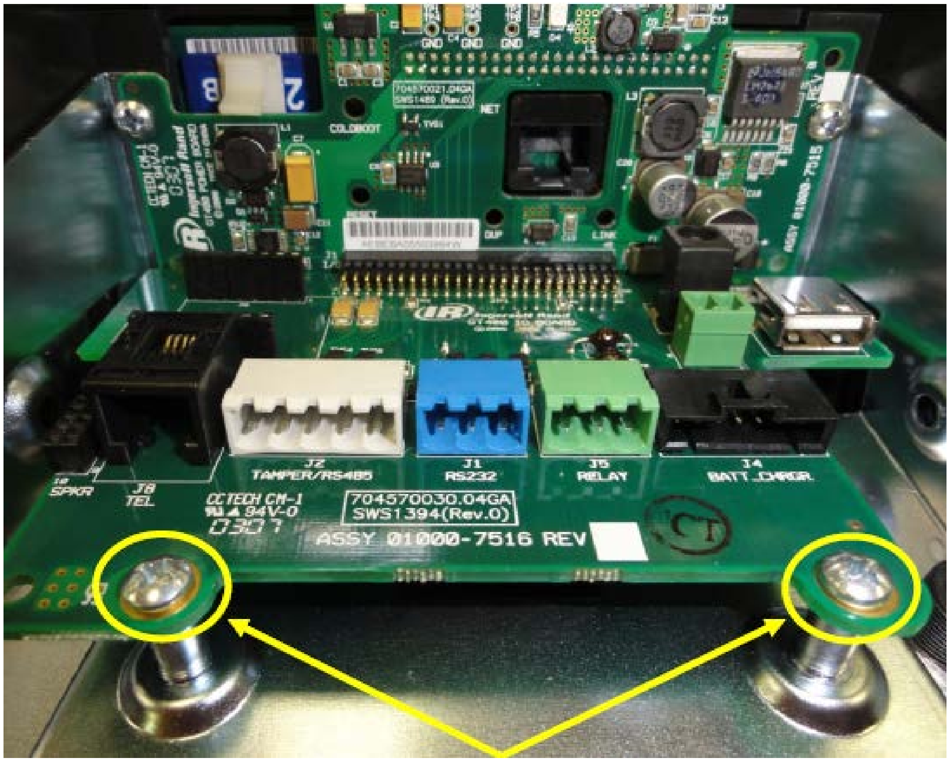
Graphic Guide to the Replacement of the Lithium Battery in the GT-400

Tools needed

- ESD Grounding Strap worn at all times
- Antistatic mat clear of debris to protect the terminal from scratches
- #2 Philips Screwdriver for the disassembly of theGT-400
- Small flat Jeweler’s type screwdriver
- Torque screwdriver must be used for the reassembly of the GT-400 set to **10.0 in-lbs**

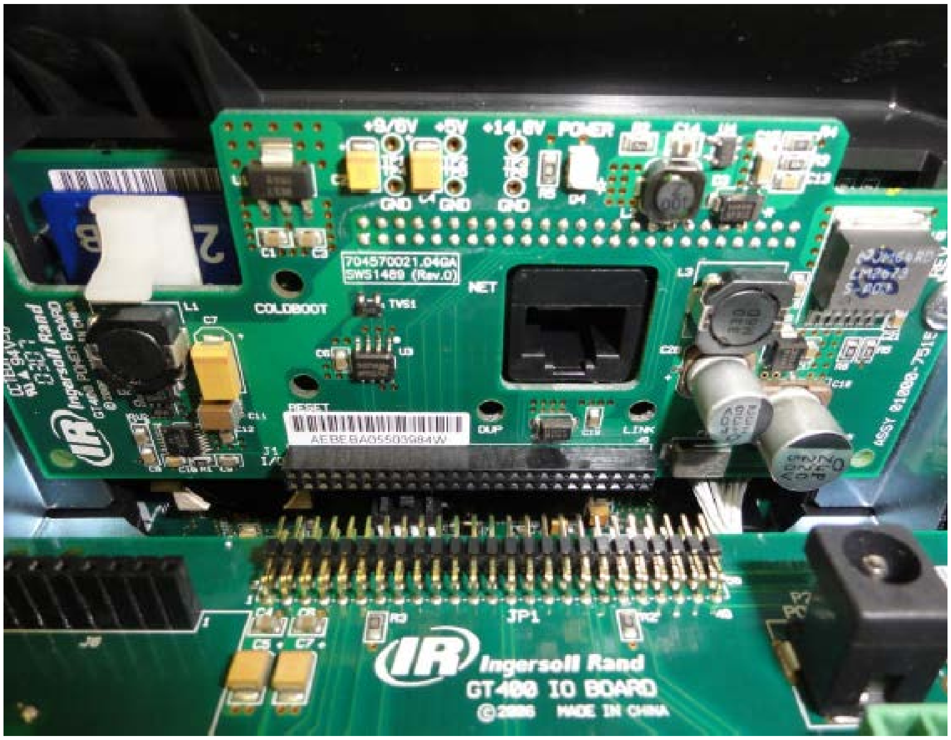
Removal of the back plate

Lay the GT-400 terminal face down of a clean antistatic mat to protect the surface from scratches and thePCBs from ESD damage. Remove the two screws highlighted and set aside for reuse.



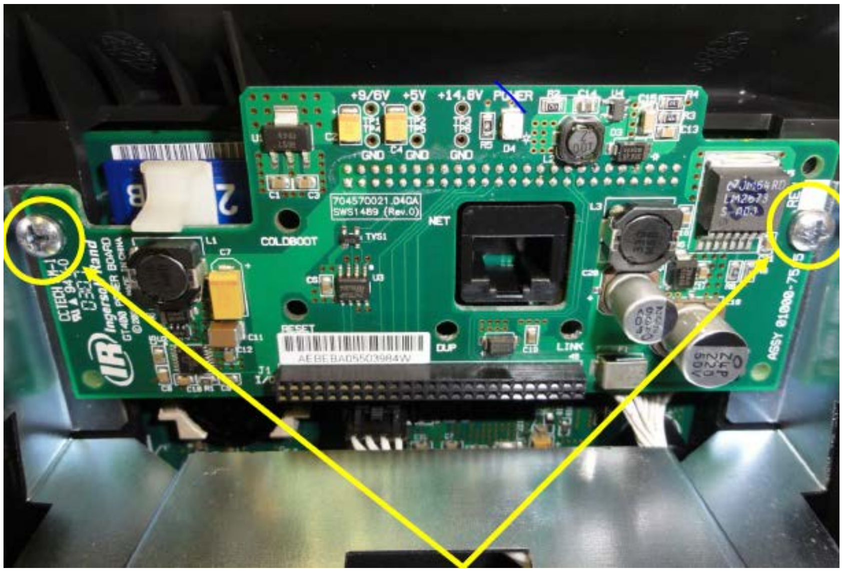
Removal of the IO board

With the terminal still lying face down and while wearing the ESD ground strap hold the IO board by the edges and gently pull the board towards you and set aside.



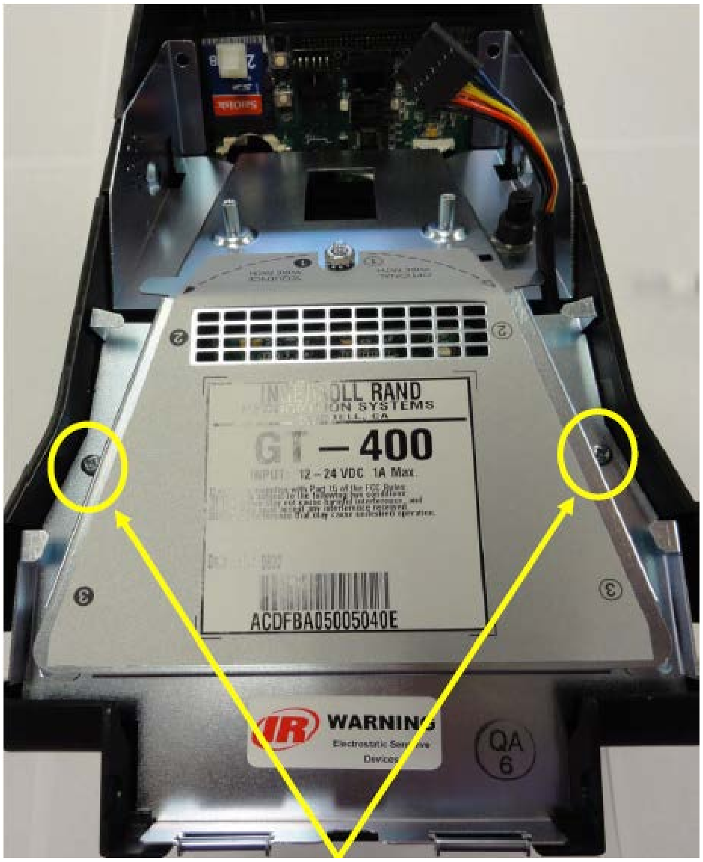
Removal of the Power board

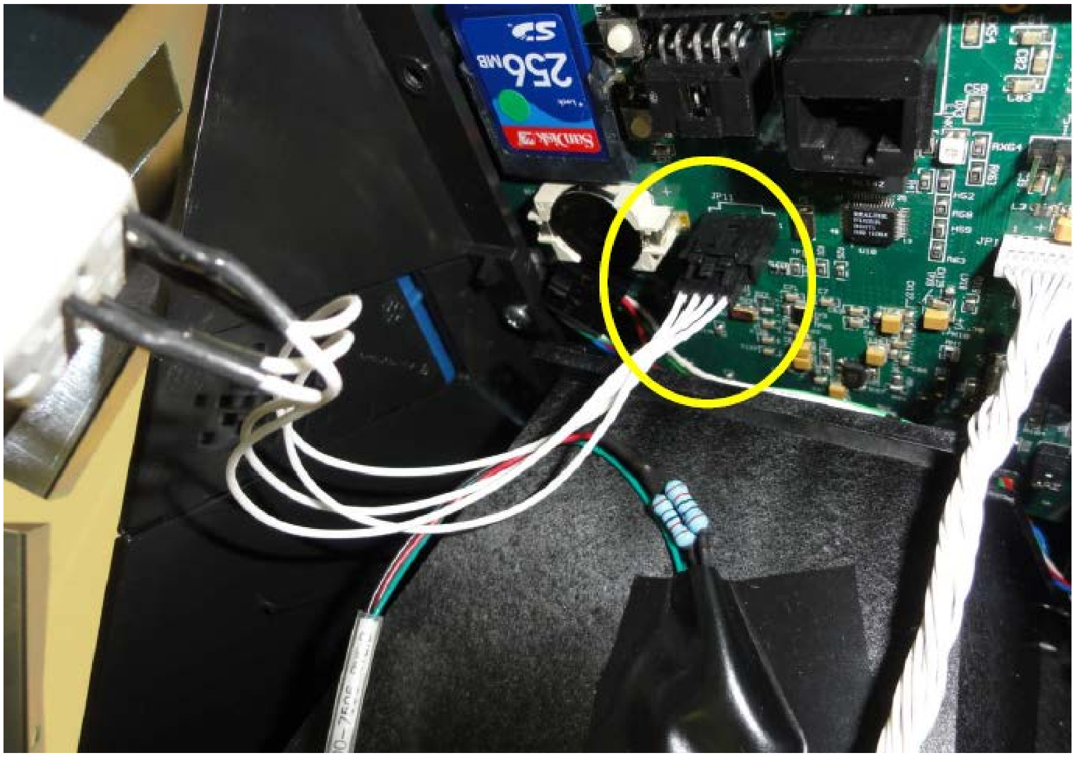
Remove the two screws highlighted and set aside for reuse. Hold the power board by the edges and gently pull the board towards you and set aside.



Removal of the back plate

Remove the two screws highlighted and set aside for reuse. Rotate the top of the back plate towards you.

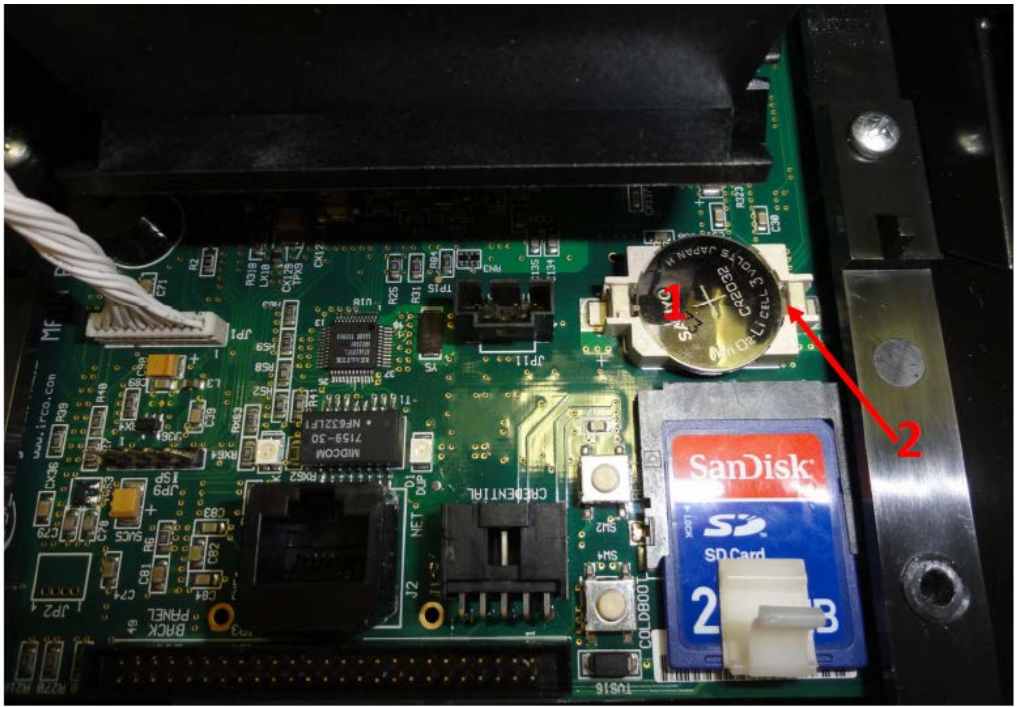




Remove the tamper switch connector from the main board. Do not pull by the wires but depress the tab to release the connector.

Removal of the lithium battery

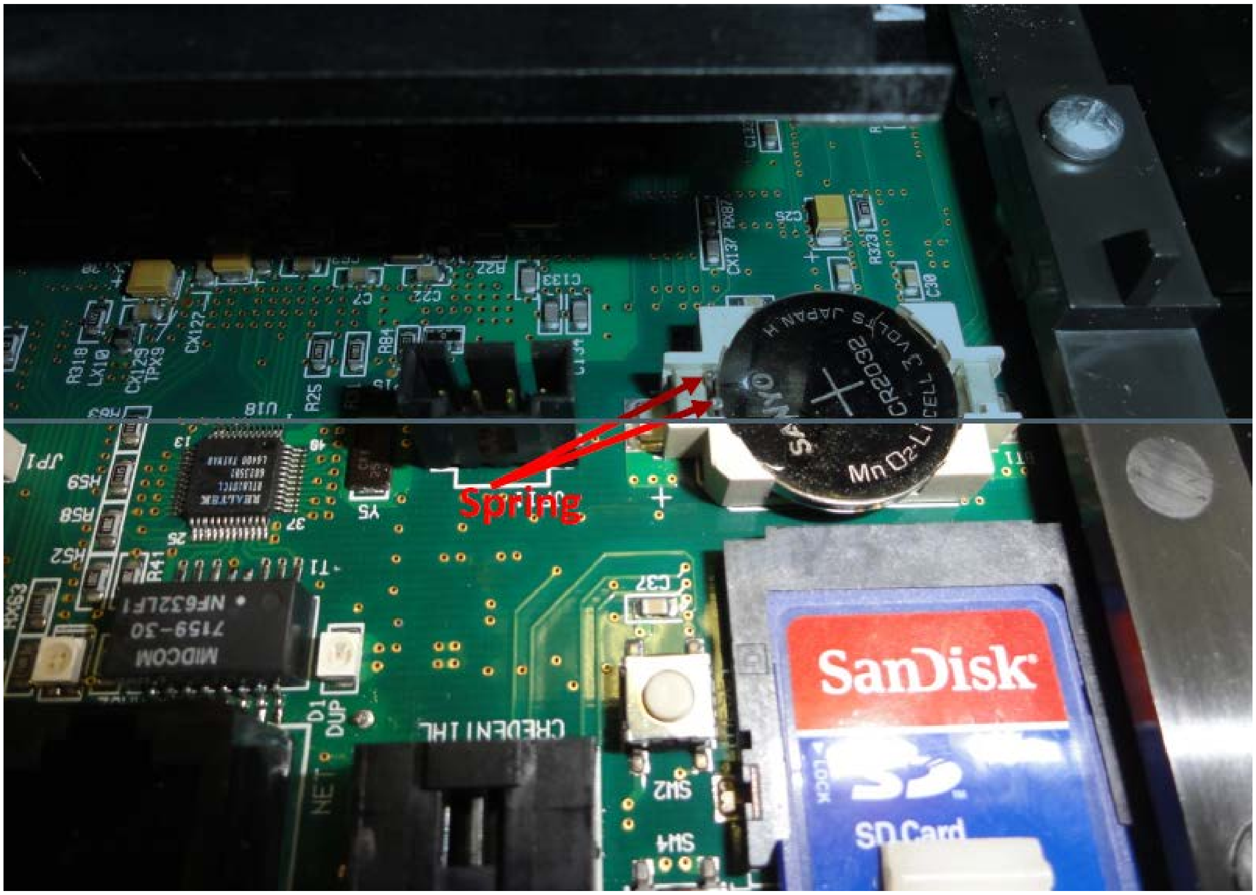
Carefully place the terminal on its top panel so that you are looking at the main board. The lithium battery is located above the SD Card.



1. Place a finger on top of the lithium battery so that it will not pop out and fall forward, into the top panel, when the battery is released. If that happens, the reader will need to be taken completely apart to retrieve the battery.

2. Take a small jeweler's size flat screwdriver and **gently release** the battery up on the right hand side of the battery holder.

Installation of the lithium battery

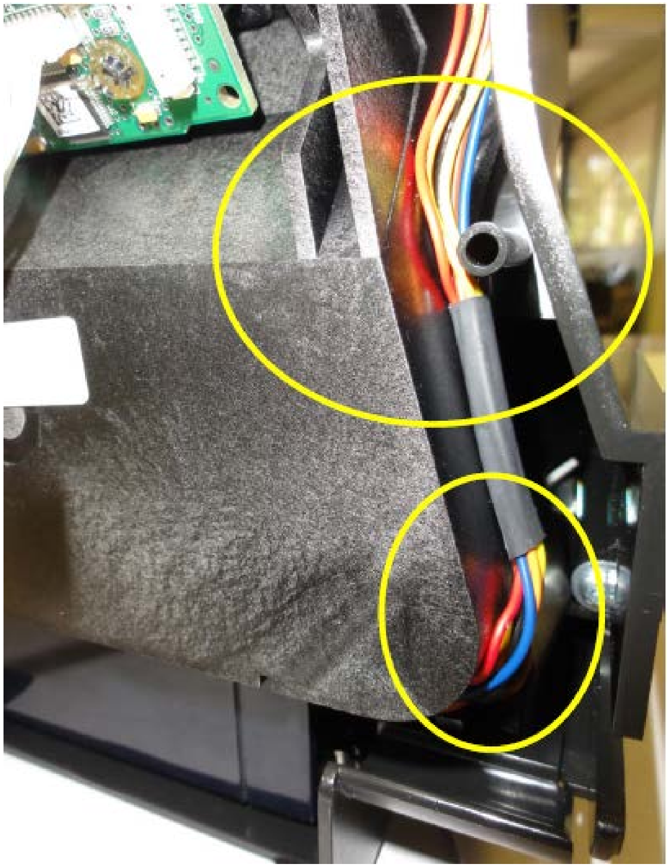


There are two types of battery holder that may be installed on the main board; one with visible spring keeps and one without. The installation of the battery is the same either way.

Place the left side of the battery into the battery holder first and snap the battery into place.

Technical Note

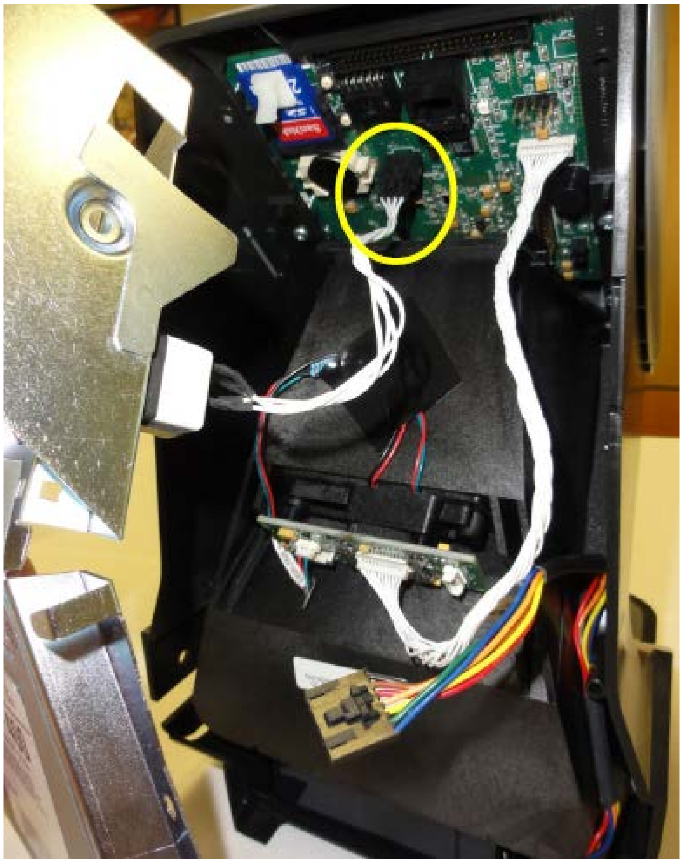
Routing the battery cable if there is a backup battery installed



Make sure that the battery cable is routed around the camera compartment as shown in the image above. The area highlighted in yellow needs special attention when installing the back plate, the wires here can be easily pinched.

Connecting the tamper switch

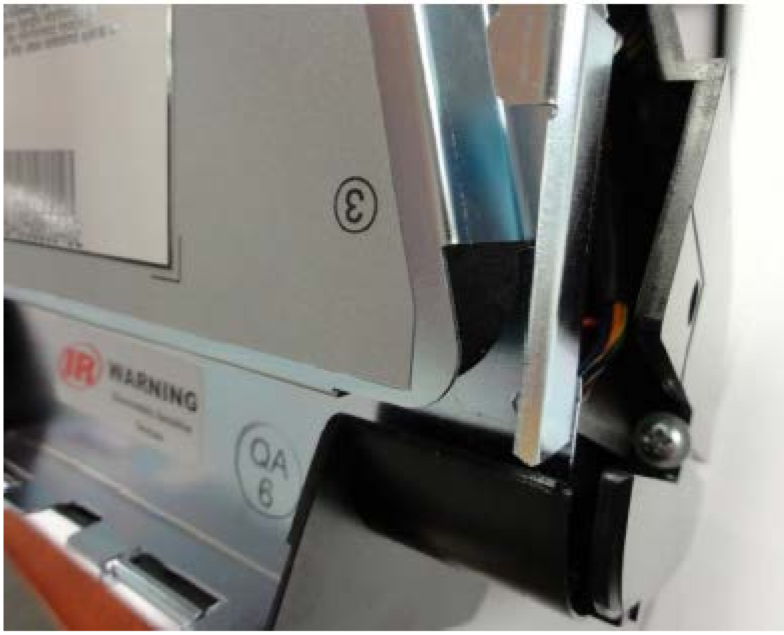
Reconnect the tamper switch cable.



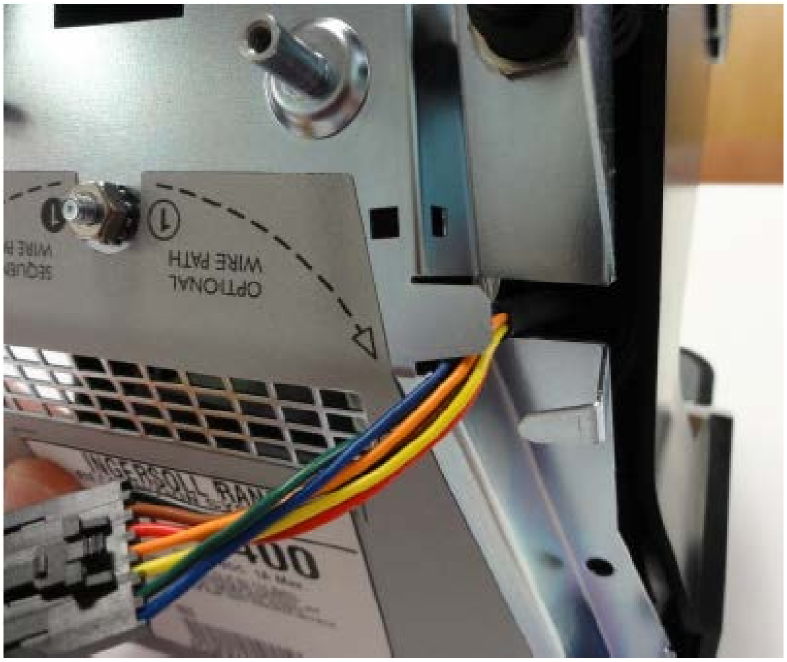
Technical Note

Reinstalling the back plate

Start with setting the back plate into the battery compartment and start rotating the back plate towards the top. If there is a backup battery installed, make sure that the BB-300 cable is not getting pinched in the lower right hand cable. Stop when you get to the camera cable.



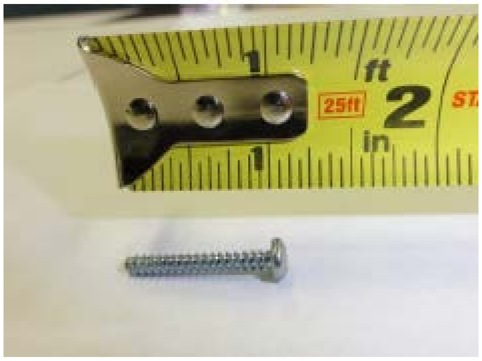
Pull the backup battery cable through the back plate as shown above.



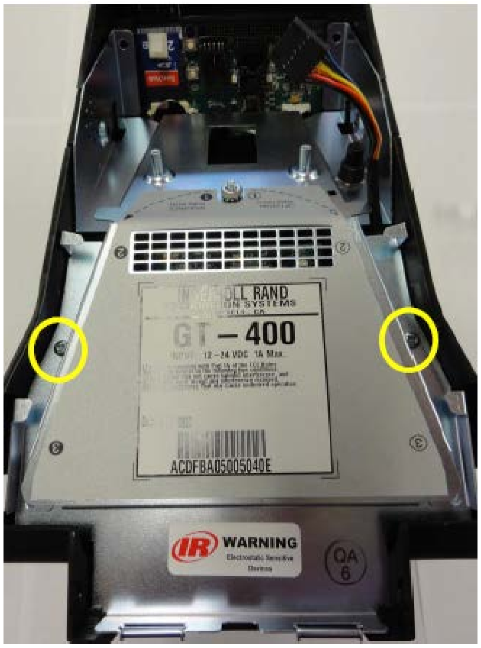
Technical Note

Installing back plate screws

*This point forward use the torque screwdriver set to **10.0 in-lbs***



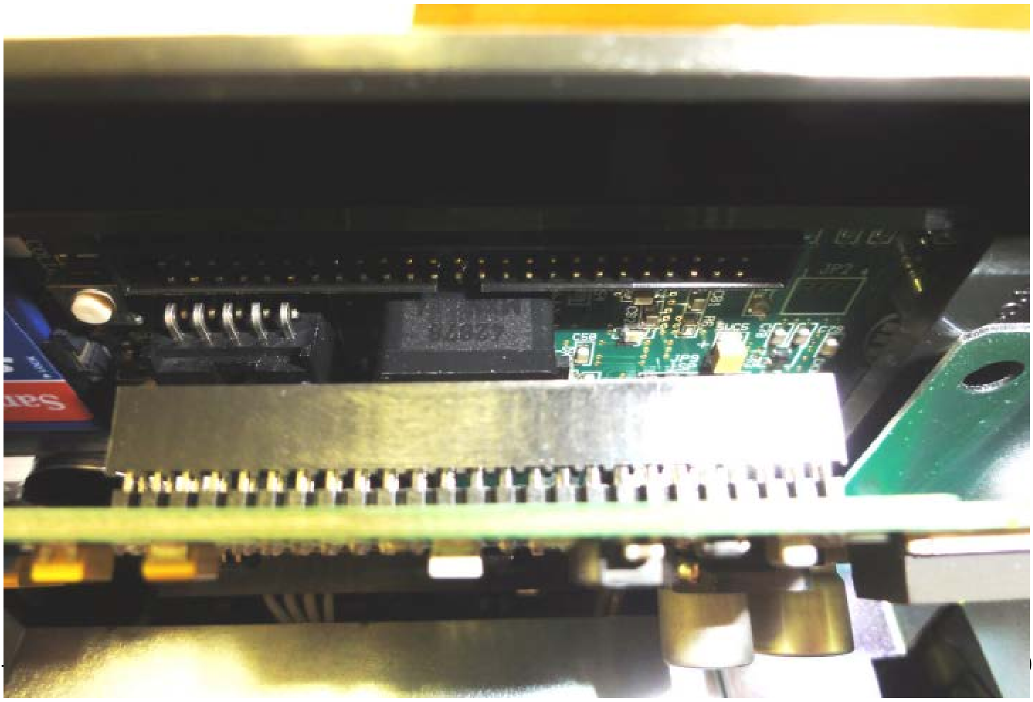
Before screwing down the back plate make sure that neither the BB-300 cable nor the white camera cable will be pinched.



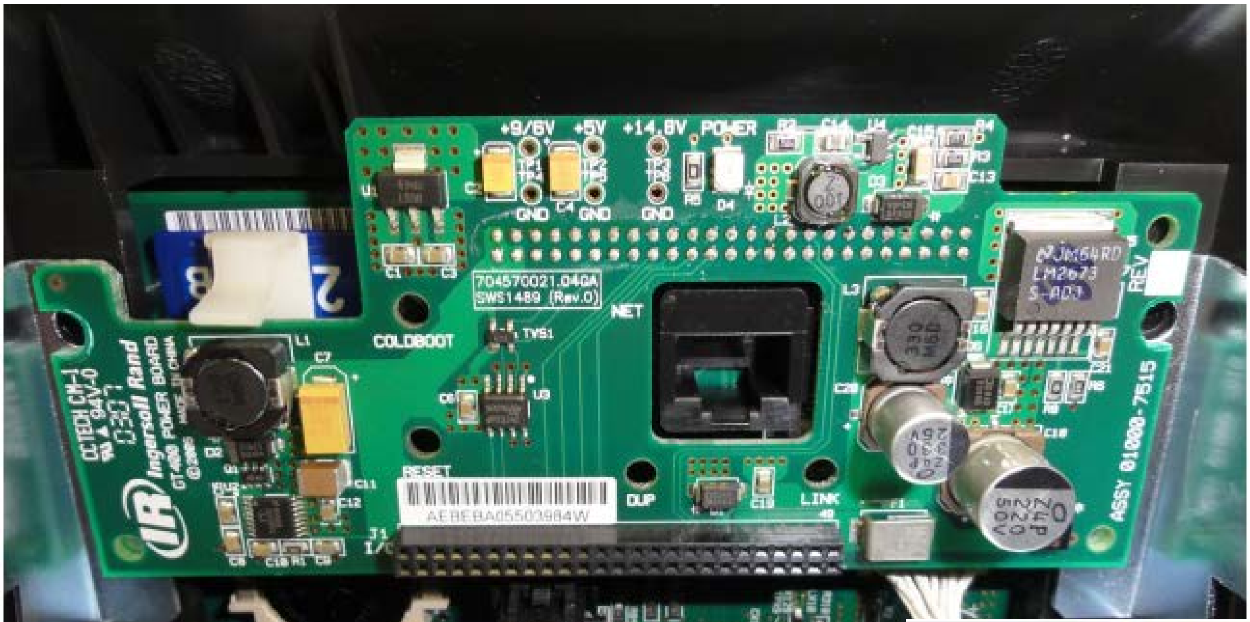
Install these screws into the two the back plate inserts. **Do not use the longer self-tapping screws used for the power board or they will break through the front of the reader.**

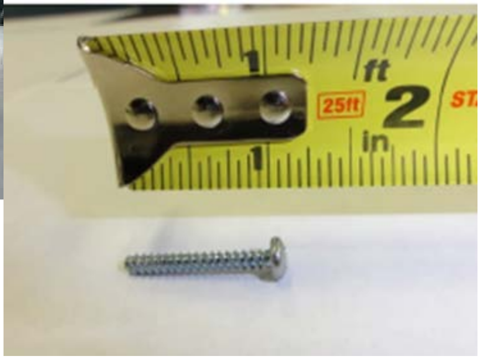
Reinstalling the power board

Making sure your ground strap is on. Align the 2 x 25 pin connector and header and gently mate the two boards.



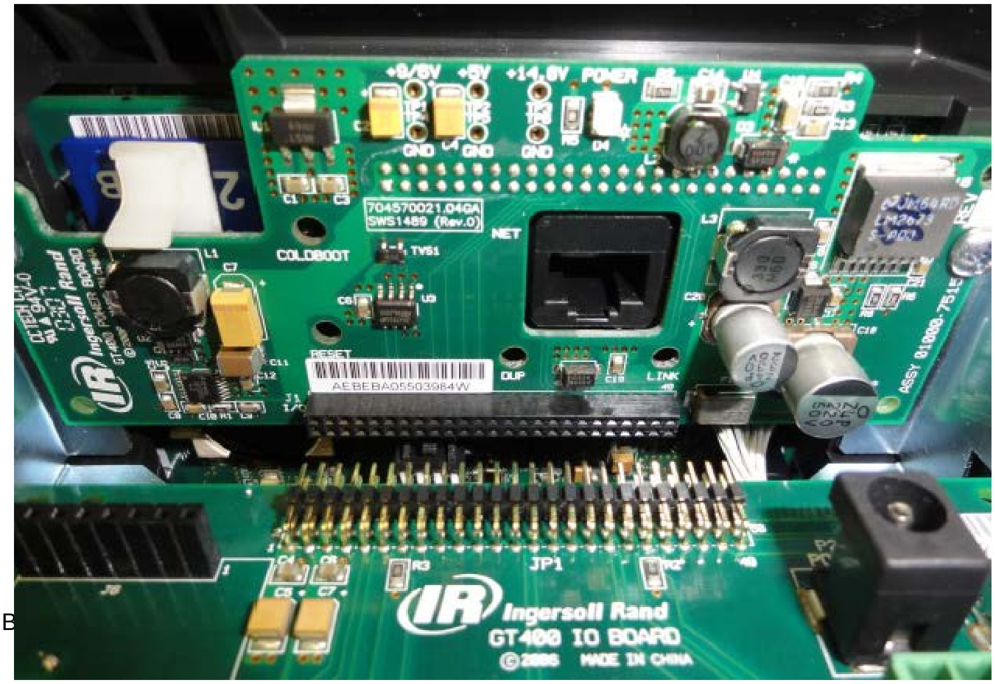
Technical Note





Secure the power board to the unit using the two screws shown in the image to the right.

Reinstalling the IO board

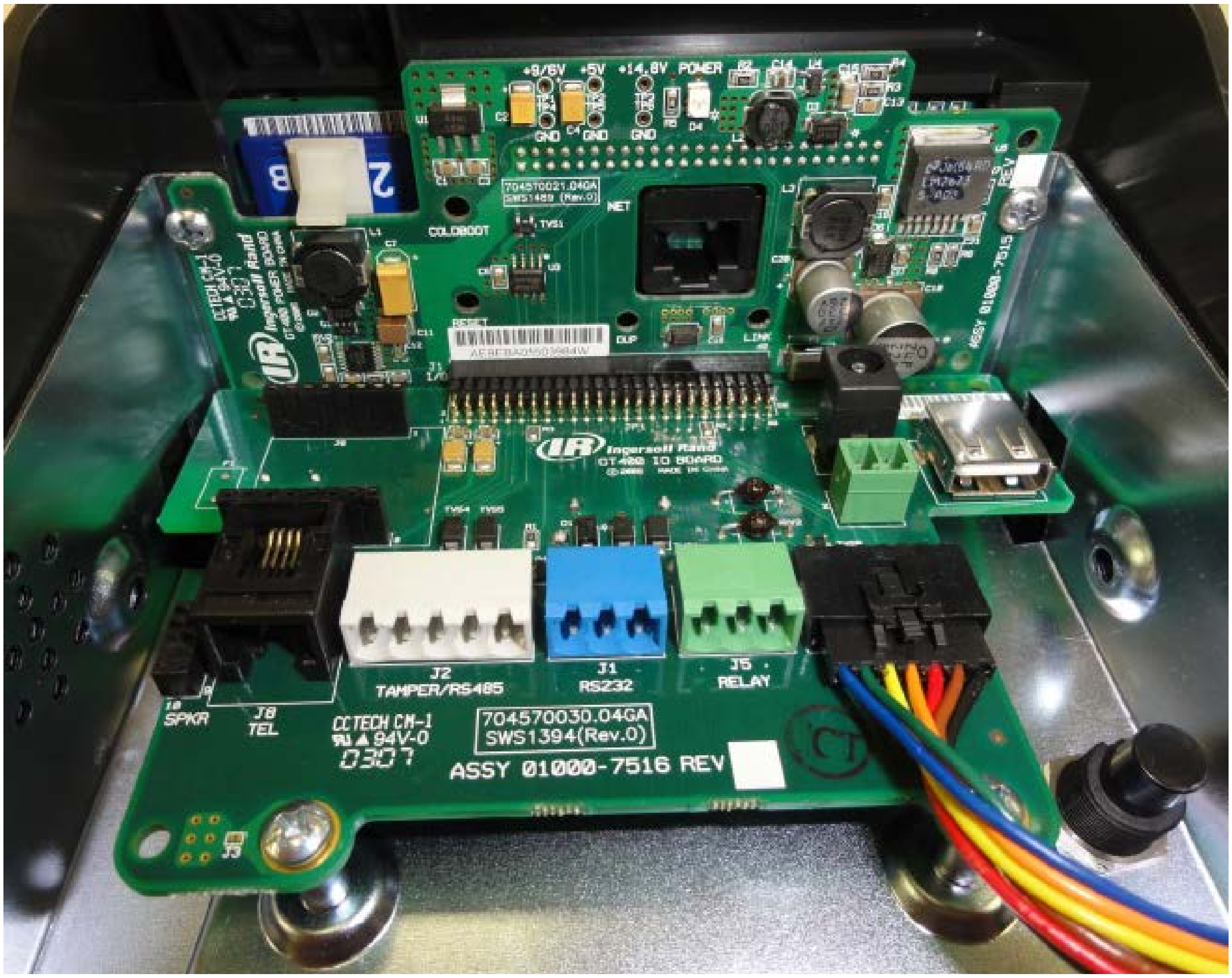


Align the IO's 2 x 25 pin header and connector and gently press them together making sure that it is installed.

Secure the IO board to the unit with the screws shown in the image above.

Technical Note

Plugging in the battery backup cable if installed



Replacement complete.

For additional information, please contact Customer Care at 877-671-7011.

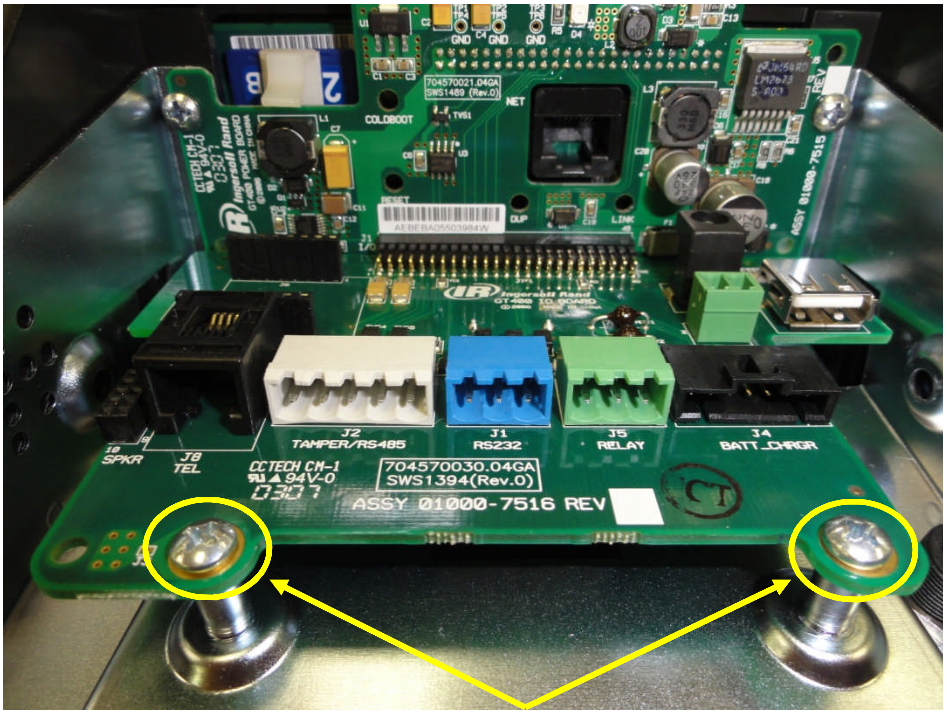
GT-400 BB-300 Installation *TECHNICAL NOTE*

Graphic guide to the installation of the BB-300 into the GT-400

Tools needed

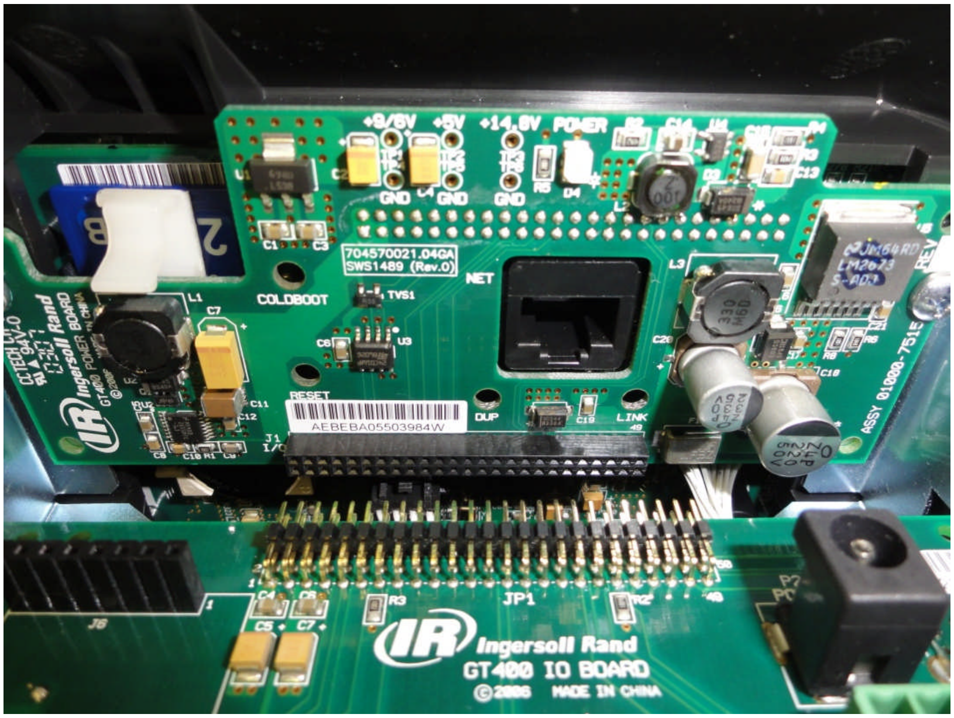
- ESD Strap
- Antistatic mat clear of debris to protect the terminal from scratches
- #2 Philips Screwdriver for the disassembly of theGT-400
- Torque screwdriver must be used for the reassembly of the GT-400 set to **10.0 in-lbs**

Removal of the back plate



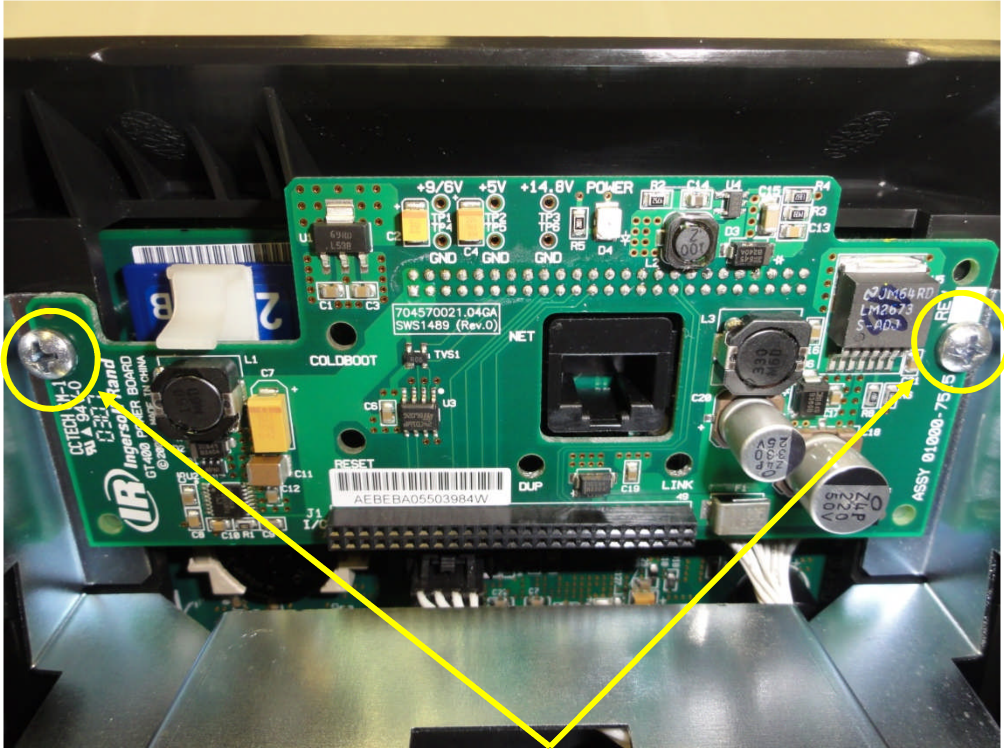
Lay the GT-400 terminal face down of a clean antistatic mat to protect the surface from scratches and the PCBs from ESD damage. Remove the two screws highlighted and set aside for reuse.

Removal of the IO board



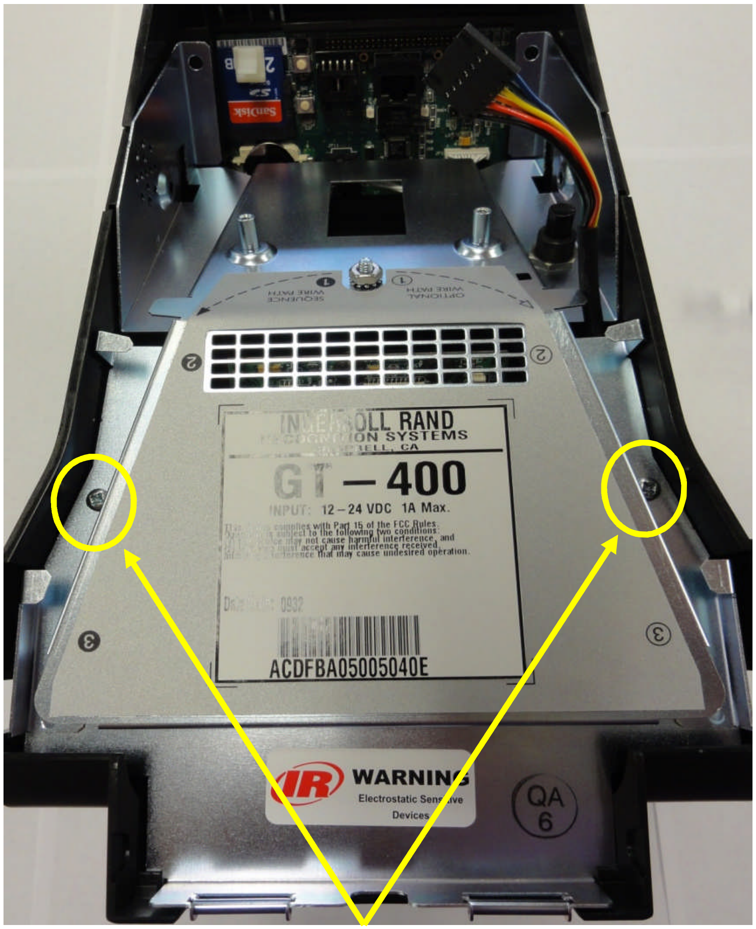
With the terminal still laying face down and while wearing the ESD ground strap hold the IO board by the edges and gently pull the board towards you and set aside.

Removal of the Power board

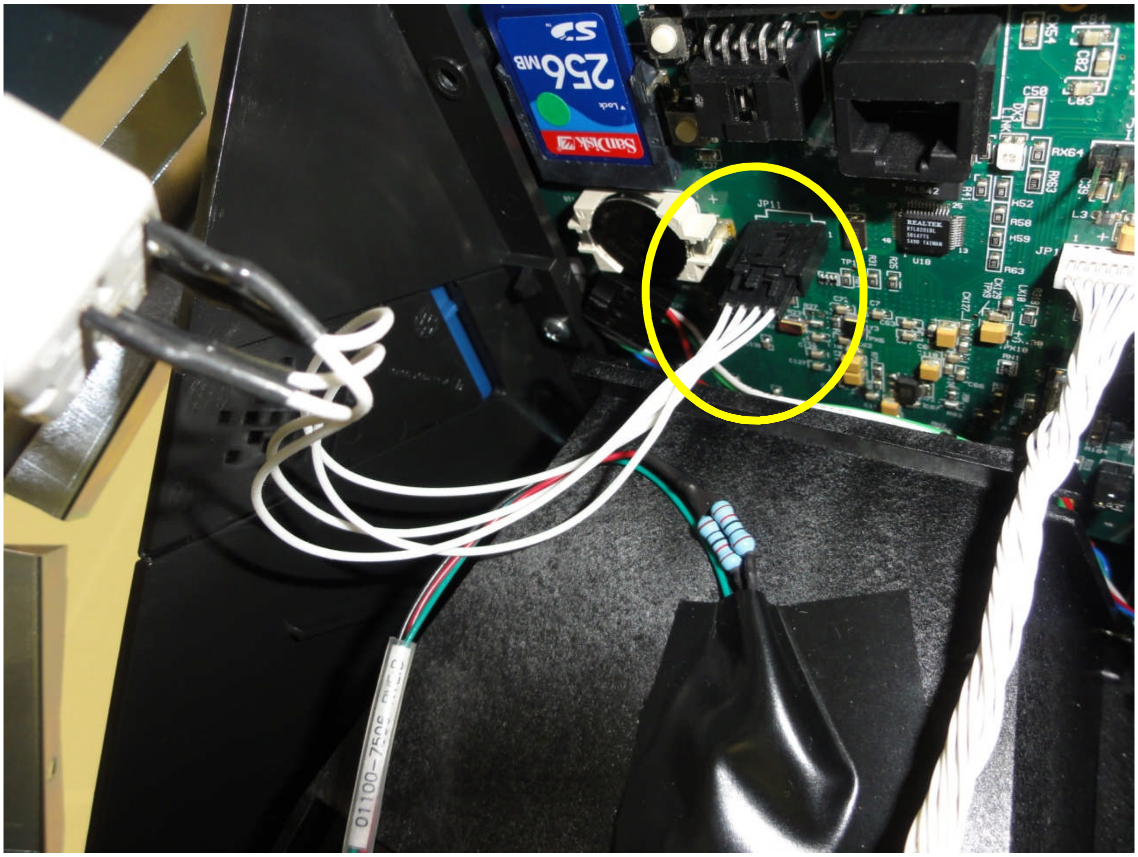


Remove the two screws highlighted and set aside for reuse. Hold the power board by the edges and gently pull the board towards you and set aside.

Removal of the back plate

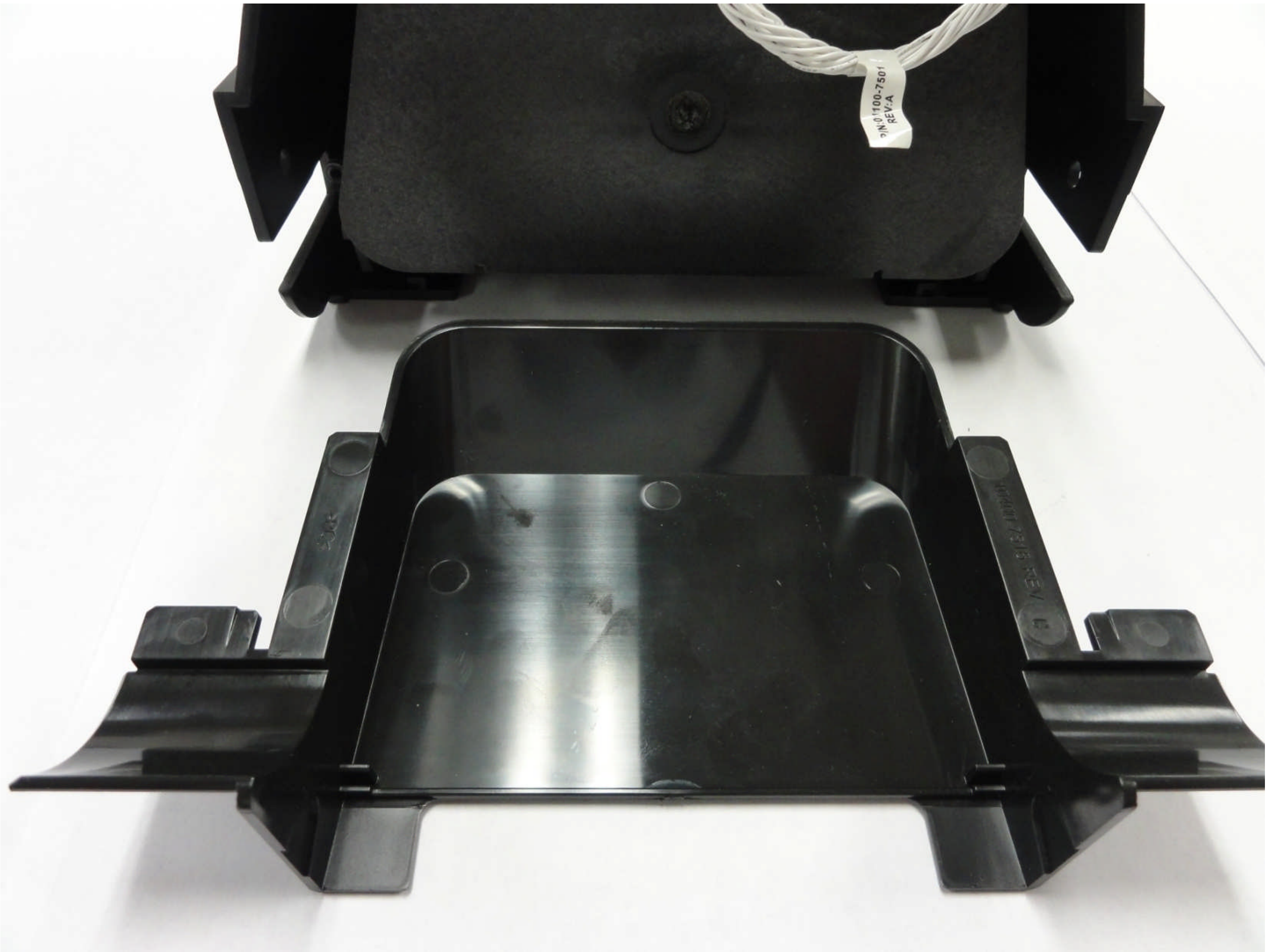


Remove the two screws highlighted and set aside for reuse. Rotate the top of the back plate towards you



Remove the tamper switch connector from the main board. Do not pull by the wires but depress the tab to release the connector.

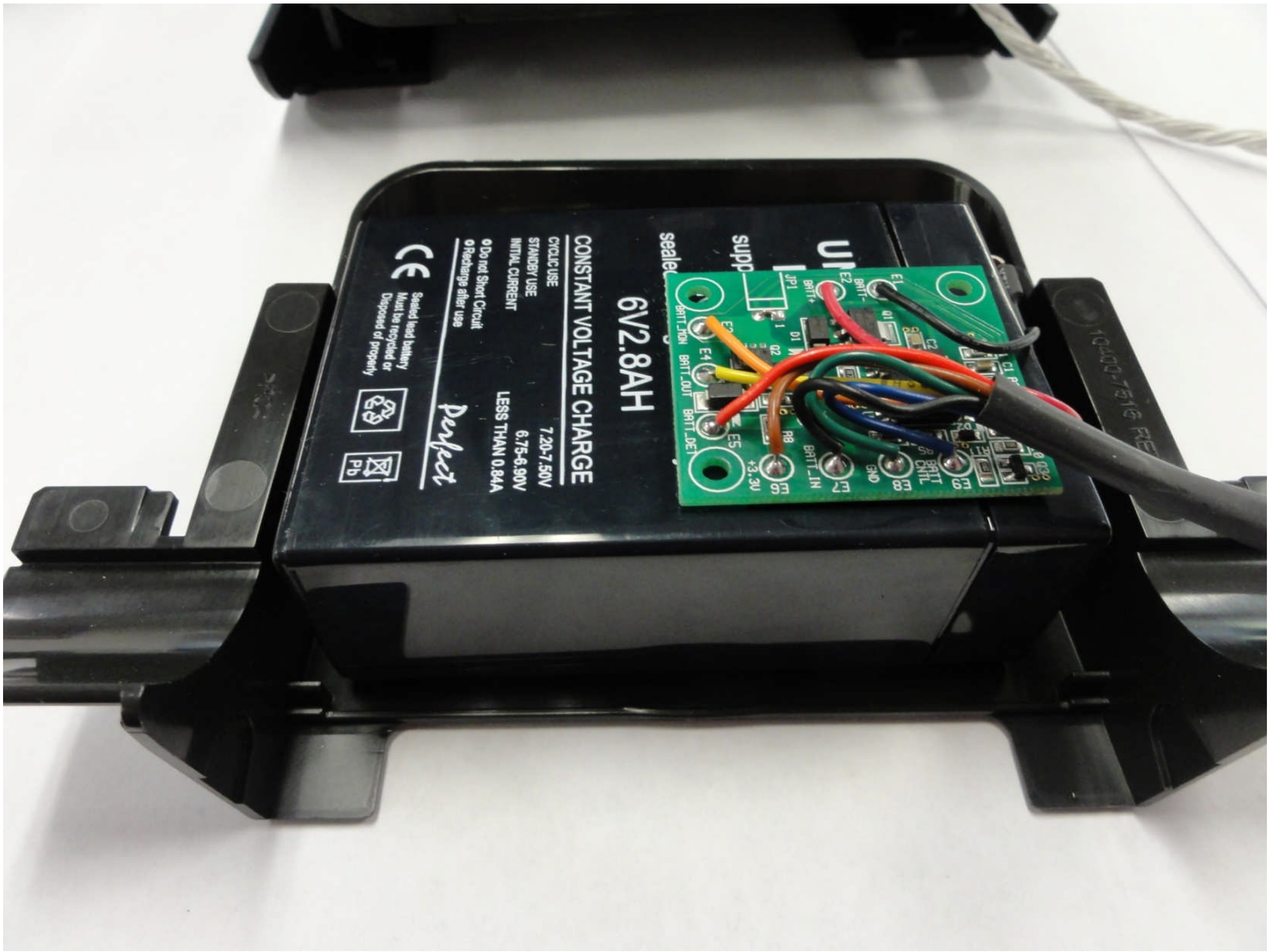
Removal of the battery compartment



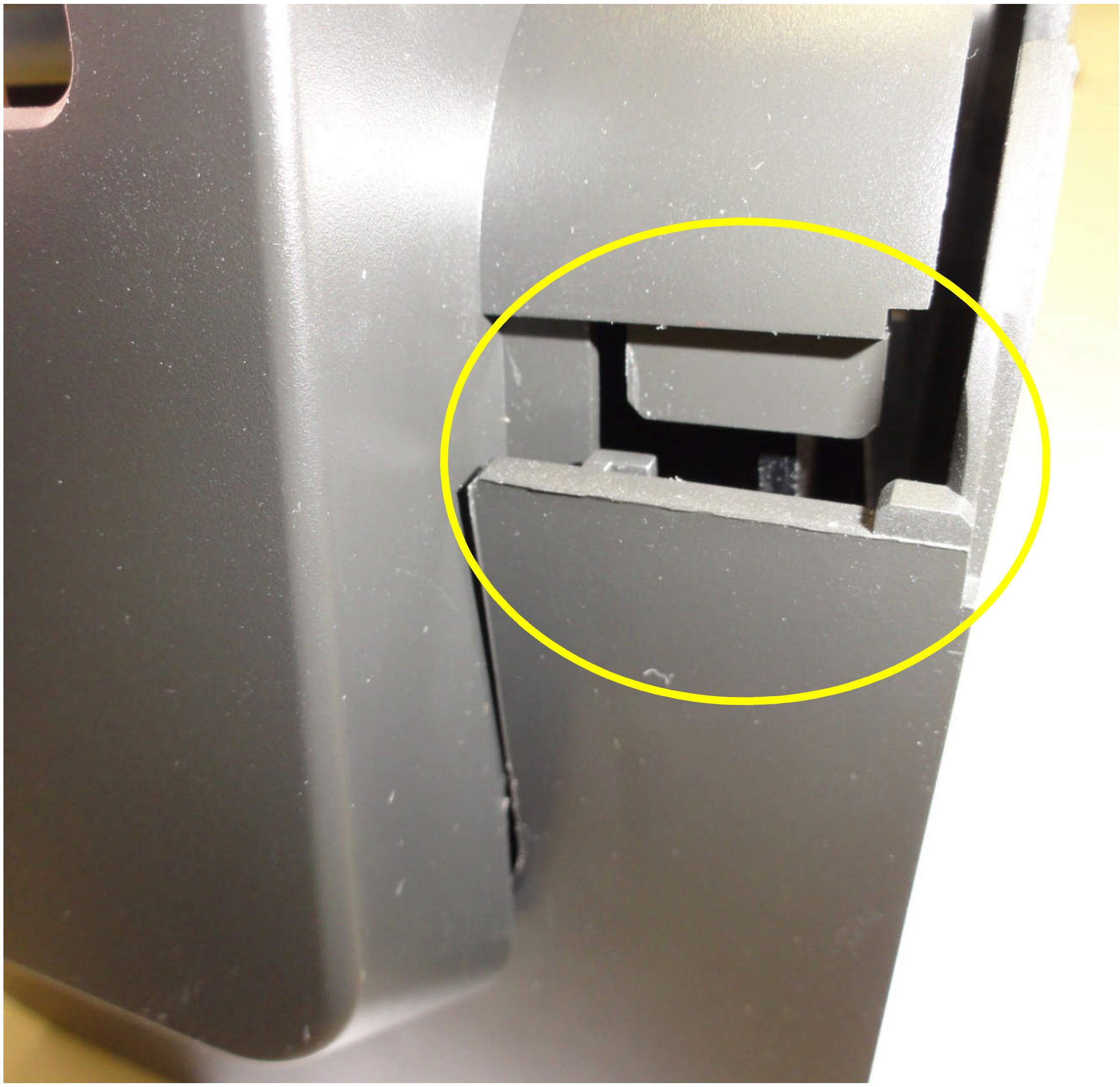
With the reader lying face down pull the battery compartment up towards you. These parts are pressure fitted so the battery compartment may need to be tapped with the heel of your hand to release the part.

Installation of the BB-300

Attach the back-up battery to the battery cover using the double sided tape. Make sure the battery is placed forward of the two slotted tabs inside the battery cover.

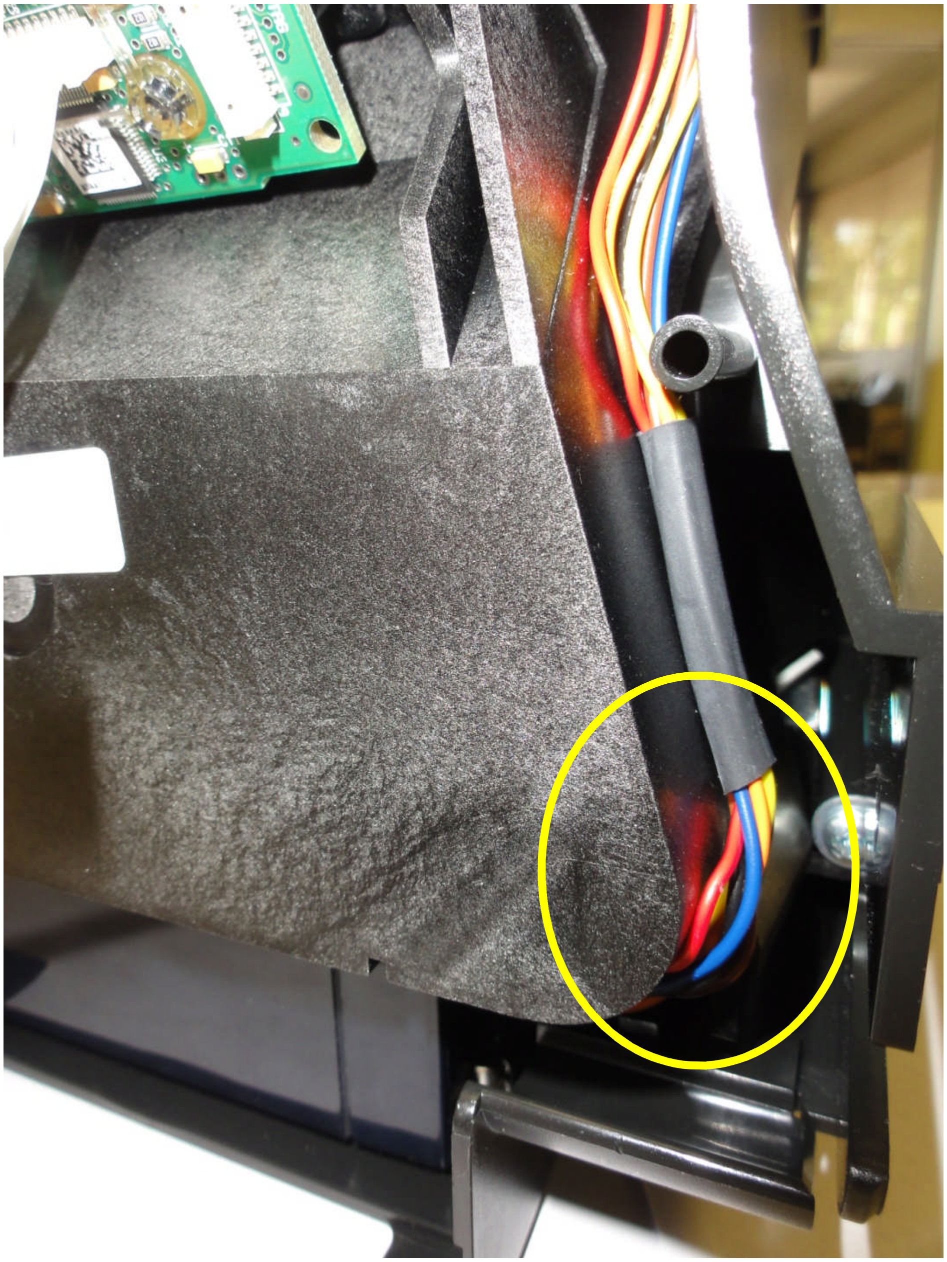


Installation of the battery compartment



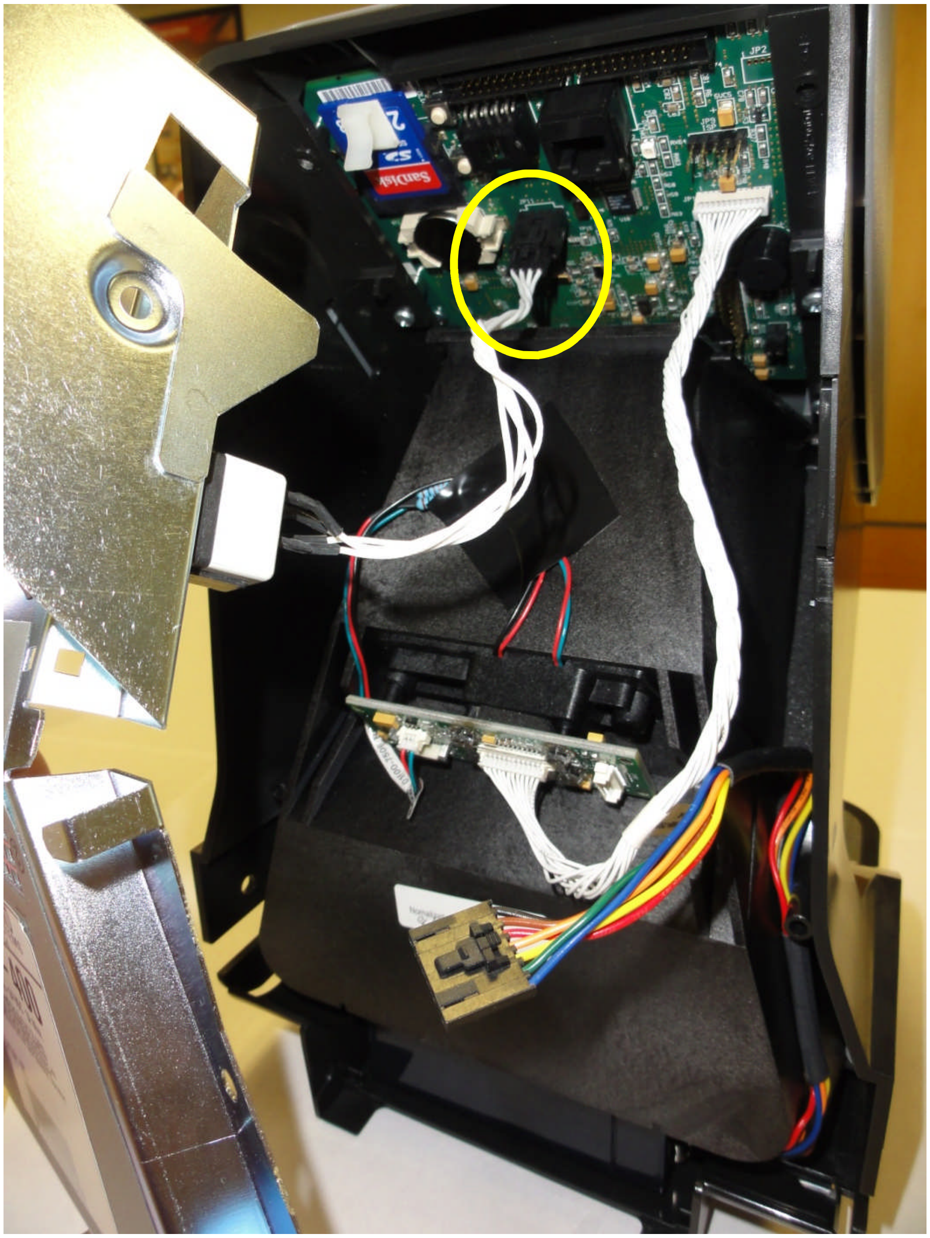
Slide the battery compartment back into the bottom of the unit slide the battery compartment so that it mates up. Press the battery compartment in so that it is flush in place.

Routing the battery cable



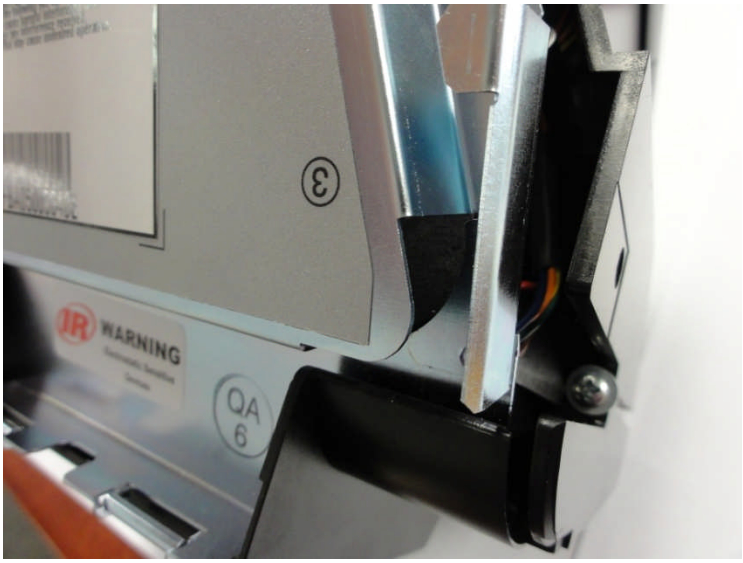
Make sure that the battery cable is routed around the camera compartment as shown in the image above. The area highlighted in yellow needs special attention when installin the back plate, the wires here can be easily pinched.

Connecting the tamper switch

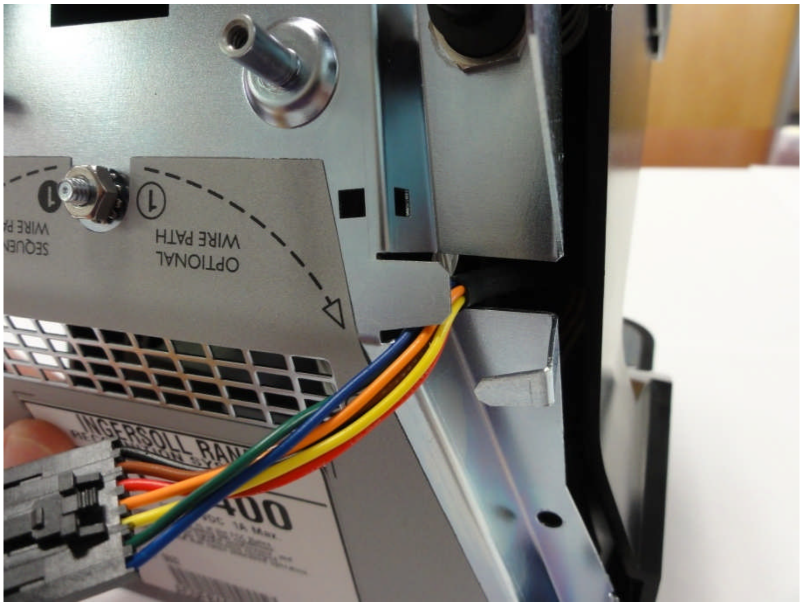


Reconnect the tamper switch cable.

Reinstalling the back plate



Start with setting the back plate into the battery compartment and start rotating the back plate towards the top. Make sure that the BB-300 cable is not getting pinched in the lower right hand cable. Stop when you get to the camera cable.

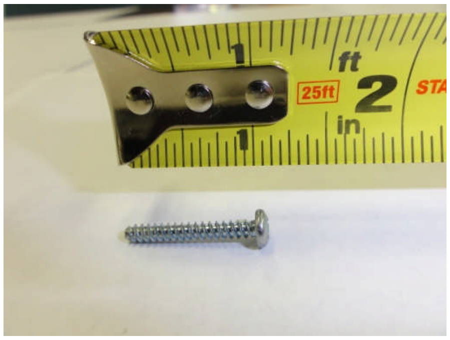


Pull the BB-300 cable through the back plate as shown above.

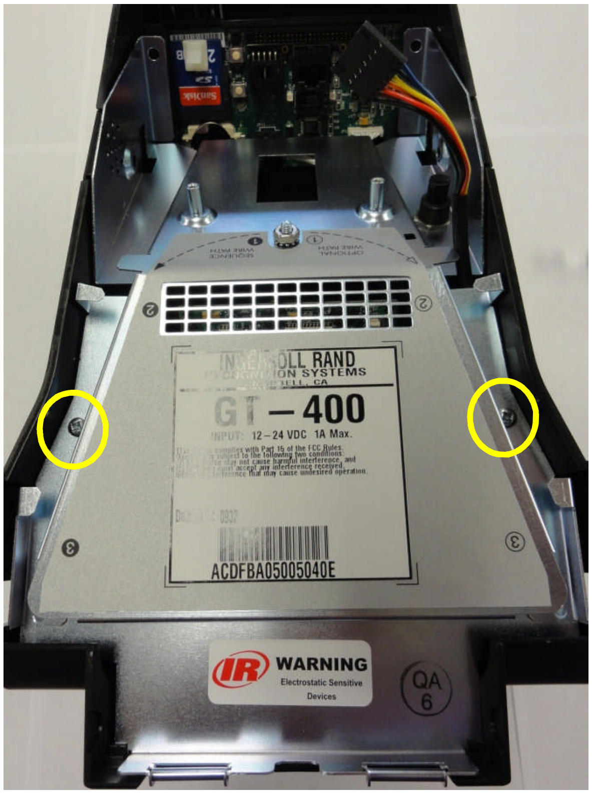
Installing back plate screws

This point forward use the torque screwdriver set to **10.0 in-lbs**

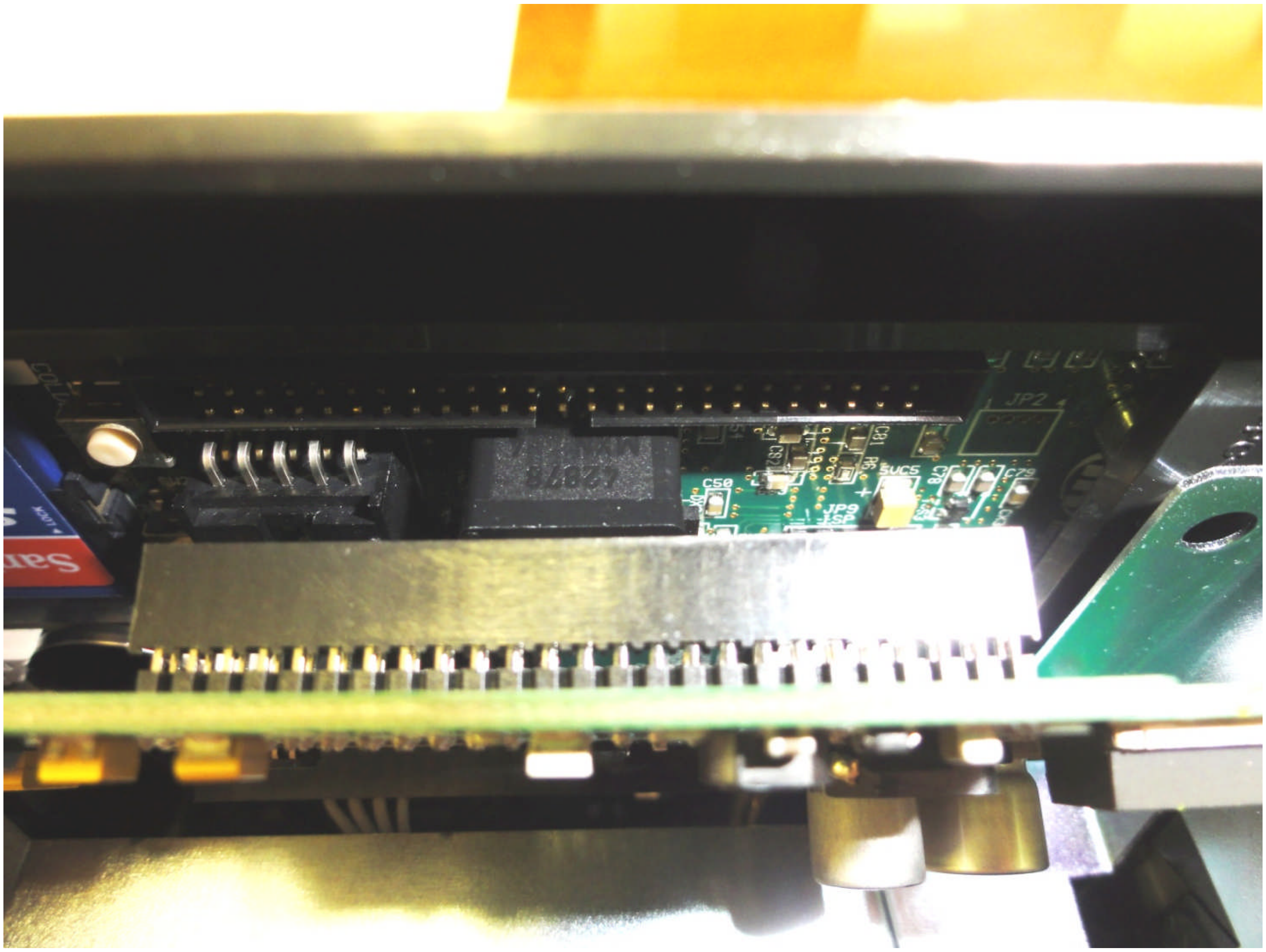
Before screwing down the back plate make sure that neither the BB-300 cable nor the white camera cable will be pinched.



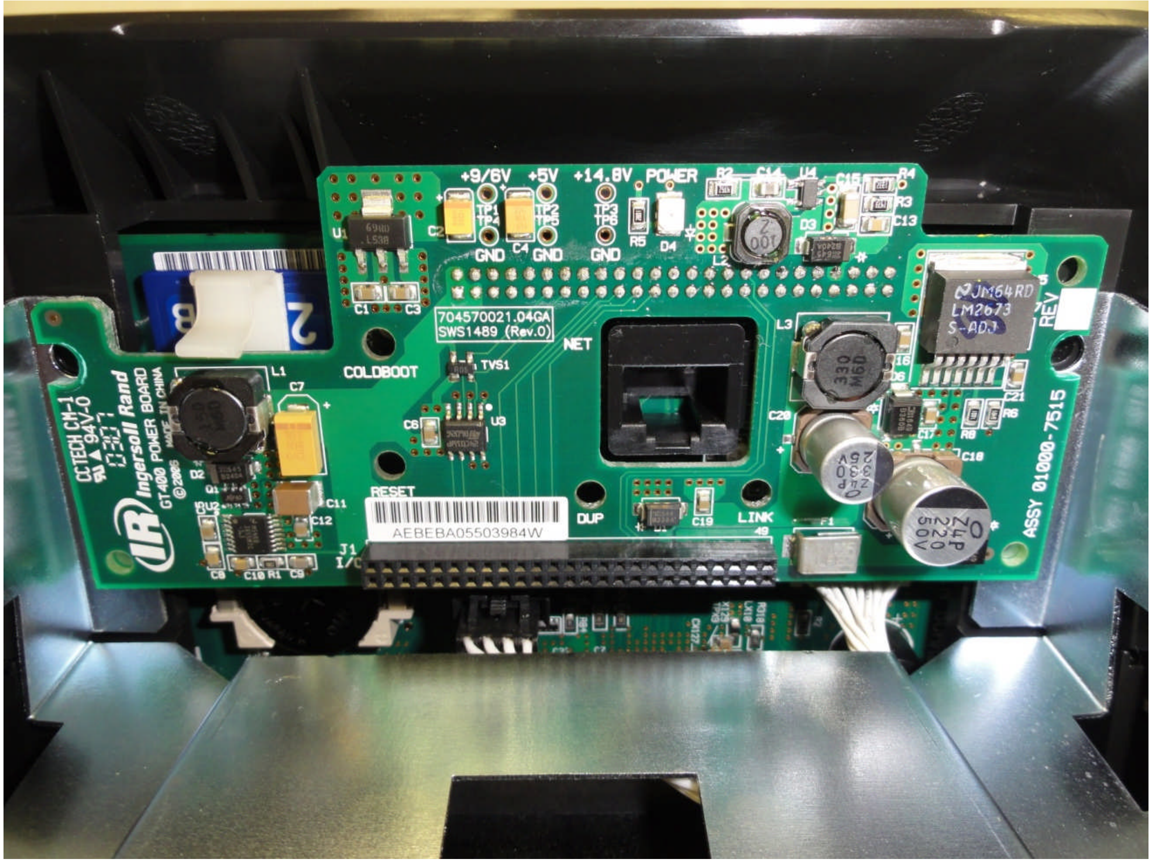
Install these screws into the two the back plate inserts. **Do not use the longer self tapping screws used for the power board or they will break through the front of the reader.**



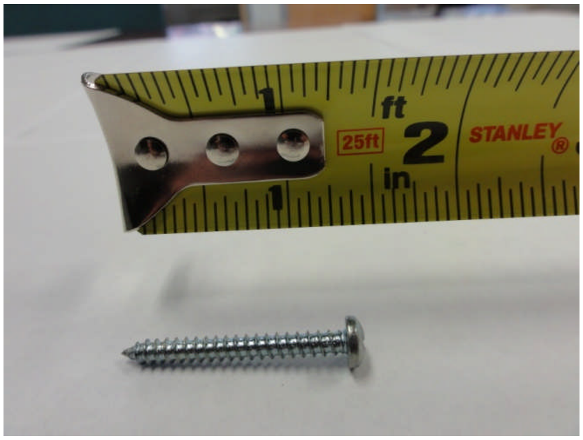
Reinstalling the power board



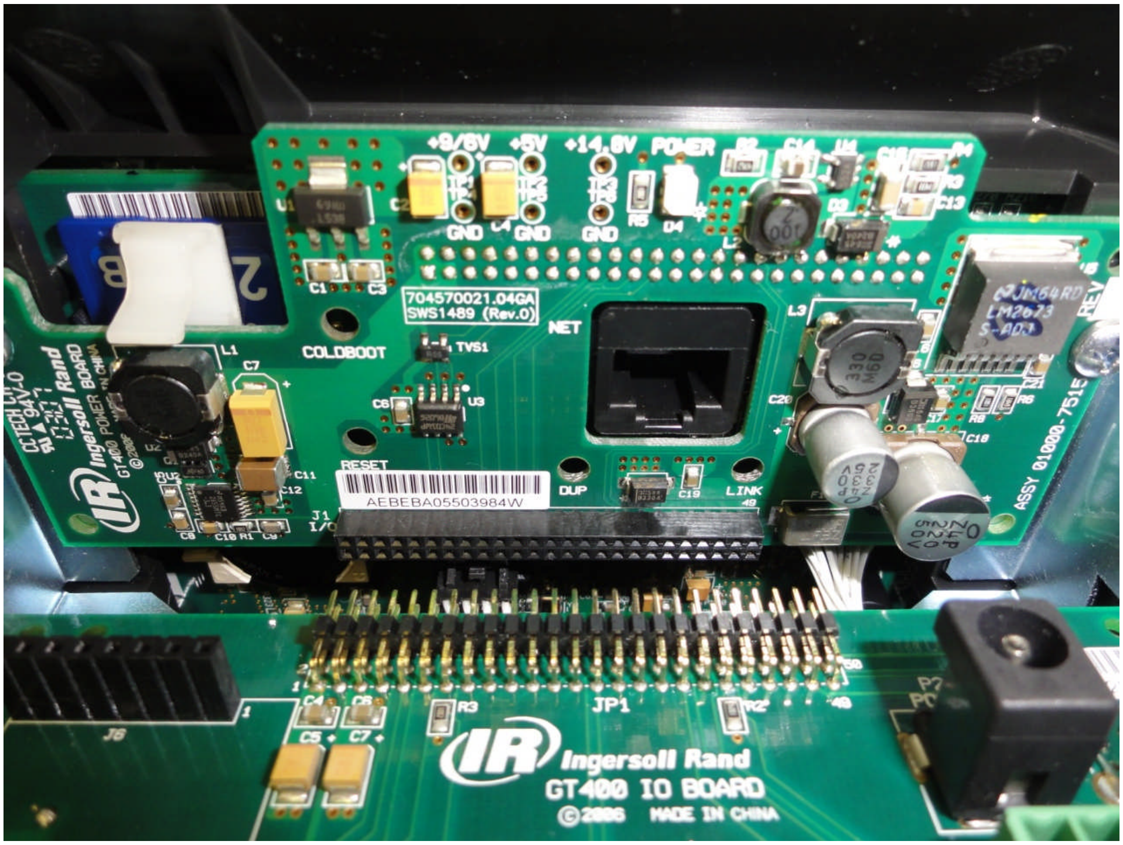
Making sure your ground strap is on. Align the 2 x 25 pin connector and header and gently mate the two boards.



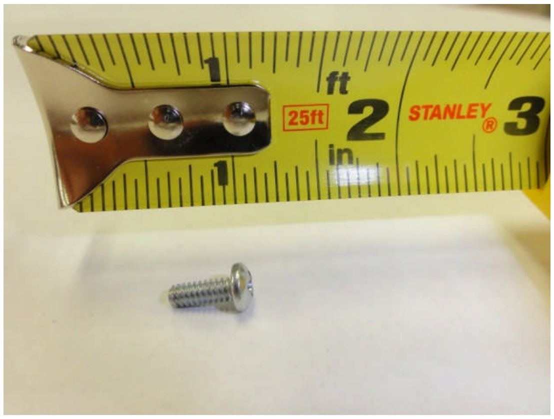
Secure the power board to the unit using the two screws shown in the image below.



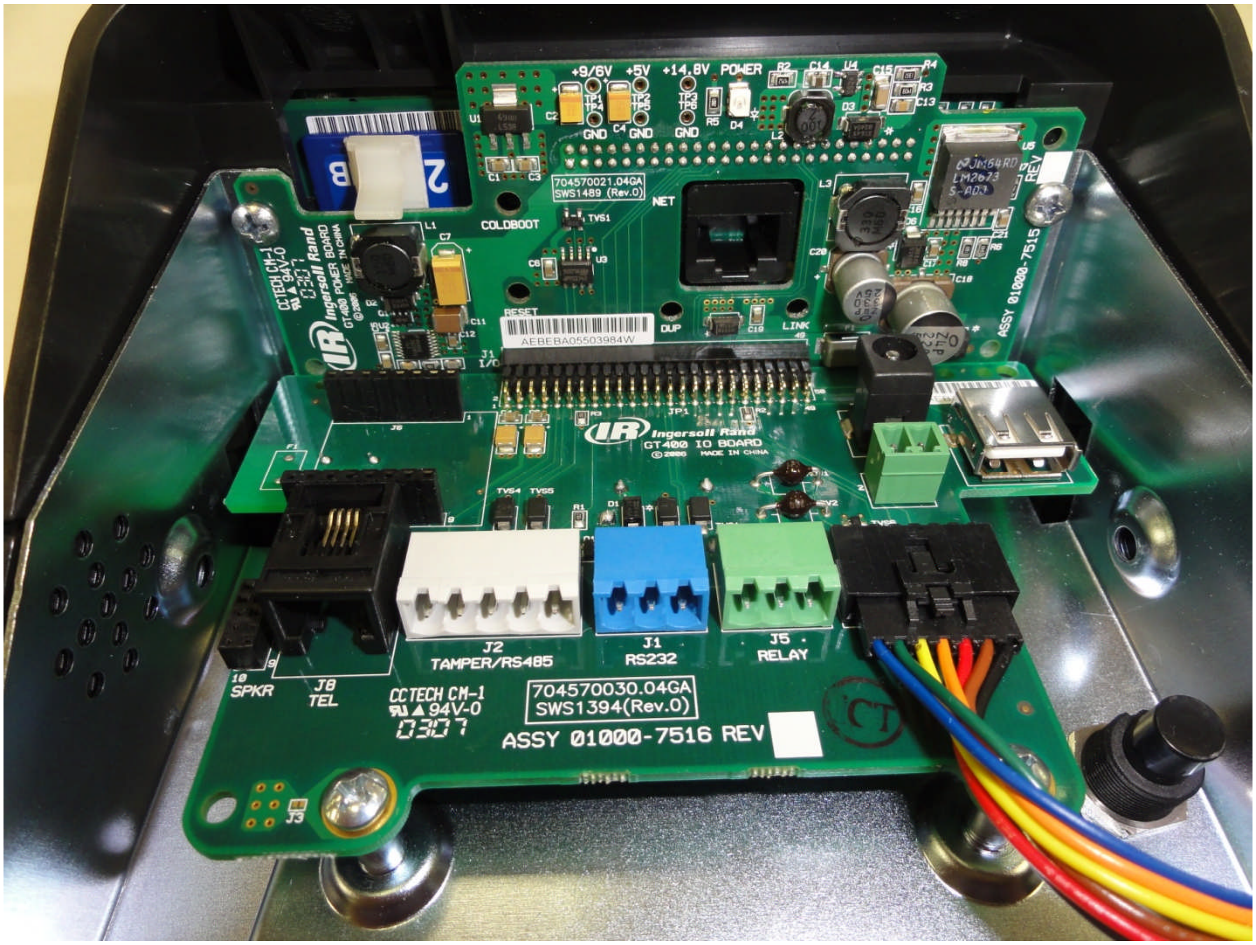
Reinstalling the IO board



Align the IO’s 2 x 25 pin header and connector and gently press them together making sure that it is installed. Secure the IO board to the unit with the screws shown in the image below.



Plugging in the battery back up



Installation complete

Technical Note

Product	GT-400
Date	May 23, 2014
Subject	SD Card Replacement

Graphic Guide to the Replacement of the SD Card in the GT-400

Tools needed

- ESD Grounding Strap worn at all times
- Antistatic mat clear of debris to protect the terminal from scratches
- #2 Philips Screwdriver for the disassembly of the GT-400
- Torque screwdriver must be used for the reassembly of the GT-400 set to 10.0 in-lbs

Technical Note

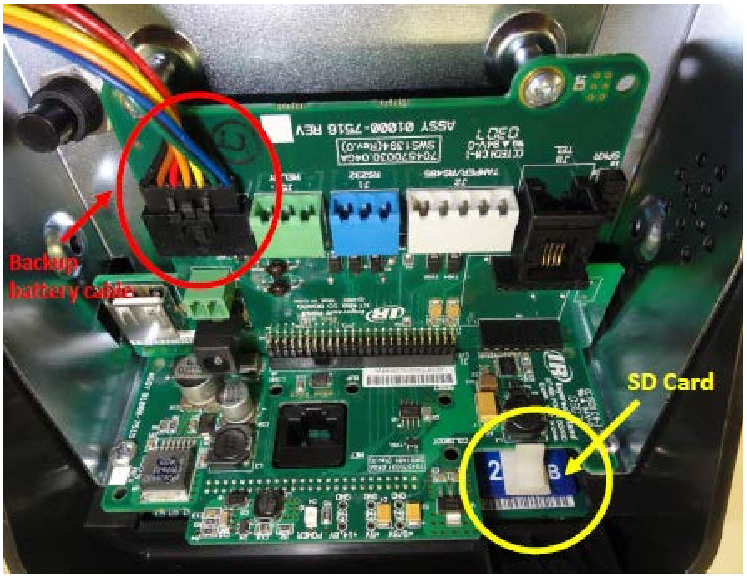
Removal of the SD Card

Gently lay the GT-400 on its top panel face down on a clean antistatic mat to protect the surface from scratches and the PCBs from ESD damage.

Warning! - If there is a BB-300 (backup battery) installed, the rainbow cable must be unplugged before the removal of the SD Card.

If the SD card that is present does not have a white TAB on it as shown in the picture above skip to page 4.

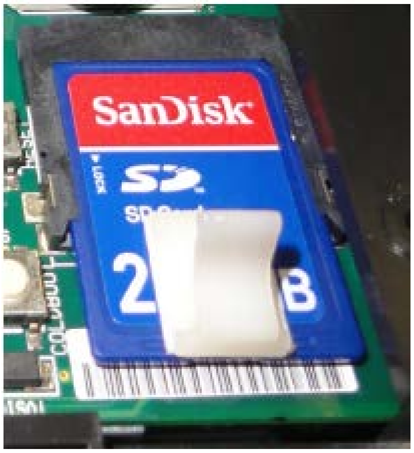
Pull white TAB on the SD card towards you and gently guide the SD card out from the slot.



Replacement of the SD Card

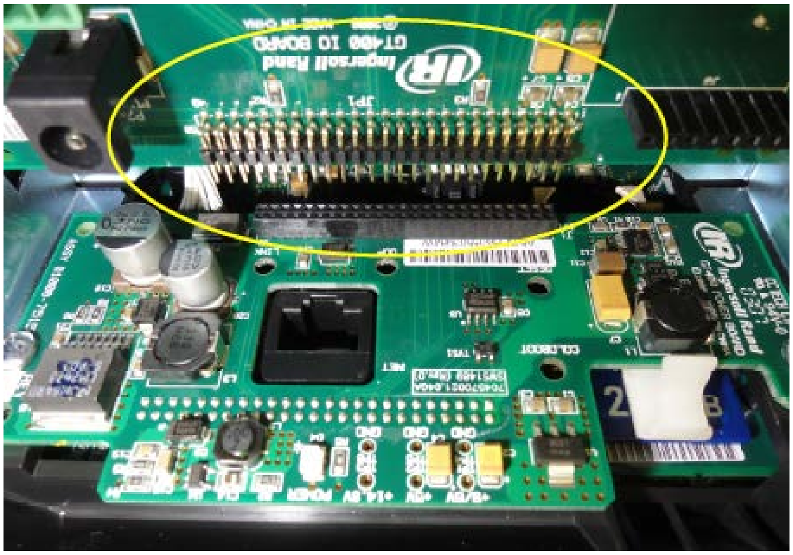
This is a picture showing how the SD card is seated into its slot under the boards. If there is a TAB on the replacement SD card there should be no issue guiding the replacement SD card properly into its slot. Once the SD card is properly seated (if applicable) plug the battery back cable back in and the replacement is complete.

Replacement complete

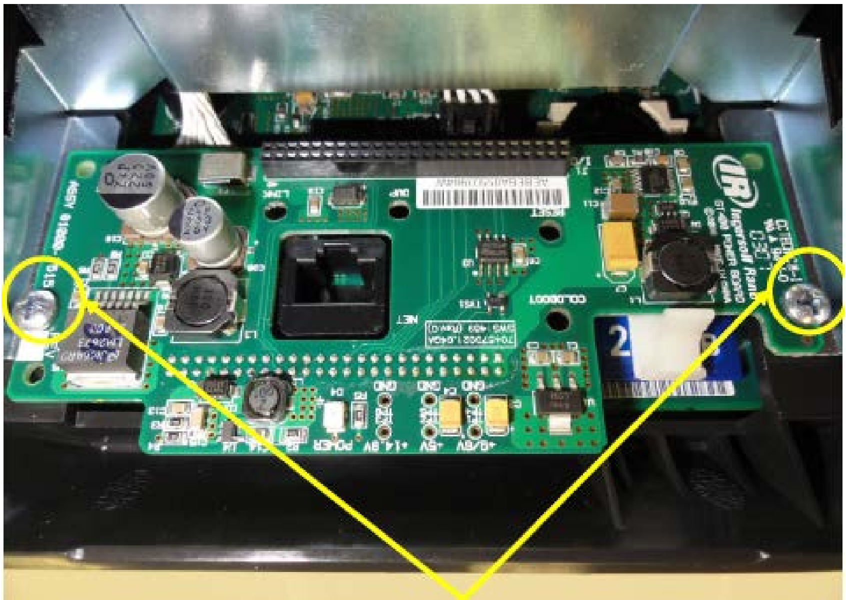


Replacement of the non-TAB SD Card

Remove the two screws highlighted and set aside for reuse.



Technical Note

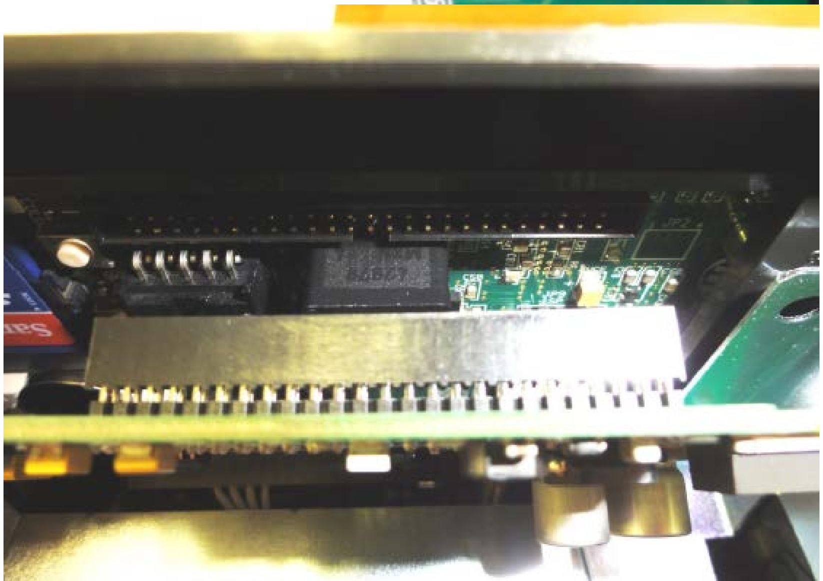


Removal of the Power board

Remove the two screws highlighted and set aside for reuse. Hold the power board by the edges and gently pull the board towards you and set aside.

Replacement of the SD Card

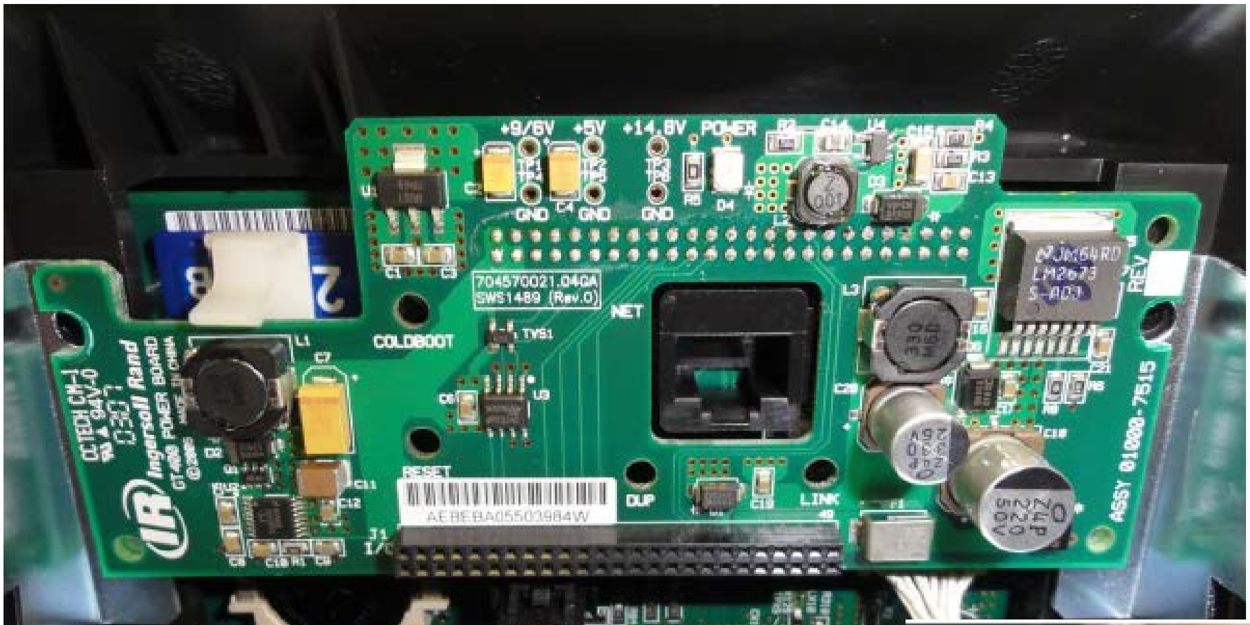
Insert the SD card so that it is seated properly.

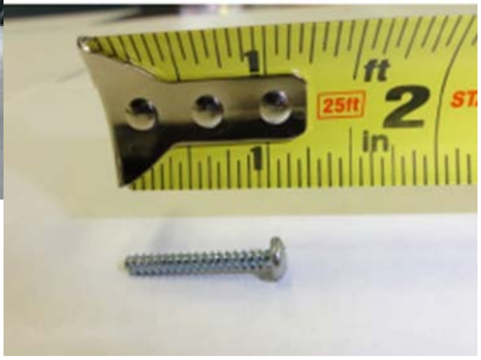


Reinstalling the power board

Making sure your ground strap is on. Align the 2 x 25 pin connector and header and gently mate the two boards.

Technical Note



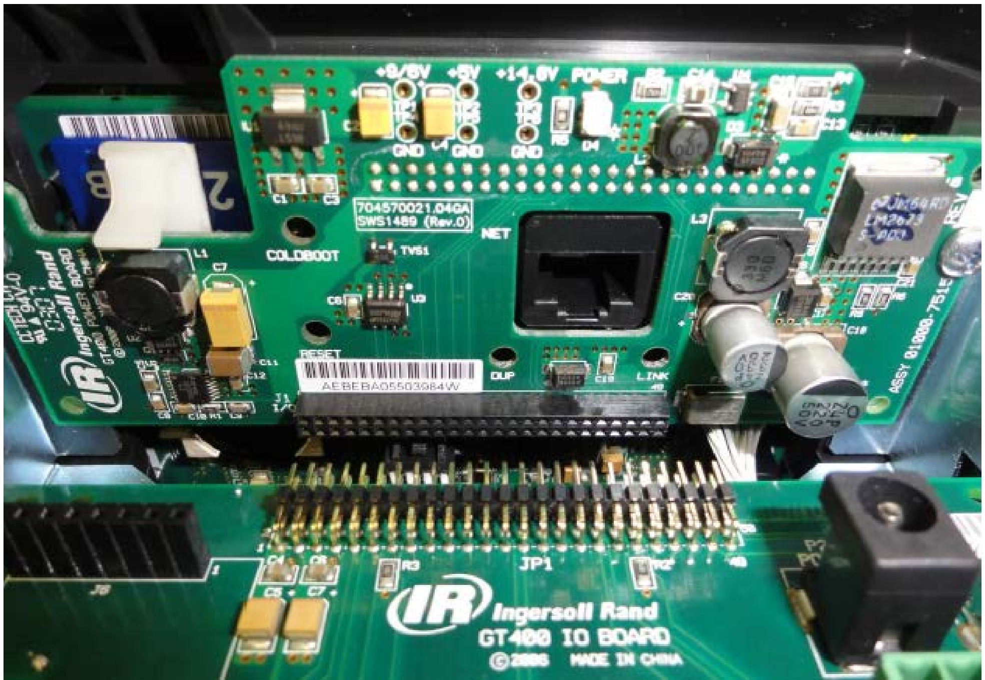


Secure the power board to the unit using the two screws shown in the image to the right.

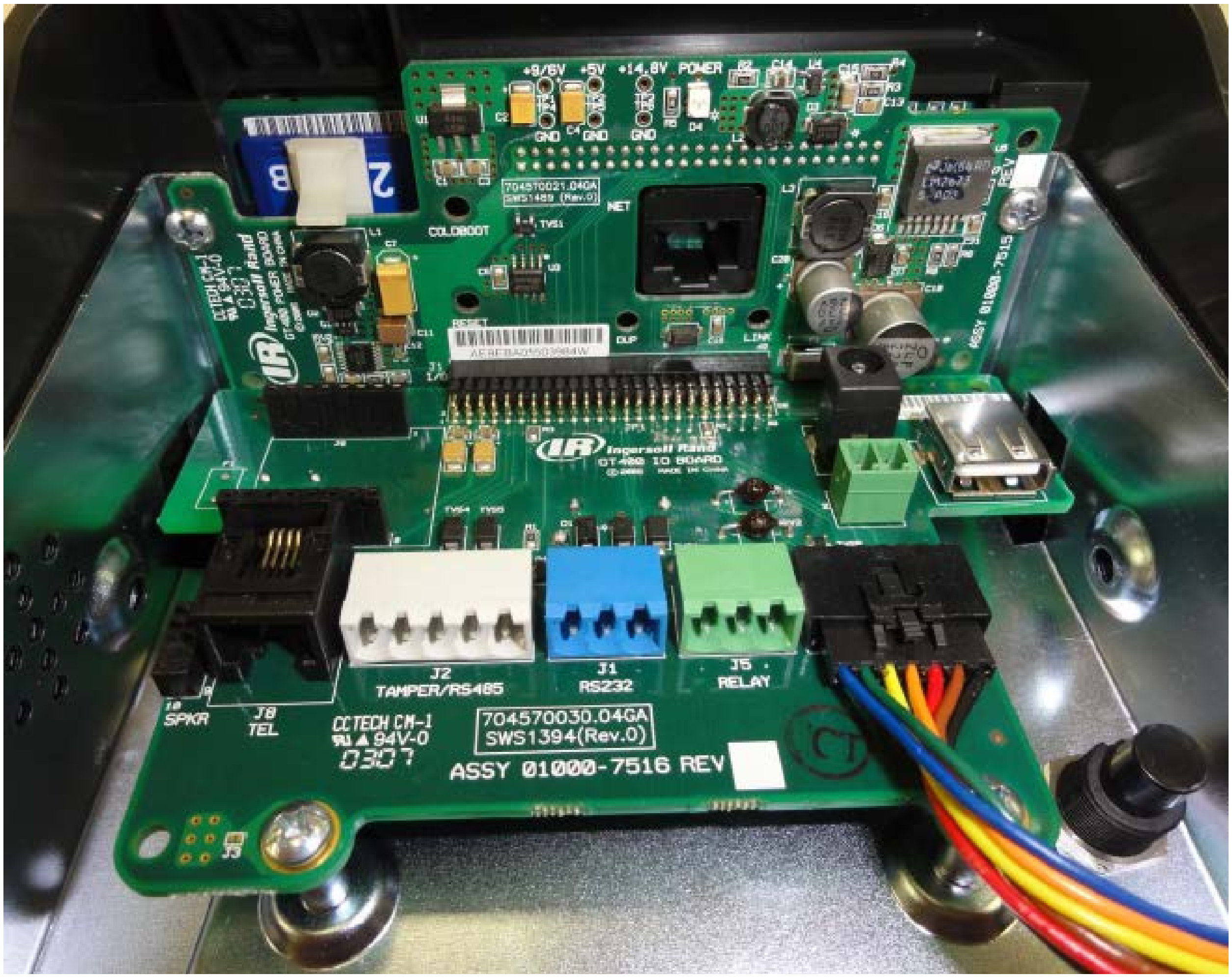
Reinstalling the IO board

Align the IO's 2 x 25 pin header and connector and gently press them together making sure that it is installed.

Secure the IO board to the unit with the screws shown in the image above.



Plugging in the battery backup cable if installed



Replacement complete.

For additional information, please contact Customer Care at 877-671-7011.

GT-400 Speaker Cover Removal and Installation

Refer to Figure 1-1 on page 2 for the instructions in this section.

A speaker cover is a trapezoidal piece that covers the speaker-hole slots on the GT-400. The plate uses a tongue-in-groove configuration to align itself with the body of the Terminal, and it has a stop wedge that will butt up against a rib in the outer shell of the chassis to prevent it from being easily removed.

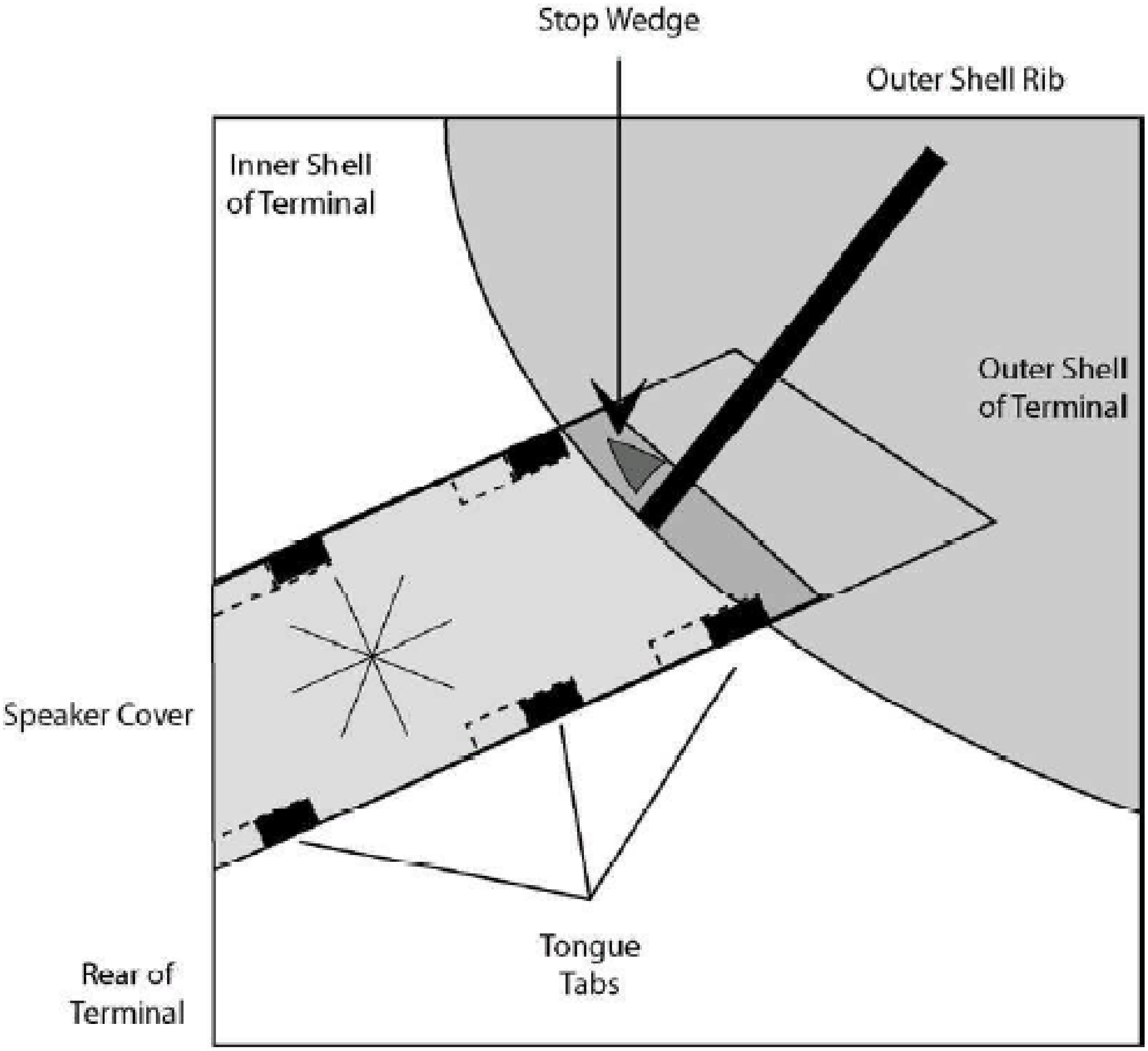
To remove the speaker cover:

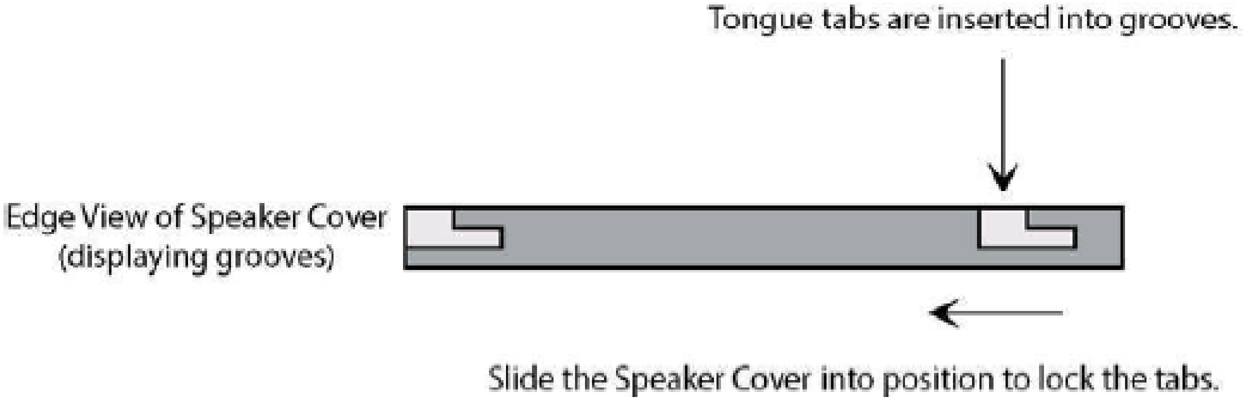
1. Gently lift the upper-edge of the Terminal’s outer shell away from the body of the Terminal.
2. Slide the speaker cover toward the front of the Terminal to free the cover’s groove slots from the Terminal’s tongue tabs.
3. Pull the bottom edge of the cover plate away from the Terminal and remove the speaker cover.

You may find that using a thin-blade screwdriver may assist in removing a speaker cover. However, if you choose to use a thin-blade screwdriver, use care as too much force may crack the body of the Terminal.

To install the speaker cover:

1. Insert the speaker cover with the wide-side down and with the stop wedge entering the body of the Terminal.
2. Align the groove slots in the speaker cover with the tongue tabs extending from the chassis of the Terminal.
3. Slide the speaker cover back so that the rear edge of the speaker cover aligns with the rear edge of the Terminal. You will hear a “snap” that indicates the cover is locked in place.


Stop Wedge
Outer Shell Rib
Inner Shell of Terminal
Outer Shell of Terminal
Speaker Cover
Tongue Tabs
Rear of Terminal


Tongue tabs are inserted into grooves.
Edge View of Speaker Cover (displaying grooves)
Slide the Speaker Cover into position to lock the tabs.

Speaker Cover Removal and Installation

Refer to Figure 1-1 on page 2 for the instructions in this section.

A speaker cover is a trapezoidal piece that covers the speaker-hole slots on the GT-400. The plate uses a tongue-in-groove configuration to align itself with the body of the Terminal, and it has a stop wedge that will butt up against a rib in the outer shell of the chassis to prevent it from being easily removed.

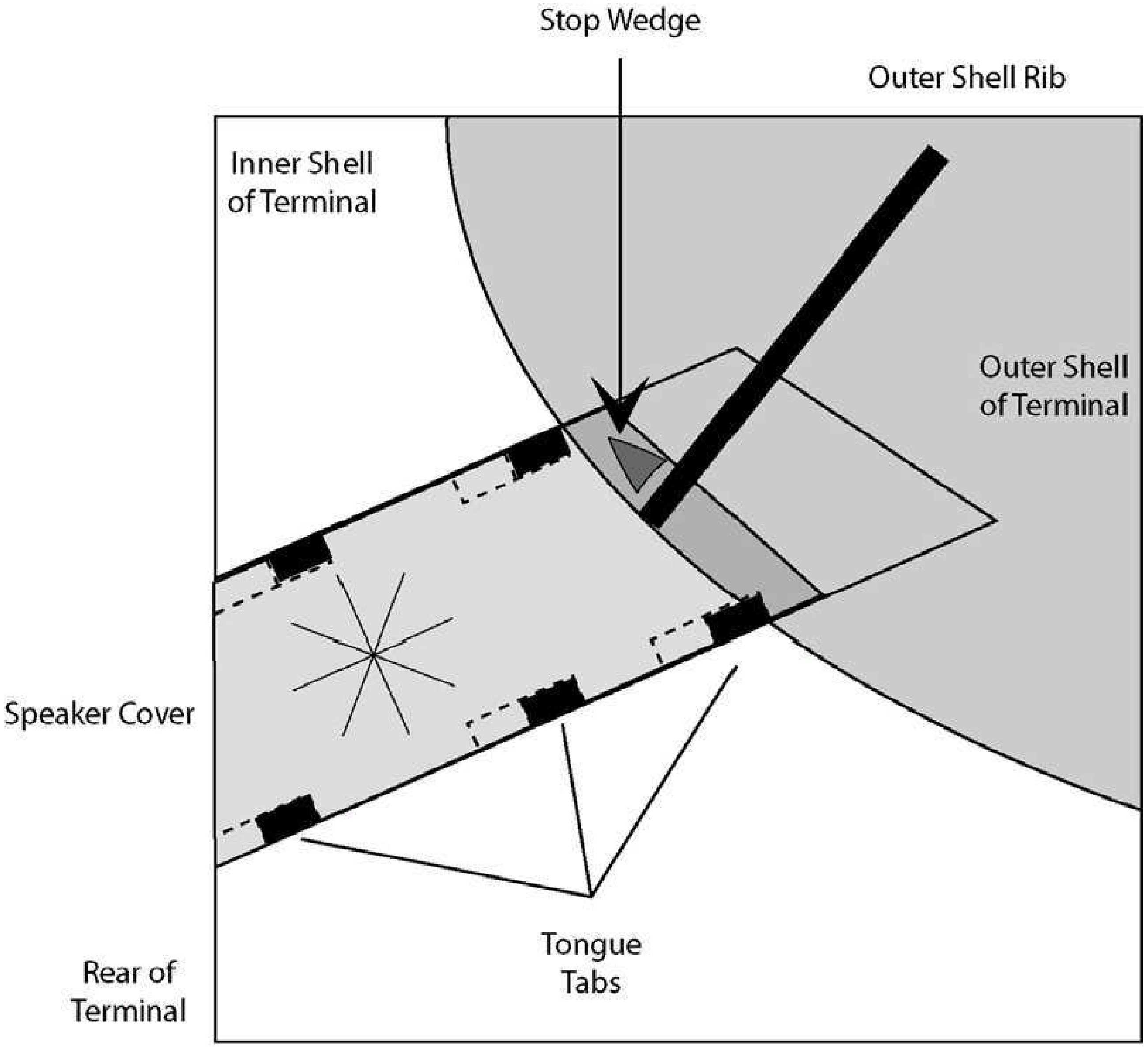
To remove the speaker cover:

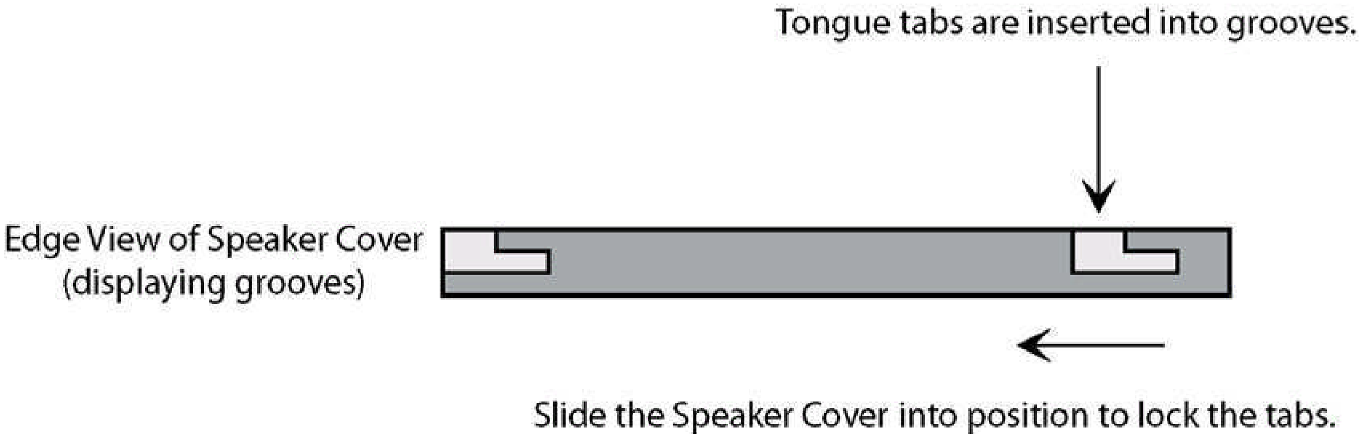
1. Gently lift the upper-edge of the Terminal's outer shell away from the body of the Terminal.
2. Slide the speaker cover toward the front of the Terminal to free the cover's groove slots from the Terminal's tongue tabs.
3. Pull the bottom edge of the cover plate away from the Terminal and remove the speaker cover.

You may find that using a thin-blade screwdriver may assist in removing a speaker cover. However, if you choose to use a thin-blade screwdriver, use care as too much force may crack the body of the Terminal.

To install the speaker cover:

1. Insert the speaker cover with the wide-side down and with the stop wedge entering the body of the Terminal.
2. Align the groove slots in the speaker cover with the tongue tabs extending from the chassis of the Terminal.
3. Slide the speaker cover back so that the rear edge of the speaker cover aligns with the rear edge of the Terminal. You will hear a "snap" that indicates the cover is locked in place.


Stop Wedge
Outer Shell Rib
Inner Shell of Terminal
Outer Shell of Terminal
Speaker Cover
Tongue Tabs
Rear of Terminal


Tongue tabs are inserted into grooves.
Edge View of Speaker Cover (displaying grooves)
Slide the Speaker Cover into position to lock the tabs.

Technical Note

Product	GT-400
Date	May 22, 2014
Subject	USB Flash Drive Replacement

GT-400 USB Flash Drive Replacement

Graphic guide to the replacement of the USB Flash Drive in the GT-400

USB Flash Drive Preparations:

- Please make sure GT-400 is already on firmware 4.4.2 or higher
  - If your GT-400 is not on firmware 4.4.2 yet, please continue to use SD Card only
  - If you want to upgrade from older firmware (e.g. 3.4.16), please contact your administrator and follow the procedures listed under “SD Card to USB Memory Stick Upgrade” of RecoveryAgent-4-4-2_Release Notes.pdf.
    - If removing of SD Card is required, please refer to 70200-0097_B_GT-400_SD_Card.pdf documentation for SD Card removal instructions.
  - USB is formatted to be compatible with GT-400
- Use of anti-static mat, clear of debris, to protect the terminal from scratches

Technical Note

Removal of the USB flash drive

Gently lay the GT-400 on its top panel face down on a clean antistatic mat to protect the surface from scratches and the PCBs from ESD damage.

Warning! - If there is a BB-300 (backup battery) installed, the rainbow cable must be unplugged before the removal of the USB flash. See Figure 1.

Pull the USB flash towards you in order to completely remove it from the slot.

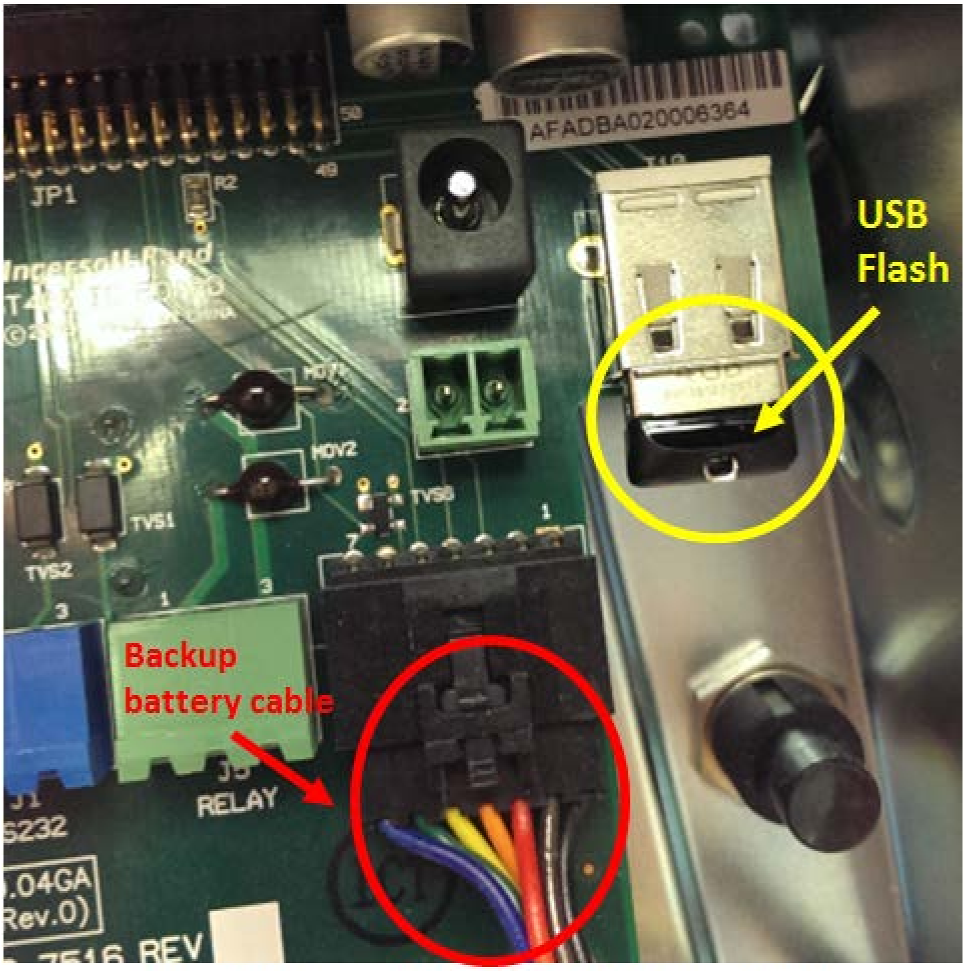
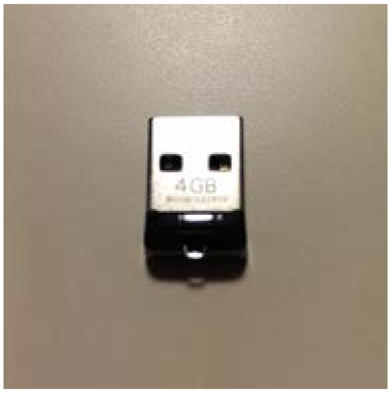
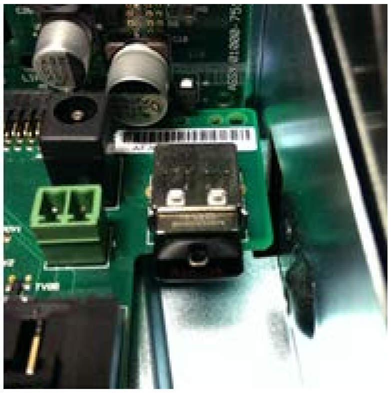


Figure 1: Removal of USB Flash & Battery Cable

Figure 2: USB





The pictures, shown above in Figure 2, illustrate how the USB flash drive is seated into its slot on the power/main board. Once the replacement USB flash drive is properly seated, plug the battery back cable back in (if applicable), insert the power supply and confirm that the unit boots properly. The replacement is complete.

For additional information, please contact Customer Care at 877-671-7011.

Wi-Fi 3rd Party Use: F-Series & G-Series

This document stands to act as a procedural guide for when using a 3rd party Wi-Fi adapter with the HandReaders, both F-Series & G-Series[1]. Schlage has performed testing to confirm that when using a Wi-Fi adapter[2], the HandReader will operate normally; so long as connections and addresses are properly set. Please use the following instructions as a guideline for initial set up of the Wi-Fi adapter.

Setup Summary of the Wireless Router and Bridge:

Host --> Switch --> Primary Wireless Router --> Wireless Router (Repeater/Bridge) --> HandReader[3]

Repeater/Bridge Setup

1. Configure the wireless router with LAN connection from the computer
   a. Set the computer to static IP mode
      i. i.e. Set the wireless router address to 192.168.0.1
      ii. i.e. Set the computer IP address to 192.168.0.100
2. Set the wireless router to repeater/bridge mode
   a. Need to make sure the primary wireless router address is different from repeater/bridge router
      i. i.e. Set the primary wireless router to 192.168.1.1
      ii. i.e. Set the repeater/bridge router to 192.168.1.10
3. Ensure that the DHCP server is disabled on the repeater/bridge router
4. Set the repeater/bridge router to connect to the primary wireless router by using security password
5. Connect a HandReader to the repeater/bridge router LAN port
   a. The GT-400 can be set either DHCP or static IP
   b. The F-Series HandReaders can be set as static IP

[1] F-Series models include: all HandPunch & HandKey models that have Ethernet enables. G-Series includes the GT-400.
[2] Wireless N150 Router: Encore 3G Mobile Broadband Wireless N150 Router plus Repeater, ENHWI-3GN3
[3] Note that the Host and the HandReaders are on the same network.

Schlage

Electronic security

Biometric Solutions

Brochures / Sales Materials

Master Index

HandKey® II

Integrated with Symmetry™ by AMAG Technology, Inc.

Overview

The Schlage HandKey II biometric HandReader seamlessly integrates with AMAG's Symmetry Security Management Software to provide a secure and convenient biometric access control solution to meet your needs.

Symmetry combines advanced Access Control Software, Door Controllers, Card Readers and network IP Security Cameras into a uniquely powerful Security Management System. Through careful design it is extremely easy to learn and use, making it suitable for any size installation in any market.

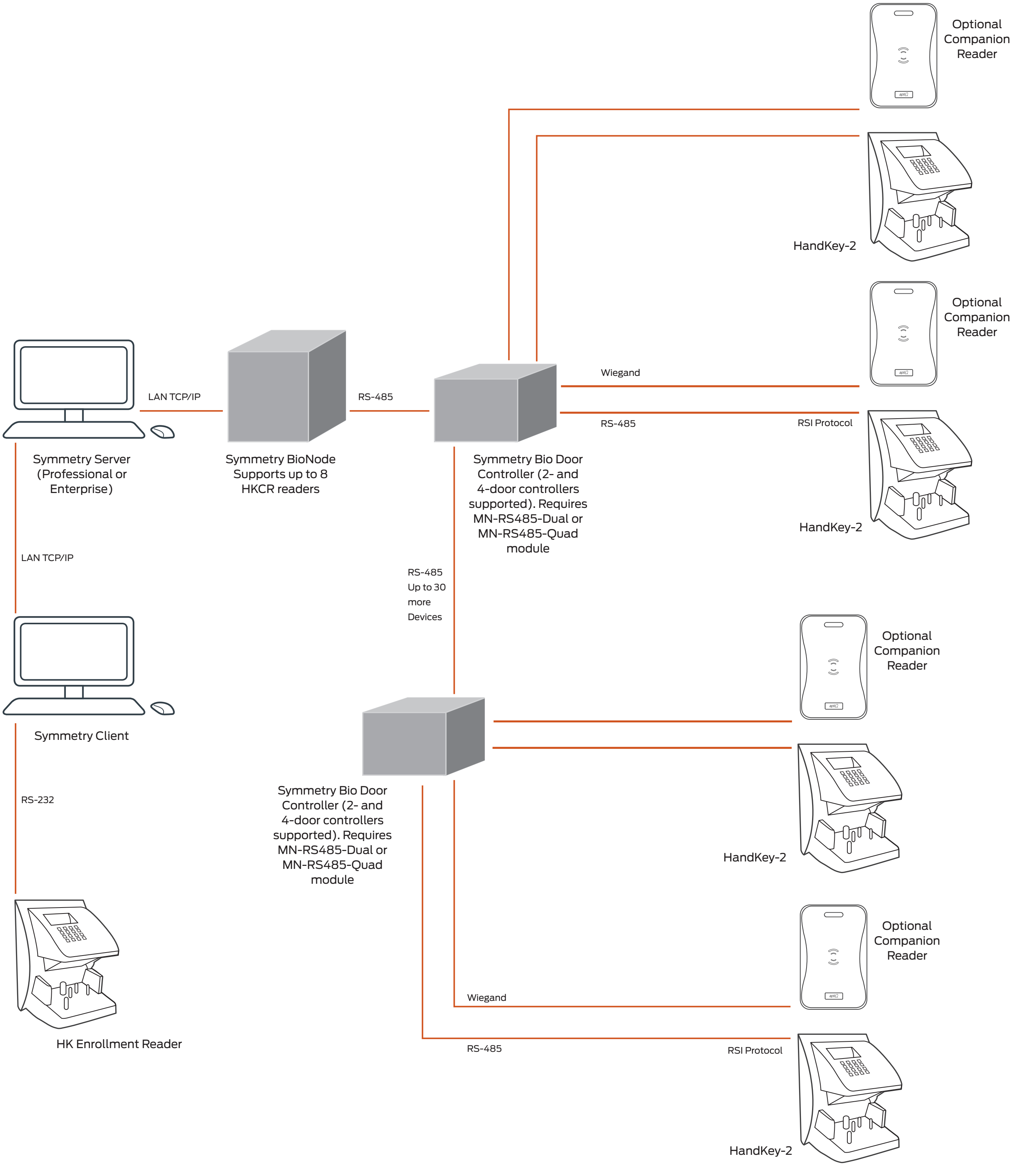
The integration of the HandKey II with Symmetry allows you to add biometric security to critical access points fast, simply, and seamlessly in new and existing systems. The HandKey II measures and verifies the size and shape of a person's hand. Through the use of hand geometry, truly verify who a person is as they access a door. An optional integrated proximity or smart card reader offers multi-factor authentication to provide even higher security for the most critical applications.

Multiple mounting options are available for the HandKey II to suit the requirements of your facility. Optional enclosures provide additional protection in a variety of difficult environments and provide protection from some weather conditions.

Features and benefits

- RS485 communications
- Template management within the access control system
- HandKey II available Reader options with Symmetry:
  - Magnetic stripe
  - Proximity
  - Barcode
  - HID iCLASS®
  - MIFARE®
  - All card readers available with Card + PIN
- Power Requirements: 12 to 24 VDC
- Additional Enclosure Options:
  - FX Enclosure for a degree of protection against dusty, dirty, or rainy environments
  - TX Enclosure for a higher degree of protection against dusty, dirty, or rainy environments
  - When used with an integrated heater option (INT-HTR), either enclosure provides a comfortable heated platen in a cold climate.

System architecture


Optional Companion Reader
HandKey-2
Optional Companion Reader
Wiegand
LAN TCP/IP
RS-485
RS-485
RSI Protocol
Symmetry Server (Professional or Enterprise)
Symmetry BioNode Supports up to 8 HKCR readers
Symmetry Bio Door Controller (2- and 4-door controllers supported). Requires MN-RS485-Dual or MN-RS485-Quad module
HandKey-2
LAN TCP/IP
RS-485 Up to 30 more Devices
Optional Companion Reader
Symmetry Client
Symmetry Bio Door Controller (2- and 4-door controllers supported). Requires MN-RS485-Dual or MN-RS485-Quad module
RS-232
HandKey-2
Optional Companion Reader
Wiegand
RS-485
RSI Protocol
HK Enrollment Reader
HandKey-2

System Capabilities

Features	
Maximum Number of readers supported by Panel	8
Maximum Number of readers supported by door controller	2- and 4-door controllers available
Maximum Number of readers supported by network interface reader	N/A
Maximum Number of devices per RS-485/ RS-422	RS-485 is point-to-point
User Support	Host
Maximum number of users supported	100,000
Other system requirements	
Access control decision maker	Panel
Access decision made when host is not available	Yes
Access decision made when panel is not available to reader	No
Credentials	
Keypad	Yes
Card + PIN+ Hand	Yes
Magstripe	Yes
125 kHz Prox Card	Yes
13.56 MHz Smart Card	Yes
Enabled functions	
Template Management: Templates are stored in Symmetry database on server/host and in the access control panel. Templates are enrolled through Symmetry client application and HK enrollment reader (RS-232 to the client computer).	
Reader Configuration: HandKey readers are configured in the Symmetry User Interface (GUI) including the definition of a threshold value (per reader).	
Operation: HandKey requires AMAG version of firmware. When cardholder provides their ID number through card (or keypad), panel determines if the cardholder has access at that date/time/location and if so, sends template to the reader with authenticate command. The match score is returned, and panel determines if the score meets/exceeds threshold.	
Remote Verification	Yes
Remote Enrollment	Yes
Special Enrollment	No
Duress Codes	Yes
ID Lockout	Yes
Set Individual User Data	No
Transaction Retrieval	Yes
Beep Commands	No
Custom Function Keys	No
Status monitors	
Communication status	Yes
Tamper switch monitoring	Yes

Please contact AMAG Technology at sales@amag.com for additional details on integrated features and credentials supported.

Supported card formats

Proximity cards (125 kHz):

- AWID®
- GE/CASI®
- HID®
- Schlage®
- XceedID®

Smart cards (13.56 MHz):

- HID iCLASS®
- MIFARE®

Options

The HandKey II from Schlage is built to provide the convenience and added security of a biometric solution to your access control system. Designed with your application in mind, the HandKey II can be configured with a number of options to suit your needs.

Options	Part number	Description
Memory options	EM-801-F3	Field upgradable memory expansion to 9,728 users
	EM-803-F3	Field upgradable memory expansion to 32,512 users
	EM-813-F3	Memory expansion to 64,768 users**
	EM-823-F3	Memory expansion to 129,536 users**
	EM-833-F3	Memory expansion to 194,304 users**
Communication options	EN-200	Field upgradable Ethernet communication module (10baseT)
	MD-500	Field upgradable internal dial up modem communication module
Card reader options	PROX	Externally top mounted HID prox reader**
	SC-100	MIFARE reader, externally side mounted**
	ICLASS	iCLASS reader**
	CR-2	Magnetic stripe reader, wall mountable
	BC-100	Bar code reader, wall mount swipe

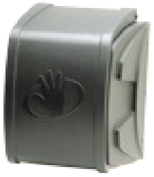
**Factor Option Only

Additional Information

For additional information contact AMAG Technology, Inc. at sales@amag.com or visit www.amag.com

Enclosure options

Enclosures are available to protect your HandKey from the elements and to enable use regardless of your environment.


FX Enclosure

TX Enclosure

Mounting options

Schlage offers options to ensure that the HandKey can be mounted in a manner appropriate for your application.

Standard Reader comes with surface wall mount bracket

Table top secure mount for flat surfaces

About Allegion

Allegion (NYSE: ALLE) creates peace of mind by pioneering safety and security. As a $2 billion provider of security solutions for homes and businesses, Allegion employs more than 7,800 people and sells products in more than 120 countries across the world. Allegion comprises 23 global brands, including strategic brands CISA®, Interflex®, LCN®, Schlage® and Von Duprin®. For more, visit **www.allegion.com**.

aptiQ ■ LCN ■ SCHLAGE ■ STEELCRAFT ■ VON DUPRIN

ALLEGION™

© 2014 Allegion
010041, Rev. 03/14
www.allegion.com/us

For additional information contact AMAG Technology, Inc. at sales@amag.com or visit www.amag.com

Frequently Asked Questions (FAQ)

1. **Q: What is biometrics?**
   A: Biometrics identifies people by a unique human characteristic. The size and shape of a hand, a fingerprint, the voice and several aspects of the eye are just some unique attributes. “The word "biometric" simply means the measurement of a living trait, whether physiological or behavioral. Biometric technologies compare a person's unique characteristics against a previously enrolled image for the purpose of recognizing.”

2. **Q: What is Hand Geometry?**
   A: HandKey uses a field-proven technology called hand geometry, which verifies an individual’s identity based on the size and shape of the hand. It does not take fingerprints or handprints.

3. **Q: Is Hand Geometry new?**
   A: Hand Geometry has been in use longer than any other biometric. Two-dimensional hand geometry devices have been around since the 1970’s. Ingersoll Rand Recognition Systems has sold thousands of HandKey HandReaders since 1986.

4. **Q: How does it work?**
   A: HandReaders work by shining a light on the user’s hand, taking a picture, and looking at the hand silhouette. The illumination is provided by LEDs similar to the remote control on a TV. Think of it as a flashlight casting a shadow of a hand. Geometric measurements of the hand (lengths, widths, areas, and heights) are calculated from the silhouette and then “compressed” by a mathematical formula into a 9-byte numerical template. Since the compression is so high, it is infeasible to reverse-engineer the 9-byte template into the hand image or even the raw geometric measurements of the person that used the HandReader

5. **Q: Do rings or Band-Aids have an effect?**
   A: Not usually enough to reject a valid user. Just make sure the ring is in the upright position and hand placement is proper and there should not be any issues.

6. **Q: What happens if I injure my hand and have it bandages or in a cast?**
   A: You can be enrolled with your left hand; palm up while the right hand is disabled. It’s not as comfortable but will work fine.

7. **Q: My employees are concerned about hygiene issues. How do I address this concern?**
   A: Every HandReader contains antimicrobial technology which inhibits the growth of a broad spectrum of bacteria, mold, and fungi, making the platen’s surface more hygienic. This silver-based agent is embedded into the materials used to produce the platen during the manufacturing process. As such, they cannot leach out or wash off the surface thus remain active for the life of the biometric reader. Schlage Biometrics has been providing HandReaders for more than 20 years. Everyday several hundred thousand hand geometry units are used by millions of people in applications like day care centers, athletic clubs, hotels, manufacturing facilities, government installations, education facilities, quick serve restaurants, and grocery stores globally. Schlage Biometric HandReaders have a proven track record in the field and are the durable and reliable biometric you can count on.

8. **Q: Are there any privacy issues?**
   A: The HandReader terminal does not collect and store an image of the hand, but instead it converts the image to a 9-byte numerical template which is a mathematical representation of size and shape of the hand. Once this numerical template is developed it is stored in a memory location which is defined by the person’s ID number. To authenticate a user already verified in the

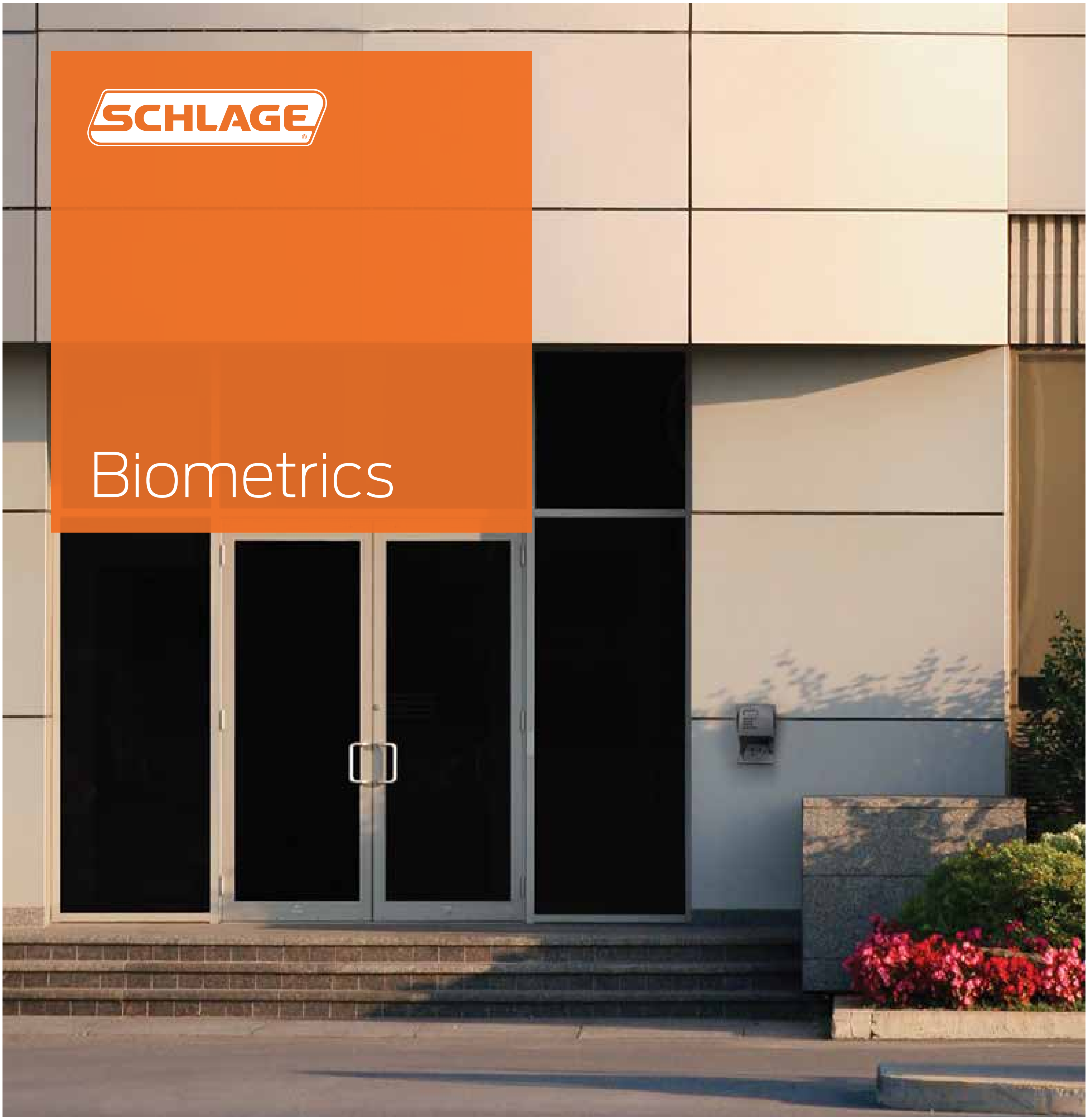
database, the users ID is entered and their hand is placed on the platen (surface area where users place their hand). An image of the hand is captured and then converted to a 9-byte numerical template. If the new template matches the stored template, the person's identity is verified and the transaction is recorded. No personally-identifiable characteristics such as scars, marks, tattoos, fingerprints or palm prints are captured or detected by the terminal.

9. **Q: Is the HandKey safe?**
   The infrared lights used in the hand reader are similar to those used in remote controls for TV's and VCR's. Internal testing concluded that the light intensity generated by the infrared lights in the HandReader is significantly less than the light intensity generated by direct sunlight. Using a HandReader for 30 seconds a day is comparable to standing in the sun for 0.2 seconds. Schlage Biometrics has submitted HandReader information to the U.S. Occupational Safety and Health Administration (OSHA). OSHA did not report any hazards. The Federal Communications Commission requires that computers meet sub-part J of Part 15 of FCC rules. This section details radiated energy. Schlage Biometrics has tested to these standards and meets or exceeds them. Schlage Biometrics also meets the requirements of the European Community and is CE

ALLEGION™

SCHLAGE®

Biometrics



Contents

Put your trust in the name you know

For more than 90 years Schlage® has been providing innovative security solutions for schools, hospitals, government facilities and a host of other commercial buildings. Today, Schlage is at the forefront of cutting edge technology with electronic locking, wireless access, biometric and smart card solutions.

With a wide range of products, functions and styles, Schlage has what you need no matter how demanding your application. And we stand behind every product we make with an outstanding service organization that will be with you every step of the way. It's our commitment to design, performance and technology that ensures you can stand behind our products too.

Reliable security with confidence

Schlage biometrics specializes in the development, marketing and service of biometric devices for access control and workforce management applications.

Located in the heart of California's Silicon Valley, Schlage biometrics offers biometric technology as a secure alternative to easily lost or compromised ID cards and PIN numbers. The technology uses hand geometry to verify a person's true identity.

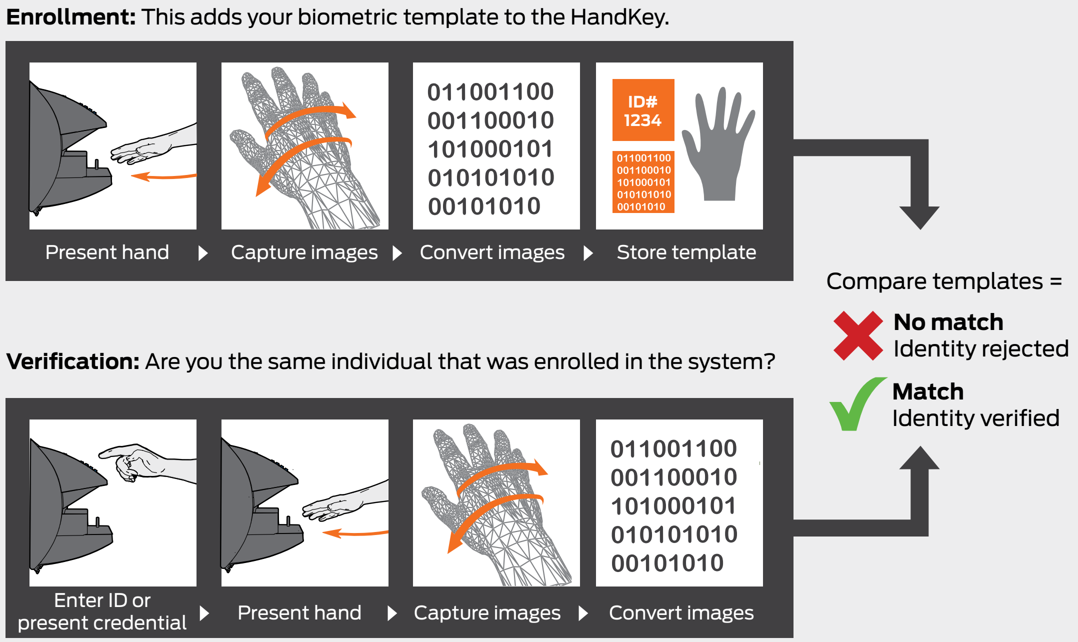
When you choose a Schlage biometrics product, you can be sure that you have done the job right the first time. After all, our products are the most reliable and dependable on the market today. Our HandKey® II is easy to install and simple to maintain. That means fewer service issues for you and low total cost of ownership.

Hand Geometry

Biometric products identify people by analyzing their unique human characteristics. Schlage Hand Geometry readers use field-proven technologies to provide increased security at any door and to ensure that the right person is at the right place at the right time. These technologies are frequently used in universities, data centers, day care centers, airports, health care facilities and government buildings.

Biometric verification

How it works



Enrollment: This adds your biometric template to the HandKey.

Compare templates =

✗ **No match** Identity rejected

✓ **Match** Identity verified

Verification: Are you the same individual that was enrolled in the system?

Top 10 reasons to select Hand Geometry

Field proven reliability

1. Hundreds of thousands of HandKeys are installed all over the world in diverse applications, providing millions of error free transactions every day

Convenience and cost savings

2. Incredibly fast installation and intuitive enrollment increases user convenience
3. Verification in less than one second makes it ideal for high throughput applications
4. High product quality + low maintenance costs = low total cost of ownership
5. Eliminate the worry of lost, stolen or unauthorized transfer of ID cards plus the cost of purchasing and maintaining these cards

Eliminate privacy concerns

6. Hand geometry technology is well accepted by end users, as there are no fingerprints or palm prints taken and the user does not leave behind any trace of their biometric data

Amazing versatility

7. HandKeys can be used as standalone systems to protect critical access points that can be easily integrated into virtually every new or existing access control system in the market today
8. Ability to customize user-specific security levels, time zones, holidays and languages based on your needs
9. Optional access control template management software allows the HandKeys to form a system that communicates alarms and transactions in real time, provides activity reports, allows supervised on-site or remote user enrollment and expiring privileges for temporary access
10. Environmental enclosures and integrated heater units make the HandKey an ideal solution for outdoor usage

Applications

The versatility and flexibility of the HandKeyII lends itself to diverse indoor and outdoor applications.

Critical infrastructure

- Transportation hubs - at airports and shipping ports to grant access to authorized personnel to aircraft/ship operations, baggage handling and other sensitive areas
- Data centers - HandReaders accommodate a large number of users, offer a high level of security, are easy to use, provide for remote enrollment & eliminate the need to carry a card
- Construction facilities - highly robust and user friendly HandReaders operate well in nearly all environmental conditions; unaffected by dirt on the hands, poor lighting conditions, or the worn fingerprints endemic of manual laborers
- They are also installed at various government research facilities
- Prisons - monitor all comings and goings at prisons and eliminate the need for posting guards at all access sites and supplying them with keys
- Military installations - protecting US troops & assets worldwide by providing reliable access to the appropriate personnel

Healthcare facilities

- Pharmacy, surgery, long term care, and research facilities – increase security by providing access to secure areas only to authorized personnel

Financial institutions

- Safe deposit vaults - enhanced security to gain access to safe deposit boxes without the need for personnel to accompany the customer in and out of the vault

Education

- Residence halls - verify students to ensure that only authorized students gain access
- Recreational facilities - minimize people's ability to transfer IDs and eliminate the need for keys / cards
- Dining halls - limit access to students who have paid for the meal plan
- Computer labs - provide access only to authorized personnel seeking access to sensitive equipment and information

Hospitality

- Lodging - access to high security, high valued openings such as data records and hotel supply areas
- Entertainment - access to high security, high valued openings in casinos, stadiums and theme parks

Commercial buildings

- Specialized high asset areas - access to high security, high valued areas such as IT, HVAC, conference rooms in addition to front doors
- Corporate campuses - provide high security to a variety of restricted areas like management offices and expensive high tech equipment rooms

HandKey II

Our HandKey II product is ideal for applications where consistent and dependable security is of prime importance. The product is easy to maintain, and provides an ideal mix of convenience, security and peace of mind.

In addition to all Hand Geometry benefits, the HandKey II offers:

- Convenience of multiple credential options such as proximity, magnetic stripe, barcode, iCLASS® and MIFARE®
- Field installable Ethernet module
- Outdoor enclosure options that make the HandKey II an ideal solution for outdoor usage
- Field upgradable and expandable memory options from 512 to 259,072 users for scalable security that grows with your needs
- Three user-definable outputs to connect to auxiliary devices such as audible or silent alarms, door locks or lighting systems
- Ability to write the industry's most compact biometric template on a card instead of in a database results in higher security & unlimited user capacity
- Specially formulated antimicrobial coating with silver ions on the platen to inhibit the growth of bacteria, mold and mildew to mitigate hygiene concerns. The coating is safe and lasts for the life of the product
- Blue hand outline on the platen facilitates easy enrollment and reduces error rates during verification

Models, options and accessories

Schlage biometrics offers a number of options and accessories to help you create a solution to meet your specific needs.

Base models	HK-2-F3
Card readers	**Prox:** Externally top mounted HID prox reader, factory option only **HID iCLASS®**: iCLASS reader, factory option only **SC-100**: MIFARE® reader, factory option only **CR-2**: Mag stripe wall mount card reader **BC-100**: Bar code reader, wall mount swipe
Memory	**EM-801-F3**: Field upgradeable memory expansion up to 9,728 users **EM-803-F3**: Field upgradeable memory expansion up to 32,512 users **EM-813-F3**: Memory expansion up to 64,768 users **EM-823-F3**: Memory expansion up to 129,536 users **EM-833-F3**: Memory expansion up to 194,304 users **EM-843-F3**: Memory expansion up to 259,072 users
Communication	**EN-200**: Field upgradeable Ethernet communication module 10baseT **MD-500**: Internal dial-up modem
Power options	**PS-110**: Power supply, 120VAC to 13.5 VDC **PS-220**: Power supply, 220VAC to 13.5 VDC **BB-200**: Optional battery backup
Mounting	**TM-100**: Table top secure mount for flat surfaces
Left hand option	N/A
Network accessories	**DC-102**: Data converter for 4 wire system, RS-232 to RS-422 with 120V, 60Hz power supply **DC-102 with 220V:** 50Hz power supply **DC-104**: Data converter for 2 or 4 wire systems, RS232 to RS485/RS 422 with 120V, 60Hz power supply **DC-104 with 220V:** 50Hz power supply

Specifications for the HandKey Series

Base models	HK-2-F3
Description	HandReader with base memory for 512 users
Verification time	≤ 1 second for comparison to reference
ID number length	1 – 10 digits
Duress code	1 leading digit, user definable
Communication	**RS-232**: Baud rate 300 bps to 28,800 bps **RS-422**: Baud rate 300 bps to 28,800 bps **RS-485**: Baud rate 300 bps to 28,800 bps **Optional Modem**: Baud rate 300 bps to 14,400 bps **Optional Ethernet**: 10 Base T
Template size	9 bytes
User memory	512 users expandable to 259, 072 users
Inputs	**Standard**: 26 bit, 9 bit ID Wiegand **Optional**: Mag stripe, bar code, smart card **HandKey input**: Request-to-exit, door switch input, 2 auxiliary inputs
Outputs	**Door control**: Lock output **Card reader emulation mode**: Wiegand, mag stripe, bar code 1 programmable auxiliary **Outputs to peripheral devices**: Audible or silent alarms, door locks, lighting systems
Event monitoring	**Tamper**: HandKey opened or removed **ID refused**: User not verified after user definable number of tries exceeded **Duress**: User entered duress code digit **Power failure**: HandKey switched to optional battery power
Programmable HandKey commands	▪ Add/remove users ▪ Set global operating thresholds ▪ Set individual user data (authority or threshold levels, time zones) ▪ Transmit data from master to remote ▪ Data received by master from remote ▪ Transmit/receive data from optional software ▪ Check status of door (tamper, door monitor switch) ▪ Time zones – 62 total (2 fixed, 60 programmable) ▪ Set language ▪ Set date format, date and time ▪ Edit holidays
Antimicrobial	Available on platen
Blue hand outline	Available on platen
Dimensions H x W x D	11.65 in x 8.85 in x 8.55 in 29.6 cm x 22.5 cm x 21.7 cm
Power requirements	12 to 24 VDC or 12 to 24 VAC 50-60 Hz 7 Watts (without options)
Weight	5.3 lbs. (2.4kgs.) (without battery back-up or wall plate)
Temperature	Operating: 0° C to +45° C / 32° F to 113° F Non-operating (storage): -10° C to +60° C / 14° F to 140° F
Relative humidity	Operating: 20% to 80% RH Non-condensing Non-operating (storage): 5% to 85% RH non-condensing

A biometric that works indoors and outdoors

Schlage biometrics provides various options to protect your HandKey II from the elements. Two different, proven solutions are available to ensure your HandKey II keeps performing regardless of your environment.

FX enclosure

Biometric HandKey enclosure

Constructed from high impact UV resistant polycarbonate material, the FX enclosure provides a degree of protection against dusty, dirty, or rainy environments. This enclosure has been designed so that it can be added to an existing installation. When used with an integrated heater option (INT-HTR), it provides a comfortable heated platen against a cold climate.

TX enclosure

Biometric HandKey enclosure

The TX Enclosure provides a higher degree of protection against dusty, dirty, or rainy environments. When used with an integrated heater option (INT-HTR), it provides a comfortable heated platen against a cold climate.

	~~FX enclosure~~	~~TX enclosure~~
Temperature range	-20F to 120F -29C to 49C	-45F to 120F -43C to 49C
Dimensions H x W x D	14.75" x 12.00" x 10.50" 37.5 cm x 30.5 cm x 26.7 cm	23.00" x 14.00" x 11.25" 58.4 cm x 35.6 cm x 28.6 cm
Gross weight	7.3 lbs / 3.3 kg	45.0 lbs / 20.4 kg
HandKey models	HK-2-F3	HK-2-F3
Heater	Factory installed option only, model no. INT-HTR	Factory installed option only, model no. INT-HTR

HandNet for Windows

HandNet for Windows lets you control and monitor a network of HandKey II readers. With just one comprehensive program, you can monitor activity and alarms on all readers, and control the access of each user.

- Automatic hand template management feature allows template distribution from enrollment HandKey II to other selected HandReaders thus eliminating the need for a user to be enrolled at every HandKey II
- Independent door control capability without the need for an access control panel
- Monitor multiple remote sites from the convenience of your PC
- Remote enrollment feature enables a HandKey II to be controlled from the software. For example a guard behind a glass partition or a supervisor in a distant office can enroll new users without physically going to the HandKey II
- Assign temporary access to selected users by specifying a user's access start and stop days and times
- Manage archive activity to keep old information available for reports
- Manage alarms for additional security

Models	HN-2-T1	HN-2-T2	HN-2-T3	HandNet Lite
Description	Manages up to 5 HandKeys	Manages up to 25 HandKeys	Manages an UNLIMITED number of HandKeys	Manage the Handkey II without access control software functionalities

Specifications for software

Base models	HandNet for Windows	HandNet Lite
Computer	Intel Pentium 1 GHz or higher, AMD Athlon 1 GHz or higher	Intel Pentium 1 GHz or higher, AMD Athlon 1 GHz or higher
Operating system	Windows XP SP3 32 bit, Windows 7 Professional SP1 32-bit and 64-bit	Windows XP SP3 32 bit, Windows 7 Professional SP1 32-bit and 64-bit, Windows Server 2003 SP2 32-bit
Drives	CD Rom for installation	CD Rom for installation
Hard disk	2 GB minimum, 1 GB free space	60 GB minimum, 10 GB free space
Monitor	Minimum resolution 1024 x 768	Minimum resolution 1024 x 768
Memory	2 GB (Minimum 1 GB)	4 GB (Minimum 2 GB)
Database	MS Access	MS SQL Server 2000 MSDE
Products supported	HK-2-F3	HK-2-F3
Template management	Available	Available
Supported communications	RS232, RS485, Ethernet	RS232, RS485, Ethernet
Time zones	Available	Available
Reports	Available	Limited - use reports from an access control panel
Door control	Available	N/A - use panel door control
Alarms	Available	N/A - use panel alarms
Open door remotely	Available	N/A - use panel door control
Network readers	Available	Available
Archives activity	Available	Available - database backup
Remote enrollment	Available	Available

Additional Schlage solutions

Workforce management

Schlage HandPunch® terminals utilize Hand Geometry technology to automate Workforce Management systems, control labor costs, eliminate costly badges and cards, reduce compliance risk and stop time fraud.

The HandPunch is a trusted and reliable solution used in a variety of workforce management applications worldwide.

- Hospitality
- Education
- Government
- Manufacturing
- Quick serve restaurants
- Construction
- Grocery
- Healthcare
- Hospitals
- Retail stores

MR: What are the Allegion email addresses?

Order processing
Phone: 877-671-7011, Option 1, Option 8
Fax: 800-452-0665
sbsom@~~irco.com~~

Technical support
Phone: 877-671-7011, Option 2, Option 8
Readers_Credentials_Biometrics_TechProdSupport@~~irco.com~~

About Allegion

Allegion (NYSE: ALLE) creates peace of mind by pioneering safety and security. As a $2 billion provider of security solutions for homes and businesses, Allegion employs more than 8,000 people and sells products in more than 120 countries across the world. Allegion comprises more than 25 global brands, including strategic brands CISA®, Interflex®, LCN®, Schlage® and Von Duprin®.

For more, visit **www.allegion.com**

ALLEGION™

ALLEGION™

SCHLAGE®

HandPunch® concerns

When it comes to managing time and attendance systems no other biometric solution compares to the Schlage® HandPunch®. Time after time our customers report the reliability of the HandPunch because it accurately identifies employees in environments where dirt, dust, and wet conditions may limit the accuracy of other biometrics. The HandPunch has been known to pay for itself in less than 9 months, making it an ideal solution to businesses that are trying to control costs due to employee payroll fraud, manual data review and correction time, and payroll error. While the benefits of implementing Schlage HandReaders are many, employees may raise concerns about the way hand geometry technology could affect their privacy rights. Schlage Biometrics understands their concerns and would like to address the issues regarding biometrics that may come up.

HandReaders work by shining a light on the user's hand, taking a picture, and looking at the hand silhouette. The illumination is provided by LEDs similar to the remote control on a TV. Think of it as a flashlight casting a shadow of a hand.

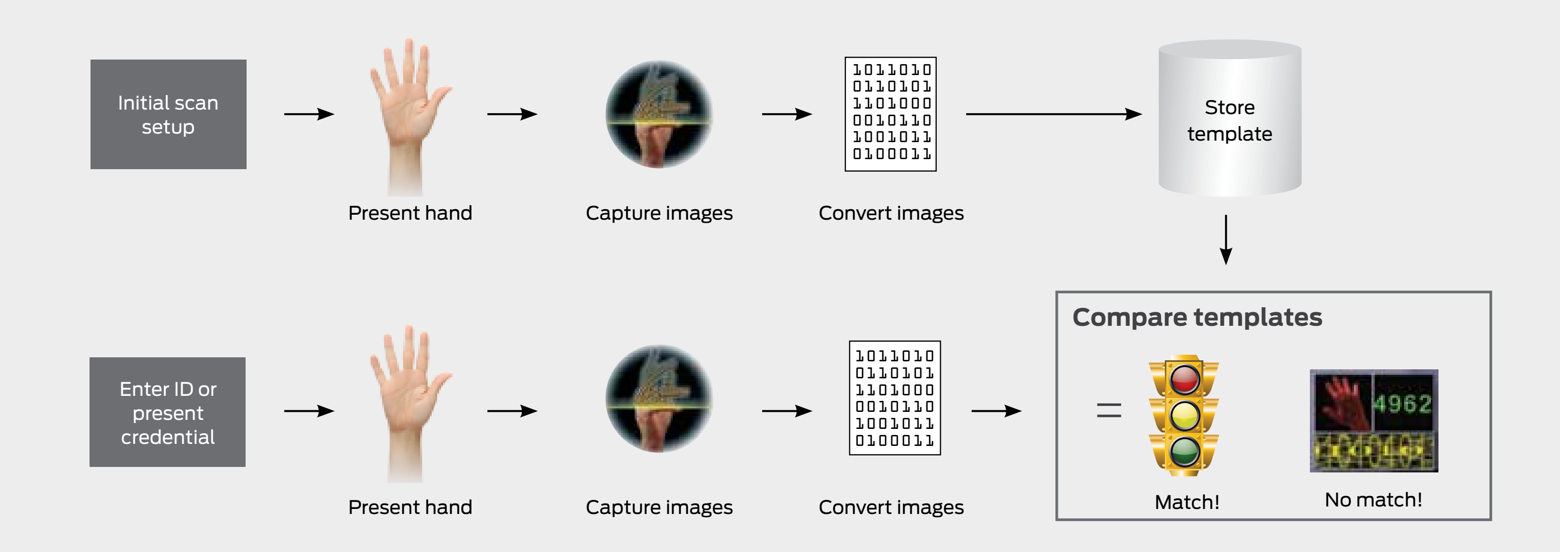
Technology

Geometric measurements of the hand (lengths, widths, areas, and heights) are calculated from the silhouette and then "compressed" by a mathematical formula into a 9-byte numerical template. Since the compression is so high, it is infeasible to reverse-engineer the 9-byte template into the hand image or even the raw geometric measurements of the person that used the HandReader.

Privacy

The HandReader terminal does not collect and store an image of the hand, but instead it converts the image to a 9-byte numerical template which is a mathematical representation of size and shape of the hand. Once this numerical template is developed it is stored in a memory location which is defined by the person's ID number.

To authenticate a user already verified in the database, the user's ID is entered and their hand is placed on the platen (surface area where users place their hand). An image of the hand is captured and then converted to a 9-byte numerical template. If the new template matches the stored template, the person's identity is verified and the transaction is recorded.



No personally-identifiable characteristics such as scars, marks, tattoos, fingerprints or palm prints are captured or detected by the terminal. According to Article 29 from the EU Advisory Body on Data Protection and Privacy: “biometric systems… which do not leave traces (e.g. shape of the hand but not fingerprints)… create less risks for the protection for fundamental rights and freedoms of individuals.”

Religion

Since the HandReader is not capable of personally-identifiable characteristics, HandReaders do not in any way have the ability to place or detect the “Mark of the Beast” or any other mark on a person’s hand. Many religious organizations and churches trust the HandReader every day to accurately and efficiently manage their time and attendance systems.

Safety

The infrared lights used in the HandReader are similar to those used in remote controls for TV’s and VCR’s. Internal testing concluded that the light intensity generated by the infrared lights in the HandReader is significantly less than the light intensity generated by direct sunlight. Using a HandReader for 30 seconds a day is comparable to standing in the sun for 0.2 seconds.

Schlage Biometrics has submitted HandReader information to the U.S. Occupational Safety and Health Administration (OSHA). OSHA did not report any hazards.

The Federal Communications Commission requires that computers meet sub-part J of Part 15 of FCC rules. This section details radiated energy. Schlage Biometrics has tested to these standards and meets the requirements of the European Community and is CE Certified.

Hygiene

Every HandReader contains antimicrobial technology which inhibits the growth of a broad spectrum of bacteria, mold, and fungi, making the platen’s surface cleaner and more hygienic. This silver-based agent is embedded into the materials used to produce the platen during the manufacturing process. Therefore, the antimicrobial surface remains active for the life of the biometric reader.

Schlage Biometrics has been providing HandReaders for more than 20 years. Every day several hundred thousand hand geometry units are used by millions of people in applications like day care centers, athletic clubs, hotels, manufacturing facilities, government installations, education facilities, and long-term care facilities globally. Schlage Biometric HandReaders have a proven track record in the field and are the durable and reliable biometric you can count on.

About Allegion

Allegion (NYSE: ALLE) creates peace of mind by pioneering safety and security. As a $2 billion provider of security solutions for homes and businesses, Allegion employs more than 8,000 people and sells products in more than 120 countries across the world. Allegion comprises more than 25 global brands, including strategic brands CISA®, Interflex®, LCN®, Schlage® and Von Duprin®. For more, visit **www.allegion.com.**

aptiQ ■ LCN ■ SCHLAGE ■ STEELCRAFT ■ VON DUPRIN

ALLEGION™

SCHLAGE®

Visitor Access Solutions

Biometric Hand Readers in K-12 Schools and Day Care Centers

As a school or day care center, you want to be able to provide peace of mind to your parents as you look after their most valuable assets—their children. Our biometric HandReaders offer the ability to manage visitor access securely and easily.

Problem:

Find a way to manage visitor access to my K-12 school or day care center throughout the day.

- Manage access of employees
- Manage access of parents and guardians
- Manage access of other visitors

Solution:

In a typical school setting, front doors are unlocked at specified times, allowing parents and other visitors to access the building during those times. During the day, most K-12 schools and day care centers manage visitors through a receptionist who keeps a log of all visitors. This creates the risk of unwanted visitors gaining entry to the facility.

A better solution is to use credentials to validate that the visitor entering the school or day care has the right to enter. Credentials include pins, cards, and biometric data. Pins and cards offer a higher level of security, but only biometrics can validate that a person is who they say they are. Biometrics include fingerprints, retinas, palm prints, and hand geometry.

Schlage offers the easiest biometric to use, our hand geometry reader, the HandKey® II. The HandKey II offers the best combination of speed and accuracy — this is why leading schools, day care centers and universities in the country are using biometric HandReaders for access control. The HandKey II can be used as a standalone system and managed through free template management software, HandNet Lite.

Biometric HandReaders offer the most secure and easy to use solution to manage visitor access at your K-12 school or day care center.

Ingersoll Rand
Security Technologies

Features and Benefits

- Reads the size and shape of a user's hand
- Easy enrollment process—easy to manage addition of new visitors to the system
- Fast—does not create backups as many parents are entering the building
- Ideal solution for outdoor usage

Ingersoll Rand
Security Technologies

877-671-7011 • securitytechnologies.ingersollrand.com

Frequently Asked Questions (FAQ)

1. **Q: What is biometrics?**
   A: Biometrics identifies people by a unique human characteristic. The size and shape of a hand, a fingerprint, the voice and several aspects of the eye are just some unique attributes. “The word "biometric" simply means the measurement of a living trait, whether physiological or behavioral. Biometric technologies compare a person's unique characteristics against a previously enrolled image for the purpose of recognizing.”

2. **Q: What is Hand Geometry?**
   A: HandKey uses a field-proven technology called hand geometry, which verifies an individual’s identity based on the size and shape of the hand. It does not take fingerprints or handprints.

3. **Q: Is Hand Geometry new?**
   A: Hand Geometry has been in use longer than any other biometric. Two-dimensional hand geometry devices have been around since the 1970’s. Ingersoll Rand Recognition Systems has sold thousands of HandKey HandReaders since 1986.

4. **Q: How does it work?**
   A: HandReaders work by shining a light on the user’s hand, taking a picture, and looking at the hand silhouette. The illumination is provided by LEDs similar to the remote control on a TV. Think of it as a flashlight casting a shadow of a hand. Geometric measurements of the hand (lengths, widths, areas, and heights) are calculated from the silhouette and then “compressed” by a mathematical formula into a 9-byte numerical template. Since the compression is so high, it is infeasible to reverse-engineer the 9-byte template into the hand image or even the raw geometric measurements of the person that used the HandReader

5. **Q: Do rings or Band-Aids have an effect?**
   A: Not usually enough to reject a valid user. Just make sure the ring is in the upright position and hand placement is proper and there should not be any issues.

6. **Q: What happens if I injure my hand and have it bandages or in a cast?**
   A: You can be enrolled with your left hand; palm up while the right hand is disabled. It’s not as comfortable but will work fine.

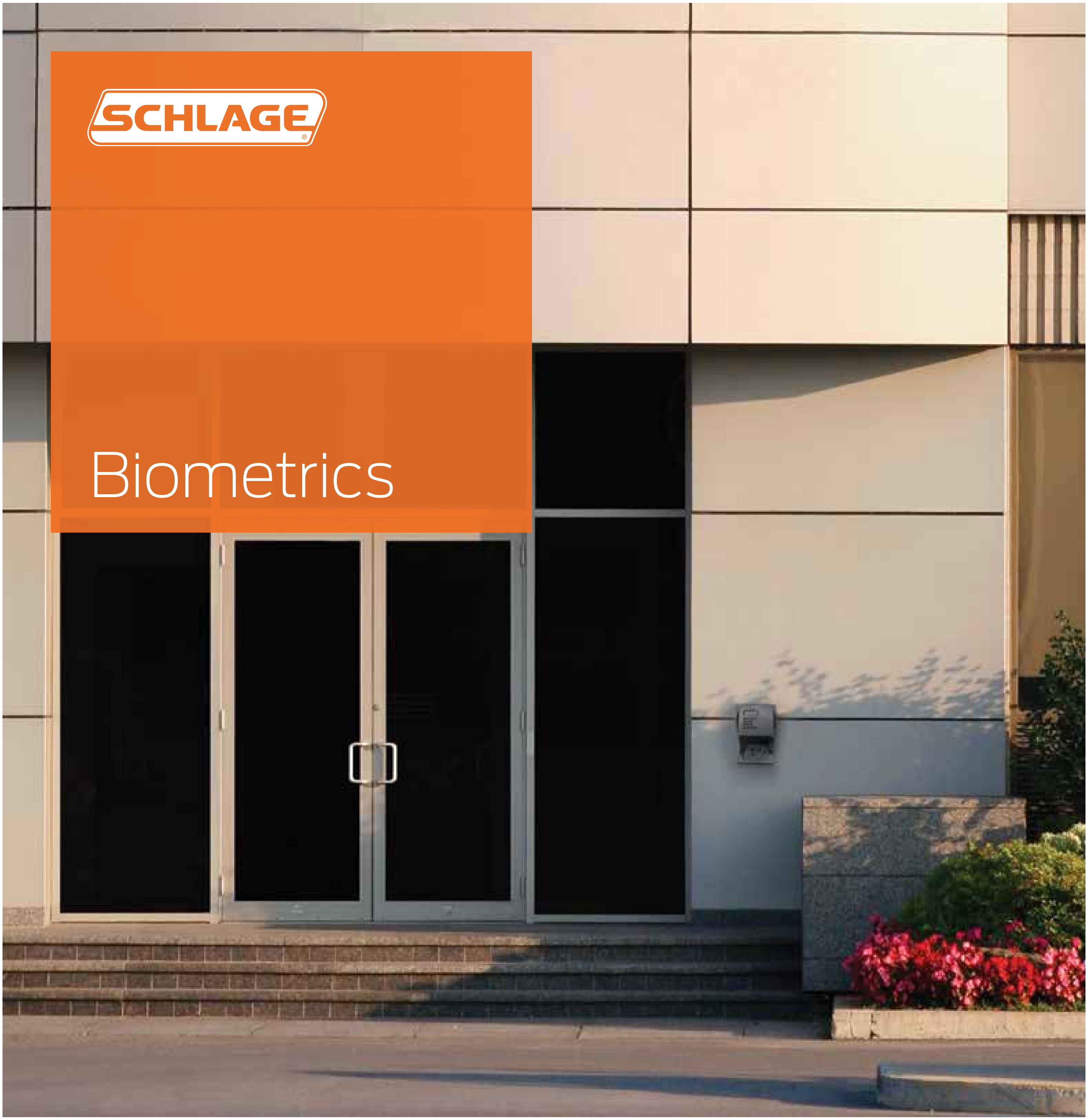
7. **Q: My employees are concerned about hygiene issues. How do I address this concern?**
   A: Every HandReader contains antimicrobial technology which inhibits the growth of a broad spectrum of bacteria, mold, and fungi, making the platen’s surface more hygienic. This silver-based agent is embedded into the materials used to produce the platen during the manufacturing process. As such, they cannot leach out or wash off the surface thus remain active for the life of the biometric reader. Schlage Biometrics has been providing HandReaders for more than 20 years. Everyday several hundred thousand hand geometry units are used by millions of people in applications like day care centers, athletic clubs, hotels, manufacturing facilities, government installations, education facilities, quick serve restaurants, and grocery stores globally. Schlage Biometric HandReaders have a proven track record in the field and are the durable and reliable biometric you can count on.

8. **Q: Are there any privacy issues?**
   A: The HandReader terminal does not collect and store an image of the hand, but instead it converts the image to a 9-byte numerical template which is a mathematical representation of size and shape of the hand. Once this numerical template is developed it is stored in a memory location which is defined by the person’s ID number. To authenticate a user already verified in the

database, the users ID is entered and their hand is placed on the platen (surface area where users place their hand). An image of the hand is captured and then converted to a 9-byte numerical template. If the new template matches the stored template, the person's identity is verified and the transaction is recorded. No personally-identifiable characteristics such as scars, marks, tattoos, fingerprints or palm prints are captured or detected by the terminal.

9. **Q: Is the HandKey safe?**
   The infrared lights used in the hand reader are similar to those used in remote controls for TV's and VCR's. Internal testing concluded that the light intensity generated by the infrared lights in the HandReader is significantly less than the light intensity generated by direct sunlight. Using a HandReader for 30 seconds a day is comparable to standing in the sun for 0.2 seconds. Schlage Biometrics has submitted HandReader information to the U.S. Occupational Safety and Health Administration (OSHA). OSHA did not report any hazards. The Federal Communications Commission requires that computers meet sub-part J of Part 15 of FCC rules. This section details radiated energy. Schlage Biometrics has tested to these standards and meets or exceeds them. Schlage Biometrics also meets the requirements of the European Community and is CE

ALLEGION™



Biometrics

Contents

Put your trust in the name you know

For more than 90 years Schlage® has been providing innovative security solutions for schools, hospitals, government facilities and a host of other commercial buildings. Today, Schlage is at the forefront of cutting edge technology with electronic locking, wireless access, biometric and smart card solutions.

With a wide range of products, functions and styles, Schlage has what you need no matter how demanding your application. And we stand behind every product we make with an outstanding service organization that will be with you every step of the way. It's our commitment to design, performance and technology that ensures you can stand behind our products too.

Reliable security with confidence

Schlage biometrics specializes in the development, marketing and service of biometric devices for access control and workforce management applications.

Located in the heart of California's Silicon Valley, Schlage biometrics offers biometric technology as a secure alternative to easily lost or compromised ID cards and PIN numbers. The technology uses hand geometry to verify a person's true identity.

When you choose a Schlage biometrics product, you can be sure that you have done the job right the first time. After all, our products are the most reliable and dependable on the market today. Our HandKey® II is easy to install and simple to maintain. That means fewer service issues for you and low total cost of ownership.

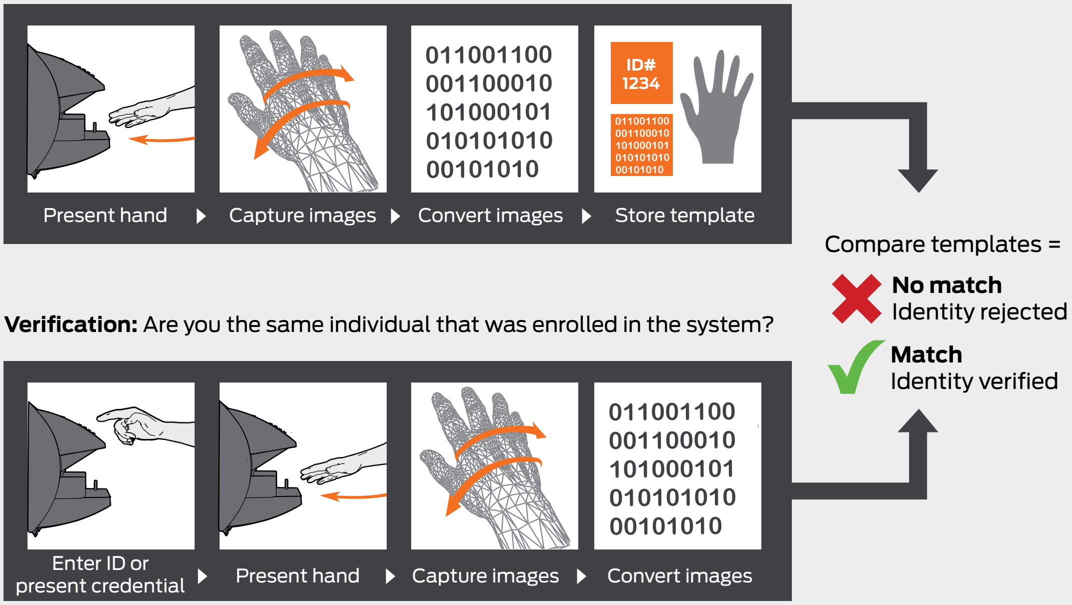
Hand Geometry

Biometric products identify people by analyzing their unique human characteristics. Schlage Hand Geometry readers use field-proven technologies to provide increased security at any door and to ensure that the right person is at the right place at the right time. These technologies are frequently used in universities, data centers, day care centers, airports, health care facilities and government buildings.

Biometric verification

How it works

Enrollment: This adds your biometric template to the HandKey.



Present hand ▸ Capture images ▸ Convert images ▸ Store template

011001100
001100010
101000101
010101010
00101010

ID#
1234

Compare templates =

✗ **No match**
Identity rejected

✓ **Match**
Identity verified

Verification: Are you the same individual that was enrolled in the system?

Enter ID or present credential ▸ Present hand ▸ Capture images ▸ Convert images

011001100
001100010
101000101
010101010
00101010

Top 10 reasons to select Hand Geometry

Field proven reliability

1. Hundreds of thousands of HandKeys are installed all over the world in diverse applications, providing millions of error free transactions every day

Convenience and cost savings

2. Incredibly fast installation and intuitive enrollment increases user convenience
3. Verification in less than one second makes it ideal for high throughput applications
4. High product quality + low maintenance costs = low total cost of ownership
5. Eliminate the worry of lost, stolen or unauthorized transfer of ID cards plus the cost of purchasing and maintaining these cards

Eliminate privacy concerns

6. Hand geometry technology is well accepted by end users, as there are no fingerprints or palm prints taken and the user does not leave behind any trace of their biometric data

Amazing versatility

7. HandKeys can be used as standalone systems to protect critical access points that can be easily integrated into virtually every new or existing access control system in the market today
8. Ability to customize user-specific security levels, time zones, holidays and languages based on your needs
9. Optional access control template management software allows the HandKeys to form a system that communicates alarms and transactions in real time, provides activity reports, allows supervised on-site or remote user enrollment and expiring privileges for temporary access
10. Environmental enclosures and integrated heater units make the HandKey an ideal solution for outdoor usage

Applications

The versatility and flexibility of the HandKeyII lends itself to diverse indoor and outdoor applications.

Critical infrastructure

- Transportation hubs - at airports and shipping ports to grant access to authorized personnel to aircraft/ship operations, baggage handling and other sensitive areas
- Data centers - HandReaders accommodate a large number of users, offer a high level of security, are easy to use, provide for remote enrollment & eliminate the need to carry a card
- Construction facilities - highly robust and user friendly HandReaders operate well in nearly all environmental conditions; unaffected by dirt on the hands, poor lighting conditions, or the worn fingerprints endemic of manual laborers
- They are also installed at various government research facilities
- Prisons - monitor all comings and goings at prisons and eliminate the need for posting guards at all access sites and supplying them with keys
- Military installations - protecting US troops & assets worldwide by providing reliable access to the appropriate personnel

Healthcare facilities

- Pharmacy, surgery, long term care, and research facilities – increase security by providing access to secure areas only to authorized personnel

Financial institutions

- Safe deposit vaults - enhanced security to gain access to safe deposit boxes without the need for personnel to accompany the customer in and out of the vault

Education

- Residence halls - verify students to ensure that only authorized students gain access
- Recreational facilities - minimize people’s ability to transfer IDs and eliminate the need for keys / cards
- Dining halls - limit access to students who have paid for the meal plan
- Computer labs - provide access only to authorized personnel seeking access to sensitive equipment and information

Hospitality

- Lodging - access to high security, high valued openings such as data records and hotel supply areas
- Entertainment - access to high security, high valued openings in casinos, stadiums and theme parks

Commercial buildings

- Specialized high asset areas - access to high security, high valued areas such as IT, HVAC, conference rooms in addition to front doors
- Corporate campuses - provide high security to a variety of restricted areas like management offices and expensive high tech equipment rooms

HandKey II

Our HandKey II product is ideal for applications where consistent and dependable security is of prime importance. The product is easy to maintain, and provides an ideal mix of convenience, security and peace of mind.

In addition to all Hand Geometry benefits, the HandKey II offers:

- Convenience of multiple credential options such as proximity, magnetic stripe, barcode, iCLASS® and MIFARE®
- Field installable Ethernet module
- Outdoor enclosure options that make the HandKey II an ideal solution for outdoor usage
- Field upgradable and expandable memory options from 512 to 259,072 users for scalable security that grows with your needs
- Three user-definable outputs to connect to auxiliary devices such as audible or silent alarms, door locks or lighting systems
- Ability to write the industry's most compact biometric template on a card instead of in a database results in higher security & unlimited user capacity
- Specially formulated antimicrobial coating with silver ions on the platen to inhibit the growth of bacteria, mold and mildew to mitigate hygiene concerns. The coating is safe and lasts for the life of the product
- Blue hand outline on the platen facilitates easy enrollment and reduces error rates during verification

Models, options and accessories

Schlage biometrics offers a number of options and accessories to help you create a solution to meet your specific needs.

Base models	HK-2-F3
Card readers	**Prox:** Externally top mounted HID prox reader, factory option only **HID iCLASS®**: iCLASS reader, factory option only **SC-100**: MIFARE® reader, factory option only **CR-2**: Mag stripe wall mount card reader **BC-100**: Bar code reader, wall mount swipe
Memory	**EM-801-F3**: Field upgradeable memory expansion up to 9,728 users **EM-803-F3**: Field upgradeable memory expansion up to 32,512 users **EM-813-F3**: Memory expansion up to 64,768 users **EM-823-F3**: Memory expansion up to 129,536 users **EM-833-F3**: Memory expansion up to 194,304 users **EM-843-F3**: Memory expansion up to 259,072 users
Communication	**EN-200**: Field upgradeable Ethernet communication module 10baseT **MD-500**: Internal dial-up modem
Power options	**PS-110**: Power supply, 120VAC to 13.5 VDC **PS-220**: Power supply, 220VAC to 13.5 VDC **BB-200**: Optional battery backup
Mounting	**TM-100**: Table top secure mount for flat surfaces
Left hand option	N/A
Network accessories	**DC-102**: Data converter for 4 wire system, RS-232 to RS-422 with 120V, 60Hz power supply **DC-102 with 220V:** 50Hz power supply **DC-104**: Data converter for 2 or 4 wire systems, RS232 to RS485/RS 422 with 120V, 60Hz power supply **DC-104 with 220V:** 50Hz power supply

Specifications for the HandKey Series

Base models	HK-2-F3
Description	HandReader with base memory for 512 users
Verification time	≤ 1 second for comparison to reference
ID number length	1 – 10 digits
Duress code	1 leading digit, user definable
Communication	**RS-232**: Baud rate 300 bps to 28,800 bps **RS-422**: Baud rate 300 bps to 28,800 bps **RS-485**: Baud rate 300 bps to 28,800 bps **Optional Modem**: Baud rate 300 bps to 14,400 bps **Optional Ethernet**: 10 Base T
Template size	9 bytes
User memory	512 users expandable to 259, 072 users
Inputs	**Standard**: 26 bit, 9 bit ID Wiegand **Optional**: Mag stripe, bar code, smart card **HandKey input**: Request-to-exit, door switch input, 2 auxiliary inputs
Outputs	**Door control**: Lock output **Card reader emulation mode**: Wiegand, mag stripe, bar code 1 programmable auxiliary **Outputs to peripheral devices**: Audible or silent alarms, door locks, lighting systems
Event monitoring	**Tamper**: HandKey opened or removed **ID refused**: User not verified after user definable number of tries exceeded **Duress**: User entered duress code digit **Power failure**: HandKey switched to optional battery power
Programmable HandKey commands	▪ Add/remove users ▪ Set global operating thresholds ▪ Set individual user data (authority or threshold levels, time zones) ▪ Transmit data from master to remote ▪ Data received by master from remote ▪ Transmit/receive data from optional software ▪ Check status of door (tamper, door monitor switch) ▪ Time zones – 62 total (2 fixed, 60 programmable) ▪ Set language ▪ Set date format, date and time ▪ Edit holidays
Antimicrobial	Available on platen
Blue hand outline	Available on platen
Dimensions H x W x D	11.65 in x 8.85 in x 8.55 in 29.6 cm x 22.5 cm x 21.7 cm
Power requirements	12 to 24 VDC or 12 to 24 VAC 50-60 Hz 7 Watts (without options)
Weight	5.3 lbs. (2.4kgs.) (without battery back-up or wall plate)
Temperature	Operating: 0° C to +45° C / 32° F to 113° F Non-operating (storage): -10° C to +60° C / 14° F to 140° F
Relative humidity	Operating: 20% to 80% RH Non-condensing Non-operating (storage): 5% to 85% RH non-condensing

A biometric that works indoors and outdoors

Schlage biometrics provides various options to protect your HandKey II from the elements. Two different, proven solutions are available to ensure your HandKey II keeps performing regardless of your environment.

FX enclosure

Biometric HandKey enclosure

Constructed from high impact UV resistant polycarbonate material, the FX enclosure provides a degree of protection against dusty, dirty, or rainy environments. This enclosure has been designed so that it can be added to an existing installation. When used with an integrated heater option (INT-HTR), it provides a comfortable heated platen against a cold climate.

TX enclosure

Biometric HandKey enclosure

The TX ~~E~~nclosure provides a higher degree of protection against dusty, dirty, or rainy environments. When used with an integrated heater option (INT-HTR), it provides a comfortable heated platen against a cold climate.

	~~FX enclosure~~	~~TX enclosure~~
Temperature range	-20F to 120F -29C to 49C	-45F to 120F -43C to 49C
Dimensions H x W x D	14.75" x 12.00" x 10.50" 37.5 cm x 30.5 cm x 26.7 cm	23.00" x 14.00" x 11.25" 58.4 cm x 35.6 cm x 28.6 cm
Gross weight	7.3 lbs / 3.3 kg	45.0 lbs / 20.4 kg
HandKey models	HK-2-F3	HK-2-F3
Heater	Factory installed option only, model no. INT-HTR	Factory installed option only, model no. INT-HTR

HandNet for Windows

HandNet for Windows lets you control and monitor a network of HandKey II readers. With just one comprehensive program, you can monitor activity and alarms on all readers, and control the access of each user.

- Automatic hand template management feature allows template distribution from enrollment HandKey II to other selected HandReaders thus eliminating the need for a user to be enrolled at every HandKey II
- Independent door control capability without the need for an access control panel
- Monitor multiple remote sites from the convenience of your PC
- Remote enrollment feature enables a HandKey II to be controlled from the software. For example a guard behind a glass partition or a supervisor in a distant office can enroll new users without physically going to the HandKey II
- Assign temporary access to selected users by specifying a user's access start and stop days and times
- Manage archive activity to keep old information available for reports
- Manage alarms for additional security

Models	**HN-2-T1**	**HN-2-T2**	**HN-2-T3**	**HandNet Lite**
Description	Manages up to 5 HandKeys	Manages up to 25 HandKeys	Manages an UNLIMITED number of HandKeys	Manage the Handkey II without access control software functionalities

Specifications for software

Base models	HandNet for Windows	HandNet Lite
Computer	Intel Pentium 1 GHz or higher, AMD Athlon 1 GHz or higher	Intel Pentium 1 GHz or higher, AMD Athlon 1 GHz or higher
Operating system	Windows XP SP3 32 bit, Windows 7 Professional SP1 32-bit and 64-bit	Windows XP SP3 32 bit, Windows 7 Professional SP1 32-bit and 64-bit, Windows Server 2003 SP2 32-bit
Drives	CD Rom for installation	CD Rom for installation
Hard disk	2 GB minimum, 1 GB free space	60 GB minimum, 10 GB free space
Monitor	Minimum resolution 1024 x 768	Minimum resolution 1024 x 768
Memory	2 GB (Minimum 1 GB)	4 GB (Minimum 2 GB)
Database	MS Access	MS SQL Server 2000 MSDE
Products supported	HK-2-F3	HK-2-F3
Template management	Available	Available
Supported communications	RS232, RS485, Ethernet	RS232, RS485, Ethernet
Time zones	Available	Available
Reports	Available	Limited - use reports from an access control panel
Door control	Available	N/A - use panel door control
Alarms	Available	N/A - use panel alarms
Open door remotely	Available	N/A - use panel door control
Network readers	Available	Available
Archives activity	Available	Available - database backup
Remote enrollment	Available	Available

Additional Schlage solutions

Workforce management

Schlage HandPunch® terminals utilize Hand Geometry technology to automate Workforce Management systems, control labor costs, eliminate costly badges and cards, reduce compliance risk and stop time fraud.

The HandPunch is a trusted and reliable solution used in a variety of workforce management applications worldwide.

- Hospitality
- Education
- Government
- Manufacturing
- Quick serve restaurants
- Construction
- Grocery
- Healthcare
- Hospitals
- Retail stores

MR: What are the Allegion email addresses?

Order processing
Phone: 877-671-7011, Option 1, Option 8
Fax: 800-452-0665
sbsom@i~~rco.com~~

Technical support
Phone: 877-671-7011, Option 2, Option 8
Readers_Credentials_Biometrics_TechProdSupport@~~irco.com~~

About Allegion

Allegion (NYSE: ALLE) creates peace of mind by pioneering safety and security. As a $2 billion provider of security solutions for homes and businesses, Allegion employs more than 8,000 people and sells products in more than 120 countries across the world. Allegion comprises more than 25 global brands, including strategic brands CISA®, Interflex®, LCN®, Schlage® and Von Duprin®.

For more, visit **www.allegion.com**

ALLEGION™

SCHLAGE®

HandPunch® concerns

When it comes to managing time and attendance systems no other biometric solution compares to the Schlage® HandPunch®. Time after time our customers report the reliability of the HandPunch because it accurately identifies employees in environments where dirt, dust, and wet conditions may limit the accuracy of other biometrics. The HandPunch has been known to pay for itself in less than 9 months, making it an ideal solution to businesses that are trying to control costs due to employee payroll fraud, manual data review and correction time, and payroll error. While the benefits of implementing Schlage HandReaders are many, employees may raise concerns about the way hand geometry technology could affect their privacy rights. Schlage Biometrics understands their concerns and would like to address the issues regarding biometrics that may come up.

HandReaders work by shining a light on the user's hand, taking a picture, and looking at the hand silhouette. The illumination is provided by LEDs similar to the remote control on a TV. Think of it as a flashlight casting a shadow of a hand.

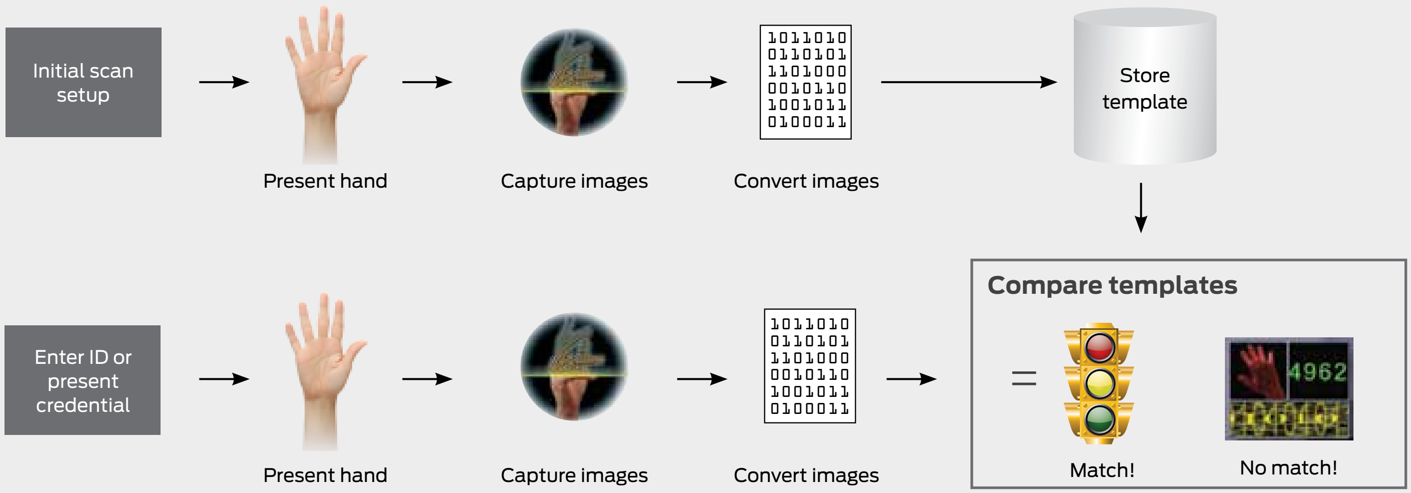
Technology

Geometric measurements of the hand (lengths, widths, areas, and heights) are calculated from the silhouette and then "compressed" by a mathematical formula into a 9-byte numerical template. Since the compression is so high, it is infeasible to reverse-engineer the 9-byte template into the hand image or even the raw geometric measurements of the person that used the HandReader.

Privacy

The HandReader terminal does not collect and store an image of the hand, but instead it converts the image to a 9-byte numerical template which is a mathematical representation of size and shape of the hand. Once this numerical template is developed it is stored in a memory location which is defined by the person's ID number.

To authenticate a user already verified in the database, the user's ID is entered and their hand is placed on the platen (surface area where users place their hand). An image of the hand is captured and then converted to a 9-byte numerical template. If the new template matches the stored template, the person's identity is verified and the transaction is recorded.



No personally-identifiable characteristics such as scars, marks, tattoos, fingerprints or palm prints are captured or detected by the terminal. According to Article 29 from the EU Advisory Body on Data Protection and Privacy: “biometric systems… which do not leave traces (e.g. shape of the hand but not fingerprints)… create less risks for the protection for fundamental rights and freedoms of individuals.”

Religion

Since the HandReader is not capable of personally-identifiable characteristics, HandReaders do not in any way have the ability to place or detect the “Mark of the Beast” or any other mark on a person’s hand. Many religious organizations and churches trust the HandReader every day to accurately and efficiently manage their time and attendance systems.

Safety

The infrared lights used in the HandReader are similar to those used in remote controls for TV’s and VCR’s. Internal testing concluded that the light intensity generated by the infrared lights in the HandReader is significantly less than the light intensity generated by direct sunlight. Using a HandReader for 30 seconds a day is comparable to standing in the sun for 0.2 seconds.

Schlage Biometrics has submitted HandReader information to the U.S. Occupational Safety and Health Administration (OSHA). OSHA did not report any hazards.

The Federal Communications Commission requires that computers meet sub-part J of Part 15 of FCC rules. This section details radiated energy. Schlage Biometrics has tested to these standards and meets the requirements of the European Community and is CE Certified.

Hygiene

Every HandReader contains antimicrobial technology which inhibits the growth of a broad spectrum of bacteria, mold, and fungi, making the platen’s surface cleaner and more hygienic. This silver-based agent is embedded into the materials used to produce the platen during the manufacturing process. Therefore, the antimicrobial surface remains active for the life of the biometric reader.

Schlage Biometrics has been providing HandReaders for more than 20 years. Every day several hundred thousand hand geometry units are used by millions of people in applications like day care centers, athletic clubs, hotels, manufacturing facilities, government installations, education facilities, and long-term care facilities globally. Schlage Biometric HandReaders have a proven track record in the field and are the durable and reliable biometric you can count on.

About Allegion

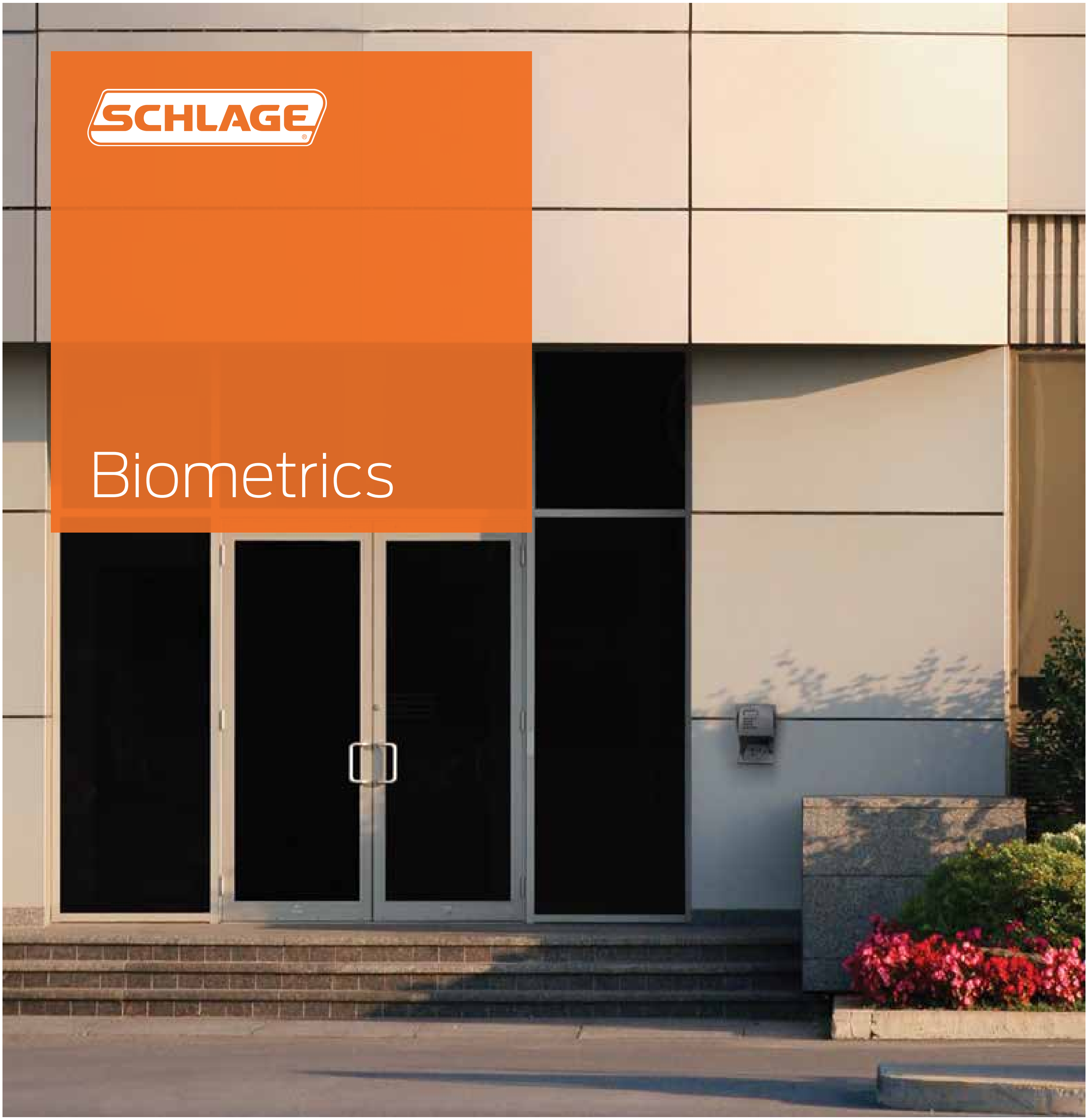
Allegion (NYSE: ALLE) creates peace of mind by pioneering safety and security. As a $2 billion provider of security solutions for homes and businesses, Allegion employs more than 8,000 people and sells products in more than 120 countries across the world. Allegion comprises more than 25 global brands, including strategic brands CISA®, Interflex®, LCN®, Schlage® and Von Duprin®. For more, visit **www.allegion.com.**

aptiQ ■ LCN ■ SCHLAGE ■ STEELCRAFT ■ VON DUPRIN

ALLEGION™

006228, Rev. 10/14
www.allegion.com/us

ALLEGION™



SCHLAGE®

Biometrics

Contents

Put your trust in the name you know

For more than 90 years Schlage® has been providing innovative security solutions for schools, hospitals, government facilities and a host of other commercial buildings. Today, Schlage is at the forefront of cutting edge technology with electronic locking, wireless access, biometric and smart card solutions.

With a wide range of products, functions and styles, Schlage has what you need no matter how demanding your application. And we stand behind every product we make with an outstanding service organization that will be with you every step of the way. It's our commitment to design, performance and technology that ensures you can stand behind our products too.

Reliable security with confidence

Schlage biometrics specializes in the development, marketing and service of biometric devices for access control and workforce management applications.

Located in the heart of California's Silicon Valley, Schlage biometrics offers biometric technology as a secure alternative to easily lost or compromised ID cards and PIN numbers. The technology uses hand geometry to verify a person's true identity.

When you choose a Schlage biometrics product, you can be sure that you have done the job right the first time. After all, our products are the most reliable and dependable on the market today. Our HandKey® II is easy to install and simple to maintain. That means fewer service issues for you and low total cost of ownership.

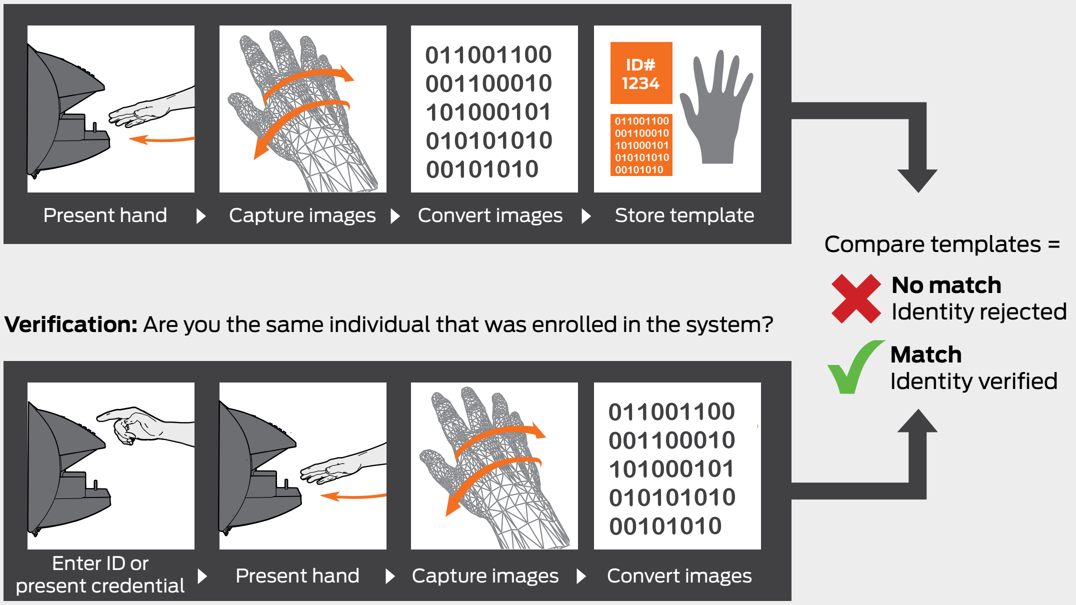
Hand Geometry

Biometric products identify people by analyzing their unique human characteristics. Schlage Hand Geometry readers use field-proven technologies to provide increased security at any door and to ensure that the right person is at the right place at the right time. These technologies are frequently used in universities, data centers, day care centers, airports, health care facilities and government buildings.

Biometric verification

How it works

Enrollment: This adds your biometric template to the HandKey.



Present hand ▸ Capture images ▸ Convert images ▸ Store template

Compare templates =

No match
Identity rejected

Match
Identity verified

Verification: Are you the same individual that was enrolled in the system?

Enter ID or present credential ▸ Present hand ▸ Capture images ▸ Convert images

Top 10 reasons to select Hand Geometry

Field proven reliability

1. Hundreds of thousands of HandKeys are installed all over the world in diverse applications, providing millions of error free transactions every day

Convenience and cost savings

2. Incredibly fast installation and intuitive enrollment increases user convenience
3. Verification in less than one second makes it ideal for high throughput applications
4. High product quality + low maintenance costs = low total cost of ownership
5. Eliminate the worry of lost, stolen or unauthorized transfer of ID cards plus the cost of purchasing and maintaining these cards

Eliminate privacy concerns

6. Hand geometry technology is well accepted by end users, as there are no fingerprints or palm prints taken and the user does not leave behind any trace of their biometric data

Amazing versatility

7. HandKeys can be used as standalone systems to protect critical access points that can be easily integrated into virtually every new or existing access control system in the market today
8. Ability to customize user-specific security levels, time zones, holidays and languages based on your needs
9. Optional access control template management software allows the HandKeys to form a system that communicates alarms and transactions in real time, provides activity reports, allows supervised on-site or remote user enrollment and expiring privileges for temporary access
10. Environmental enclosures and integrated heater units make the HandKey an ideal solution for outdoor usage

Applications

The versatility and flexibility of the HandKeyII lends itself to diverse indoor and outdoor applications.

Critical infrastructure

- Transportation hubs - at airports and shipping ports to grant access to authorized personnel to aircraft/ship operations, baggage handling and other sensitive areas
- Data centers - HandReaders accommodate a large number of users, offer a high level of security, are easy to use, provide for remote enrollment & eliminate the need to carry a card
- Construction facilities - highly robust and user friendly HandReaders operate well in nearly all environmental conditions; unaffected by dirt on the hands, poor lighting conditions, or the worn fingerprints endemic of manual laborers
- They are also installed at various government research facilities
- Prisons - monitor all comings and goings at prisons and eliminate the need for posting guards at all access sites and supplying them with keys
- Military installations - protecting US troops & assets worldwide by providing reliable access to the appropriate personnel

Healthcare facilities

- Pharmacy, surgery, long term care, and research facilities – increase security by providing access to secure areas only to authorized personnel

Financial institutions

- Safe deposit vaults - enhanced security to gain access to safe deposit boxes without the need for personnel to accompany the customer in and out of the vault

Education

- Residence halls - verify students to ensure that only authorized students gain access
- Recreational facilities - minimize people's ability to transfer IDs and eliminate the need for keys / cards
- Dining halls - limit access to students who have paid for the meal plan
- Computer labs - provide access only to authorized personnel seeking access to sensitive equipment and information

Hospitality

- Lodging - access to high security, high valued openings such as data records and hotel supply areas
- Entertainment - access to high security, high valued openings in casinos, stadiums and theme parks

Commercial buildings

- Specialized high asset areas - access to high security, high valued areas such as IT, HVAC, conference rooms in addition to front doors
- Corporate campuses - provide high security to a variety of restricted areas like management offices and expensive high tech equipment rooms

HandKey II

Our HandKey II product is ideal for applications where consistent and dependable security is of prime importance. The product is easy to maintain, and provides an ideal mix of convenience, security and peace of mind.

In addition to all Hand Geometry benefits, the HandKey II offers:

- Convenience of multiple credential options such as proximity, magnetic stripe, barcode, iCLASS® and MIFARE®
- Field installable Ethernet module
- Outdoor enclosure options that make the HandKey II an ideal solution for outdoor usage
- Field upgradable and expandable memory options from 512 to 259,072 users for scalable security that grows with your needs
- Three user-definable outputs to connect to auxiliary devices such as audible or silent alarms, door locks or lighting systems
- Ability to write the industry's most compact biometric template on a card instead of in a database results in higher security & unlimited user capacity
- Specially formulated antimicrobial coating with silver ions on the platen to inhibit the growth of bacteria, mold and mildew to mitigate hygiene concerns. The coating is safe and lasts for the life of the product
- Blue hand outline on the platen facilitates easy enrollment and reduces error rates during verification

Models, options and accessories

Schlage biometrics offers a number of options and accessories to help you create a solution to meet your specific needs.

Base models	HK-2-F3
Card readers	**Prox:** Externally top mounted HID prox reader, factory option only **HID iCLASS**®: iCLASS reader, factory option only **SC-100**: MIFARE® reader, factory option only **CR-2**: Mag stripe wall mount card reader **BC-100**: Bar code reader, wall mount swipe
Memory	**EM-801-F3**: Field upgradeable memory expansion up to 9,728 users **EM-803-F3**: Field upgradeable memory expansion up to 32,512 users **EM-813-F3**: Memory expansion up to 64,768 users **EM-823-F3**: Memory expansion up to 129,536 users **EM-833-F3**: Memory expansion up to 194,304 users **EM-843-F3**: Memory expansion up to 259,072 users
Communication	**EN-200**: Field upgradeable Ethernet communication module 10baseT **MD-500**: Internal dial-up modem
Power options	**PS-110**: Power supply, 120VAC to 13.5 VDC **PS-220**: Power supply, 220VAC to 13.5 VDC **BB-200**: Optional battery backup
Mounting	**TM-100**: Table top secure mount for flat surfaces
Left hand option	N/A
Network accessories	**DC-102**: Data converter for 4 wire system, RS-232 to RS-422 with 120V, 60Hz power supply **DC-102 with 220V:** 50Hz power supply **DC-104**: Data converter for 2 or 4 wire systems, RS232 to RS485/RS 422 with 120V, 60Hz power supply **DC-104 with 220V:** 50Hz power supply

Specifications for the HandKey Series

Base models	HK-2-F3
Description	HandReader with base memory for 512 users
Verification time	≤ 1 second for comparison to reference
ID number length	1 – 10 digits
Duress code	1 leading digit, user definable
Communication	**RS-232**: Baud rate 300 bps to 28,800 bps **RS-422**: Baud rate 300 bps to 28,800 bps **RS-485**: Baud rate 300 bps to 28,800 bps **Optional Modem**: Baud rate 300 bps to 14,400 bps **Optional Ethernet**: 10 Base T
Template size	9 bytes
User memory	512 users expandable to 259, 072 users
Inputs	**Standard**: 26 bit, 9 bit ID Wiegand **Optional**: Mag stripe, bar code, smart card **HandKey input**: Request-to-exit, door switch input, 2 auxiliary inputs
Outputs	**Door control**: Lock output **Card reader emulation mode**: Wiegand, mag stripe, bar code 1 programmable auxiliary **Outputs to peripheral devices**: Audible or silent alarms, door locks, lighting systems
Event monitoring	**Tamper**: HandKey opened or removed **ID refused**: User not verified after user definable number of tries exceeded **Duress**: User entered duress code digit **Power failure**: HandKey switched to optional battery power
Programmable HandKey commands	▪ Add/remove users ▪ Set global operating thresholds ▪ Set individual user data (authority or threshold levels, time zones) ▪ Transmit data from master to remote ▪ Data received by master from remote ▪ Transmit/receive data from optional software ▪ Check status of door (tamper, door monitor switch) ▪ Time zones – 62 total (2 fixed, 60 programmable) ▪ Set language ▪ Set date format, date and time ▪ Edit holidays
Antimicrobial	Available on platen
Blue hand outline	Available on platen
Dimensions H x W x D	11.65 in x 8.85 in x 8.55 in 29.6 cm x 22.5 cm x 21.7 cm
Power requirements	12 to 24 VDC or 12 to 24 VAC 50-60 Hz 7 Watts (without options)
Weight	5.3 lbs. (2.4kgs.) (without battery back-up or wall plate)
Temperature	Operating: 0° C to +45° C / 32° F to 113° F Non-operating (storage): -10° C to +60° C / 14° F to 140° F
Relative humidity	Operating: 20% to 80% RH Non-condensing Non-operating (storage): 5% to 85% RH non-condensing

A biometric that works indoors and outdoors

Schlage biometrics provides various options to protect your HandKey II from the elements. Two different, proven solutions are available to ensure your HandKey II keeps performing regardless of your environment.

FX enclosure

Biometric HandKey enclosure

Constructed from high impact UV resistant polycarbonate material, the FX enclosure provides a degree of protection against dusty, dirty, or rainy environments. This enclosure has been designed so that it can be added to an existing installation. When used with an integrated heater option (INT-HTR), it provides a comfortable heated platen against a cold climate.

TX enclosure

Biometric HandKey enclosure

The TX ~~E~~nclosure provides a higher degree of protection against dusty, dirty, or rainy environments. When used with an integrated heater option (INT-HTR), it provides a comfortable heated platen against a cold climate.

	~~FX enclosure~~	~~TX enclosure~~
Temperature range	-20F to 120F -29C to 49C	-45F to 120F -43C to 49C
Dimensions H x W x D	14.75" x 12.00" x 10.50" 37.5 cm x 30.5 cm x 26.7 cm	23.00" x 14.00" x 11.25" 58.4 cm x 35.6 cm x 28.6 cm
Gross weight	7.3 lbs / 3.3 kg	45.0 lbs / 20.4 kg
HandKey models	HK-2-F3	HK-2-F3
Heater	Factory installed option only, model no. INT-HTR	Factory installed option only, model no. INT-HTR

HandNet for Windows

HandNet for Windows lets you control and monitor a network of HandKey II readers. With just one comprehensive program, you can monitor activity and alarms on all readers, and control the access of each user.

- Automatic hand template management feature allows template distribution from enrollment HandKey II to other selected HandReaders thus eliminating the need for a user to be enrolled at every HandKey II
- Independent door control capability without the need for an access control panel
- Monitor multiple remote sites from the convenience of your PC
- Remote enrollment feature enables a HandKey II to be controlled from the software. For example a guard behind a glass partition or a supervisor in a distant office can enroll new users without physically going to the HandKey II
- Assign temporary access to selected users by specifying a user's access start and stop days and times
- Manage archive activity to keep old information available for reports
- Manage alarms for additional security

Models	HN-2-T1	HN-2-T2	HN-2-T3	HandNet Lite
Description	Manages up to 5 HandKeys	Manages up to 25 HandKeys	Manages an UNLIMITED number of HandKeys	Manage the Handkey II without access control software functionalities

Specifications for software

Base models	HandNet for Windows	HandNet Lite
Computer	Intel Pentium 1 GHz or higher, AMD Athlon 1 GHz or higher	Intel Pentium 1 GHz or higher, AMD Athlon 1 GHz or higher
Operating system	Windows XP SP3 32 bit, Windows 7 Professional SP1 32-bit and 64-bit	Windows XP SP3 32 bit, Windows 7 Professional SP1 32-bit and 64-bit, Windows Server 2003 SP2 32-bit
Drives	CD Rom for installation	CD Rom for installation
Hard disk	2 GB minimum, 1 GB free space	60 GB minimum, 10 GB free space
Monitor	Minimum resolution 1024 x 768	Minimum resolution 1024 x 768
Memory	2 GB (Minimum 1 GB)	4 GB (Minimum 2 GB)
Database	MS Access	MS SQL Server 2000 MSDE
Products supported	HK-2-F3	HK-2-F3
Template management	Available	Available
Supported communications	RS232, RS485, Ethernet	RS232, RS485, Ethernet
Time zones	Available	Available
Reports	Available	Limited - use reports from an access control panel
Door control	Available	N/A - use panel door control
Alarms	Available	N/A - use panel alarms
Open door remotely	Available	N/A - use panel door control
Network readers	Available	Available
Archives activity	Available	Available - database backup
Remote enrollment	Available	Available

Additional Schlage solutions

Workforce management

Schlage HandPunch® terminals utilize Hand Geometry technology to automate Workforce Management systems, control labor costs, eliminate costly badges and cards, reduce compliance risk and stop time fraud.

The HandPunch is a trusted and reliable solution used in a variety of workforce management applications worldwide.

- Hospitality
- Education
- Government
- Manufacturing
- Quick serve restaurants
- Construction
- Grocery
- Healthcare
- Hospitals
- Retail stores

MR: What are the Allegion email addresses?

Order processing
Phone: 877-671-7011, Option 1, Option 8
Fax: 800-452-0665
sbsom@i~~rco.com~~

Technical support
Phone: 877-671-7011, Option 2, Option 8
Readers_Credentials_Biometrics_TechProdSupport@~~irco.com~~

About Allegion

Allegion (NYSE: ALLE) creates peace of mind by pioneering safety and security. As a $2 billion provider of security solutions for homes and businesses, Allegion employs more than 8,000 people and sells products in more than 120 countries across the world. Allegion comprises more than 25 global brands, including strategic brands CISA®, Interflex®, LCN®, Schlage® and Von Duprin®.

For more, visit **www.allegion.com**

NUCLEUS RESEARCH

GUIDEBOOK

ALLEGION: SCHLAGE HANDPUNCH GUIDEBOOK

July 2014

Document o170

Nucleus Research is the leading provider of value-focused technology research and advice.

NucleusResearch.com

THE BOTTOM LINE

Using biometrics to automate collection of time and attendance data can reduce buddy punching, manual data review, correction time, and payroll error. The Schlage HandPunch gives customers a reliable and industrial option over other biometrics, delivering additional operational benefits by using hand geometry to increase reliability and reduce privacy concerns. Customers maximizing the full potential of the technology can realize payback periods of less than 9 months facilitated through reduced errors, reduced or eliminated systems and materials costs, increased productivity, improved reporting and data visibility, along with reduced compliance risk.

THE SOLUTION

The Schlage HandPunch is a biometric terminal system for time punch entry and record generation used in conjunction with workforce management and human capital management software. The terminal uses hand geometry to verify an employee's identity, eliminating invasive measures such as fingerprint matching or facial recognition used by more conventional biometric terminals. The company's terminal gives customers the benefits associated with employee verification for records management.

To use the terminal, employees enter a PIN or code and place their hand to generate a recorded time punch associated with the time of day. Features of the HandPunch include:

- Employee messaging and self-service. The terminal can be configured to display messages and menus specific to each employee and referenced by their ID. Keys can also be defined to let employees view and enter requests and update information.
- Clock-based editing. Managers can enter a password to modify data entry points without the need to access a computer.
- Bell and door scheduling. Employers can manage shifts and breaks while controlling access to facilities.
- Data integration. Data stored and used in the terminals to identify and access employment records can integrate directly with other applications in HR and payroll to ensure accuracy and reduce manual data review.

WHY SCHLAGE HANDPUNCH

Payroll is a significant source of operating costs for all companies and a small percent change in payroll error can be the difference of finishing a pay period profitably or in the red. Companies have and are investing in workforce management systems (WFM) that improve payroll accuracy. While WFM traditionally mitigates the risk of errors in reporting and cost analysis, standalone enterprise software based on sign-in sheets, time punches, or schedule verifications can be error prone, slow, and incapable of reducing the risk associated with not validating an employee ID.

The Schlage HandPunch uses hand geometry to improve the accuracy of time and attendance, eliminating the possibility of productivity cost drains caused by actions such as buddy punching – the practice of one employee signing in or out for another. While other terminals identify users through palm prints, fingerprints, or iris scans, the HandPunch registers the size and shape of an employee's hand, stores it in the system, and runs a verification match from the database to match an employee to his or her corresponding user record. The technology's use of geometry removes the invasive and often unreliable genetic identification techniques used by other systems, opting instead for large-scale measurements that require less precision to produce a higher level of accuracy in verification.

KEY BENEFITS

Nucleus found that companies using the Schlage HandPunch realized several benefits that result in cost savings over the term of use. Key direct benefits include reduced errors and reduced materials costs, while key indirect benefits include increased productivity, increased data visibility, and reduced compliance risk.

REDUCED ERRORS

Reliable biometrics reduce the risk of employees altering time clock and payroll-related information. As a result, companies can drive down the potential of buddy punching, manipulation of rounding rules, and employee location disputes that arise around legal length of time for donning and doffing and permitted overtime. The average payroll error rate amounts to 1.2 percent of payroll and automating time and attendance and ensuing accuracy serves to reduce this rate. One customer found that moving from paper time cards that could not determine one user from another to the HandPunch system significantly reduced buddy punching. Other customers also found that moving from electronic badge systems to the new system reduced the risk that an employee would lose or forget a badge.

The average payroll error rate amounts to 1.2 percent of payroll and automating time and attendance and ensuring accuracy serves to reduce this rate.

Customers noted:

- *"People will use any excuse when they're late but because the HandPunch was more reliable than fingerprint scanning, I mandated the use of the HandPunch: You will prove to me in the system that you were here or you will not get paid. We still monitor the* *clocks but I know we've saved a fair amount on payroll overpayments because employees believe they will be caught."*

- *"We had problems monitoring time in and out accuracy. It used to take managers away from their other tasks to have to manage it. We tried different methods and ultimately the HandPunch made it so we didn't need a lot of direct oversight to reduce our cost of managing or eliminating errors. No one can punch in or out for another employee letting us see where, when, and how employees are on the clock and it is that simple."*

Customers also found that the HandPunch terminal's use of hand geometry proved more reliable than fingerprint scans, or handprints. Nucleus identified the following advantages of the increased reliability that contributed to fewer errors in timestamp reporting:

- The HandPunch takes an image from multiple angles and relies on visible details while a fingerprint relies on small-scale details that are subjected to environmental conditions such as dirty fingerprints or smudged scanners.
- The HandPunch updates itself based on a built-in biometric template for each user over, adjusting as users' change either from self-induced causes such as weight loss or gain, or from natural causes such as temperature changes or injuries.

One customer found that:

- *"We work in a manufacturing environment and dirt is not uncommon. It's very common for people to have dirty hands from working in the plant all day and with a fingerprint scanner, I had to stand out there every day because there were so many errors."*

REDUCED OR ELIMINATED SYSTEMS AND MATERIALS COSTS

Companies that moved from paper time cards or badge recognition systems to automated terminal units with biometrics eliminated the cost of time cards and badges that average 5 cents per card and 15 cents per badge. Additionally, they eliminated the cost of storing time cards for payroll records and supporting badge systems inclusive of the cost of replacing worn, lost, or stolen badges.

Companies that moved from paper time cards or badge recognition systems to automated terminal units with biometrics eliminated the cost of time cards and badges that average 5 cents per card and 15 cents per badge.

One customer commented:

- *"Employees would come to us having either lost, torn, or demagnetized their badges. We had gone to a new system from timecards because those would get lost, mishandled, or torn and we now had a more expensive resource to keep in inventory. The switch to the new terminal eliminated that without much risk of bad entries."*

INCREASED PRODUCTIVITY

Organizations using the HandPunch reduced the time required for employee identification and punching in and out. The system requires fewer materials to engage the system eliminating objects such as time cards and badges that stand between end users and accessing the terminal. It also reduces the time that HR spends in the back office matching schedules to time punches, supervising the time punch process, and verifying overtime ahead of signing off on payroll.

HandPunch users take advantage of the technology's benefits, realizing productivity increases in a number of areas including:

- Improved management productivity. Automated data entry eliminated the need for manual data reviews and individual amendments to employee records and time stamp entries. The biometric also increases the rate of accuracy in accessibility making it easier for managers to compile and review employee records, and for departmental heads to focus on actionable activities instead of spending time approving timecards.

One customer using a basic terminal noted:

- *"Even though the clock added the hours, they had to be scrutinized. It became an outdated thing."*

- Improved employee productivity. Rapid, reliable timekeeping ensured that employees spent more time on the job and less time entering timestamps. Basic, automated time clocks depended on employees keeping their personal ID cards accessible and in good form; characteristics that more often than not resulted in lost, forgotten, or damaged badges. Deploying the HandPunch accelerated the time punch process, decreasing the amount of time employees spent entering time and attendance data and increasing the amount of time they put into their primary role.

One customer found that:

- *"Most of the time when our people are leaving, it's all at the same time… and they would try to stop working to try to be first to punch out so they didn't have to wait. [The] HandPunch takes only 30 seconds a person, and most of that time is people remembering their ID number and entering it."*

- Improved administration. Automating payroll and time and attendance using biometrics also reduces overall payroll administration time. One organization found that it was able to redeploy more than one quarter of an HR staff member's time to other activities by eliminating management of paper time cards. Another organization reported that employees were able to save more than 30 hours per week reviewing time cards and processing timesheets.

Automated payroll and attendance with biometrics allowed redeployment of HR staff time to other activities by eliminating paper time cards at times by more than ¼. Employees could reduce the time needed to review and process timesheets by up to 30 hours per week.

INCREASED DATA ACCESSIBILITY

Automated data collection and timestamp entry with the HandPunch increased manager visibility into employee work habits and locations. As a result, organizations realized improved monitoring as well as improved audit capabilities. One company found that management could increase the rate at which they identified missing punches or punches where the start and finish locations did not match, establish the reasoning, and resolve the data conflict. Another company found that facilitating immediate access to all of the information in their HRIS system through the HandPunch let managers determine if an employee began their day in one department and finished in another.

One customer noted:

- *"In our organization, employees float between different departments. We would often find out after the fact that they were clocking in and out in departments they weren't scheduled to be working in that day. The HandPunch let us match the location to the punch to understand where employees were using the system to prompt us to find out why."*

The technology also lets managers perform weekly reviews of employee activity to see if staff members have erratic work hours or habits that can be detrimental to employee engagement, customer engagement, and employee-driven business outcomes. The system recorded more accurate and precise data that improved payroll budgeting projections, enabled managers to allocate employee resources more effectively, and decreased the time needed to resolve audits and discrepancies. Nucleus also found that greater visibility for both managers and employees reduced employee concerns about favoritism in scheduling and employee timestamp corrections.

REDUCED COMPLIANCE RISK

Companies found that using an accurate, auditable time and attendance tracking system reduced their risk of cost overages and fines caused by non-compliance measures. It also reduced the amount of time managers spent managing compliance risks and ensuring that internal labor practices in scheduling aligned with FLSA, FMLA, ACA, union, state, local, and other federal rules and regulations. Companies reported compliance to be the largest operational cost after labor, direct inventory and facilities. Compliance costs are not readily known up front and are subject to change throughout a calendar year leaving many HR departments in the dark about the size of their actual risk. While the HandPunch terminals do not report the cost of the risk, they enabled customers to manage individual employees' labor hours through unbiased reporting to ensure that designated, known rules were being followed. As a result, managers were able to access data to minimize the up-front risk of non-compliance and eligibility verification costs for irregularly scheduled employees.

One customer noted:

- *"To employees, a punch in or out is just adding time for pay. To us, we have to be careful about accuracy so we don't run into compliance risks. [The] HandPunch gave us that added layer against basic errors like buddy punching or slipping in some added time that could cause us big problems with government rules and pay amounts."*

KEY COST AREAS

The main cost area for the HandPunch was the initial hardware investment. Other areas reported by customers included:

- Integration. Schlage has several business partners that can integrate with the software forming the user interface in the technology but integration with other systems may be necessary to connect the time and attendance data to the central HRIS for payroll reporting. Customers typically run into added costs for this in the way of consulting provided by their existing HRIS or payroll provider when they are implementing the HandPunch after deploying their HRIS or payroll solutions.
- Personnel. Initial personnel time was required to support implementation of the technology and manage the integration with existing HRIS applications. In spite of reports of labor hours spent, Nucleus found that personnel time required was minimal.
- Training. Some basic, initial training was reported for employees and managers to be familiarized with the technology's user interface. Nucleus found that the HandPunch UI was intuitive and that the training time reported was also minimal.

BEST PRACTICES

Maximizing the return of any software or technology investment is up to the practices used to implement and maintain the solution while keeping internal staff fluent in its use. Nucleus found organizations followed a number of best practices to maximize their return on investment with the HandPunch and reduce the amount of time it took to recuperate the cost of the technology.

- Clear communications. Customers reported several concerns surrounding the HandPunch's implementation surrounding employee data privacy, government data sharing, and data use. The HandPunch does not collect fingerprints or palm data and cannot be used with systems such as the Automated Fingerprint Identification System (AFIS) that connects to law enforcement. Companies should communicate this to employees up front and further use it to segue into how hand geometry data will be collected and used inside the company. Implementing seemingly invasive means of tracking raises concerns among employees and manager need to keep the lines of communications open and include employees in the implementation as much as possible without hindering the deployment timeline.

- Test environment. Deploying to a select group of employees to show how the technology can streamline entering a timestamp and tracking absence and leave requests can help identify initial deployment problems, identify security issues, and create an advocacy panel of employees to increase adoptability among the greater workforce.
- Integration management. The more uses of the HandPunch and the data it generates and tracks, the greater the potential ROI. Integrating the system directly into back-end payroll and HR applications can reduce data management time, errors, omissions, and costs, leading to greater savings across multiple solutions and increasing the value of the implementation.

CONCLUSION

As companies look to reduce labor costs and improve operational efficiency, they need to be considering automating time and attendance to return visibility into labor data for more effective and productive management. While many organizations have automated some aspects of workforce management, many remain challenged to produce accuracy and eliminate employee-generated errors such as buddy punching. Nucleus has found that employees are less likely to attempt buddy punching or other fraud if they believe a system is accurate because they cannot argue with a data-driven outcome correlated with other solutions to deliver context for improved accuracy.

Deploying the HandPunch significantly reduces payroll errors associated with accidental and employee-induced errors, delivering significant returns by reducing the cost of payroll. Companjies supporting paper-based, badge-based, or invasive biometric-based systems can eliminate system error costs associated with failed scans, misread scans, lost, damaged, stolen, or forgotten badges, and timecard storage. Nucleus found that deployed properly, the HandPunch can deliver a payback period of less than 9 months, and companies moving from a paper or badge-based system are likely to see an even shorter period driven by elimination of higher materials costs.

ALLEGION™

SCHLAGE®

HandPunch® concerns

When it comes to managing time and attendance systems no other biometric solution compares to the Schlage® HandPunch®. Time after time our customers report the reliability of the HandPunch because it accurately identifies employees in environments where dirt, dust, and wet conditions may limit the accuracy of other biometrics. The HandPunch has been known to pay for itself in less than 9 months, making it an ideal solution to businesses that are trying to control costs due to employee payroll fraud, manual data review and correction time, and payroll error. While the benefits of implementing Schlage HandReaders are many, employees may raise concerns about the way hand geometry technology could affect their privacy rights. Schlage Biometrics understands their concerns and would like to address the issues regarding biometrics that may come up.

HandReaders work by shining a light on the user's hand, taking a picture, and looking at the hand silhouette. The illumination is provided by LEDs similar to the remote control on a TV. Think of it as a flashlight casting a shadow of a hand.

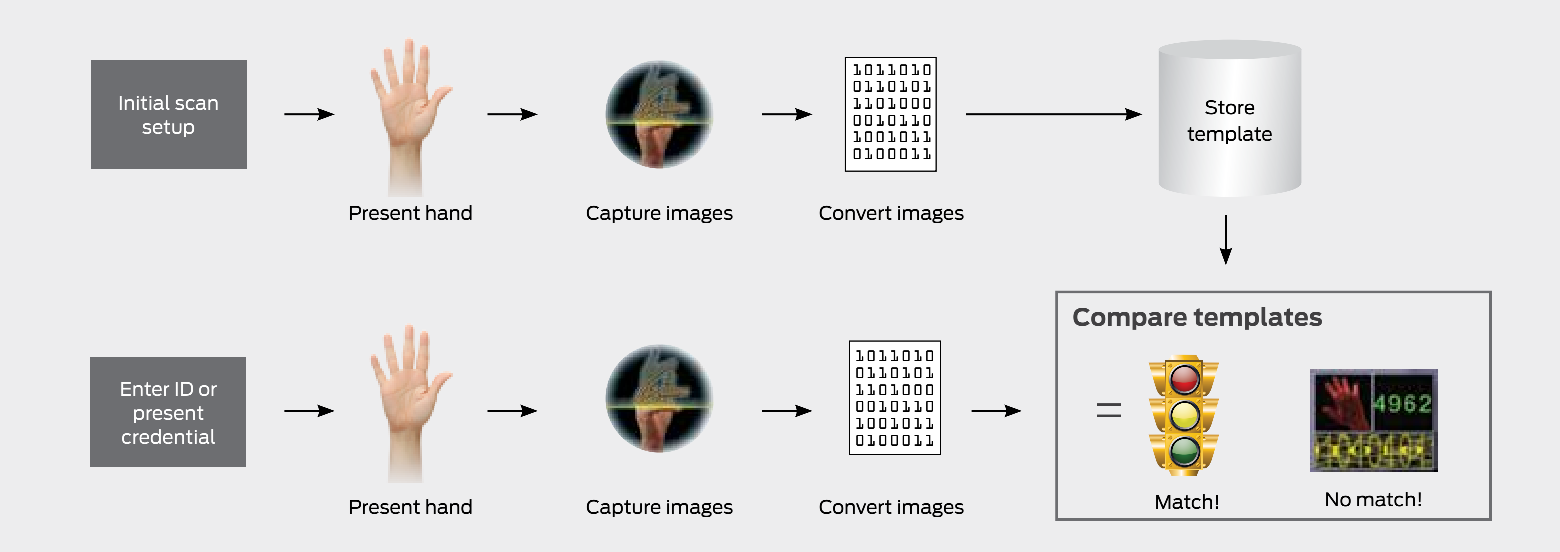
Technology

Geometric measurements of the hand (lengths, widths, areas, and heights) are calculated from the silhouette and then "compressed" by a mathematical formula into a 9-byte numerical template. Since the compression is so high, it is infeasible to reverse-engineer the 9-byte template into the hand image or even the raw geometric measurements of the person that used the HandReader.

Privacy

The HandReader terminal does not collect and store an image of the hand, but instead it converts the image to a 9-byte numerical template which is a mathematical representation of size and shape of the hand. Once this numerical template is developed it is stored in a memory location which is defined by the person's ID number.

To authenticate a user already verified in the database, the user's ID is entered and their hand is placed on the platen (surface area where users place their hand). An image of the hand is captured and then converted to a 9-byte numerical template. If the new template matches the stored template, the person's identity is verified and the transaction is recorded.



No personally-identifiable characteristics such as scars, marks, tattoos, fingerprints or palm prints are captured or detected by the terminal. According to Article 29 from the EU Advisory Body on Data Protection and Privacy: "biometric systems... which do not leave traces (e.g. shape of the hand but not fingerprints)... create less risks for the protection for fundamental rights and freedoms of individuals."

Religion

Since the HandReader is not capable of personally-identifiable characteristics, HandReaders do not in any way have the ability to place or detect the "Mark of the Beast" or any other mark on a person's hand. Many religious organizations and churches trust the HandReader every day to accurately and efficiently manage their time and attendance systems.

Safety

The infrared lights used in the HandReader are similar to those used in remote controls for TV's and VCR's. Internal testing concluded that the light intensity generated by the infrared lights in the HandReader is significantly less than the light intensity generated by direct sunlight. Using a HandReader for 30 seconds a day is comparable to standing in the sun for 0.2 seconds.

Schlage Biometrics has submitted HandReader information to the U.S. Occupational Safety and Health Administration (OSHA). OSHA did not report any hazards.

The Federal Communications Commission requires that computers meet sub-part J of Part 15 of FCC rules. This section details radiated energy. Schlage Biometrics has tested to these standards and meets the requirements of the European Community and is CE Certified.

Hygiene

Every HandReader contains antimicrobial technology which inhibits the growth of a broad spectrum of bacteria, mold, and fungi, making the platen's surface cleaner and more hygienic. This silver-based agent is embedded into the materials used to produce the platen during the manufacturing process. Therefore, the antimicrobial surface remains active for the life of the biometric reader.

Schlage Biometrics has been providing HandReaders for more than 20 years. Every day several hundred thousand hand geometry units are used by millions of people in applications like day care centers, athletic clubs, hotels, manufacturing facilities, government installations, education facilities, and long-term care facilities globally. Schlage Biometric HandReaders have a proven track record in the field and are the durable and reliable biometric you can count on.

About Allegion

Allegion (NYSE: ALLE) creates peace of mind by pioneering safety and security. As a $2 billion provider of security solutions for homes and businesses, Allegion employs more than 8,000 people and sells products in more than 120 countries across the world. Allegion comprises more than 25 global brands, including strategic brands CISA®, Interflex®, LCN®, Schlage® and Von Duprin®. For more, visit **www.allegion.com.**

aptiQ ■ LCN ■ SCHLAGE ■ STEELCRAFT ■ VON DUPRIN

ALLEGION™

006228, Rev. 10/14
www.allegion.com/us

ALLEGION™

SCHLAGE

Effectiveness of hand geometry

HandPunch® increases reliability, eliminates buddy punching and reduces privacy concerns.

- Find out how HandPunch can deliver a payback in fewer than nine months.
- Discover why hand geometry provides more accurate verification than fingerprint technologies.
- Learn how implementing hand geometry biometrics can significantly reduce payroll errors.
- Find out how HandPunch verifies employees without invading their privacy.
- Learn why customers choose the HandPunch for their time and attendance needs.

Get your exclusive copy of the Nucleus Research white paper report on the effectiveness of hand geometry in time and attendance.

Visit us online at www.handreader.com or call 877-671-7011.

The Schlage HandPunch delivers a reliable and industrial option and provides additional benefits over other biometric technologies.

About Allegion

Allegion (NYSE: ALLE) creates peace of mind by pioneering safety and security. As a $2 billion provider of security solutions for homes and businesses, Allegion employs more than 8,000 people and sells products in more than 120 countries across the world. Allegion comprises more than 25 global brands, including strategic brands CISA®, Interflex®, LCN®, Schlage® and Von Duprin®. For more, visit **www.allegion.com.**

aptiQ ■ LCN ■ SCHLAGE ■ STEELCRAFT ■ VON DUPRIN

ALLEGION™

ALLEGION
PIONEERING SAFETY™

Schlage HandPunch Reader Cross-Reference Chart

Reader	GT-400	HP-4000	HP-3000-E	HP-3000	HP-2000	HP-1000E	HP-1000
User Capacity	Dependant upon partner terminal application	530 Standard Expandable to 51,516	512 Standard Expandable to 259,072	512 Standard Expandable to 259,072	512 Non-Expandable	100 Non-Expandable	50 Standard Expandable to 512
Transaction Buffer Capacity	Dependant upon partner terminal application	7680	5120 XL Model - 7680	5120 XL Model - 7680	5120 XL Model - 7680	5120 XL Model - 7680	5120 XL Model - 7680
Display Type	3.8 in 320X240 QVGA monochrome display	2 lines 16 characters per line	2 lines 16 characters per line	2 lines 16 characters per line	2 lines 16 characters per line	2 lines 16 characters per line	2 lines 16 characters per line
Low/High Resolution Templates	High	Low	Low	Low	Low	Low	Low
Alpha Numeric Keypad	●	-	-	-	-	-	-
Function Key Buttons	8	10	2	2	2	-	-
Dynamic and Static Labeling	Dynamic & Static	Static	Static	Static	Static	Static	Static
Field Encryption	●	-	-	-	-	-	-
Anti-microbial	Keypad, Housing and Platen surface	Platen surface	Platen surface	Platen surface	Platen surface	Platen surface	Platen surface

Communication	GT-400	HP-4000	HP-3000-E	HP-3000	HP-2000	HP-1000E	HP-1000
Ethernet	●	○	●	○	○	●	-
DHCP IP Address	●	-	-	-	-	-	-
Static IP Address	●	●	●	●	●	●	-
XML-RPC Interface to Host	●	-	-	-	-	-	-
RS-232 Host Coms	-	●	-	●	●	-	●
RS-422	-	●	-	●	-	-	-
Modem	-	○	-	○	○	-	○

I/O	GT-400	HP-4000	HP-3000-E	HP-3000	HP-2000	HP-1000E	HP-1000
Aux Inputs	-	2	2	2	-	-	-
Aux Outputs	Internal Relay	3	3	3	-	-	-
Printer Output	USB	●	●	●	○	●	○

Credential Inputs	GT-400	HP-4000	HP-3000-E	HP-3000	HP-2000	HP-1000E	HP-1000
PIN - ID (Digit Length)	Unlimited	10	10	10	10	10	10
Barcode Card Reader	○	●	External Option	External Option	-	-	-
Prox	♦	External Option	○	○	-	-	-
iCLASS (CSN read only)	♦	External Option	○	○	-	-	-
Mag stripe	♦	External Option	External Option	External Option	-	-	-
MIFARE/EV1 (CSN read only)	♦	External Option	○	○	-	-	-

Key: ● = Default ○ = Optional - = Not Available

♦ = Future phase External = Not Supplied by Schlage

ALLEGION

PIONEERING SAFETY™

Terminal Application	GT-400 (L4)	HP-4000	HP-3000-E	HP-3000	HP-2000	HP-1000E	HP-1000
Time Zone Restrictions	Dependant upon the partners terminal application	●	●	●	-	-	-
Bell Schedule		●	●	●	-	-	-
User Messages		●	-	-	-	-	-
Custom User Data Fields		●	-	-	-	-	-
User Name Display		●	-	-	-	-	-
Break Compliant		●	XL Model	XL Model	XL Model	XL Model	XL Model
Auto Print Booking Transactions		●	-	-	-	-	-
Supervisor Override Functions		●	●	●			
Schedules		● Individual	● Global	● Global	-	-	-

Support	GT-400	HP-4000	HP-3000-E	HP-3000	HP-2000	HP-1000E	HP-1000
Telnet Access to the Terminal	●	-	-	-	-	-	-
Remote Power-Off via telnet	●	-	-	-	-	-	-
Remote Reboot via telnet	●	-	-	-	-	-	-
Status Display	-	●	●	●	●	●	●

Key: ● = Default ○ = Optional - = Not Available

♦ = Future phase External = Not Supplied by Schlage

ALLEGION™

SCHLAGE®

HandPunch® GT-400

The HandPunch® GT-400 is a versatile and flexible workforce management solution that lends itself to a diverse array of facilities and work groups.

- Healthcare facilities
- Restaurants
- Grocery stores
- Government municipalities
- Manufacturing facilities
- Educational facilities
- Hospitality and Entertainment venues

Hand geometry technology

The HandPunch® GT-400 uses hand geometry, the length, thickness, and curvature of fingers (or simply size and shape of a user's hand), to verify each employee. Hand geometry technology takes measurements of the hand and converts them into a 20-byte numerical template. This template is then matched with the enrollment template and the user's identity is verified. Hand geometry technology is not affected by tattoos, jewelry, fingernails, lotions, dirt, smudges or dust. The reading and verification process takes less than a second with impeccable reliability.

HandPunch GT-400

The HandPunch GT-400 coupled with a software provider, is—hands down—one of the most effective solutions for workforce management. What does that mean for you? It means daily, tangible benefits such as accurate record keeping, risk mitigation, and increased employee productivity that drive your bottom line and provide peace of mind for you and your employees.

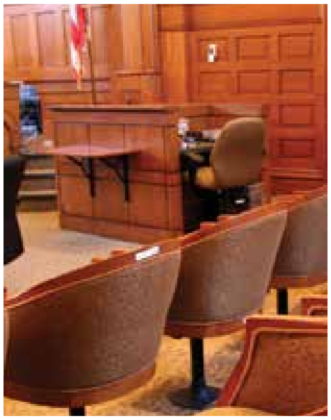
The HandPunch GT-400 uses the size and shape of each employee's hand for verification, so it's fast, efficient and easy to use. It functions well in environments where dirt, dust, grease, moisture, swelling, and dryness are present. For this reason, HandPunch technology is the ideal biometric for all applications.

With a large LCD screen and programmable soft keys, the HandPunch provides a conduit for employee communication right at the terminal. It also delivers a host of other benefits that include:

Reduced payroll and administrative costs
Because punch-in and punch-out data is read and recorded at the point of entry, the translation of timecard records is eliminated—along with any discrepancies between time worked and time reported. This can add up to a significant reduction in administrative costs.

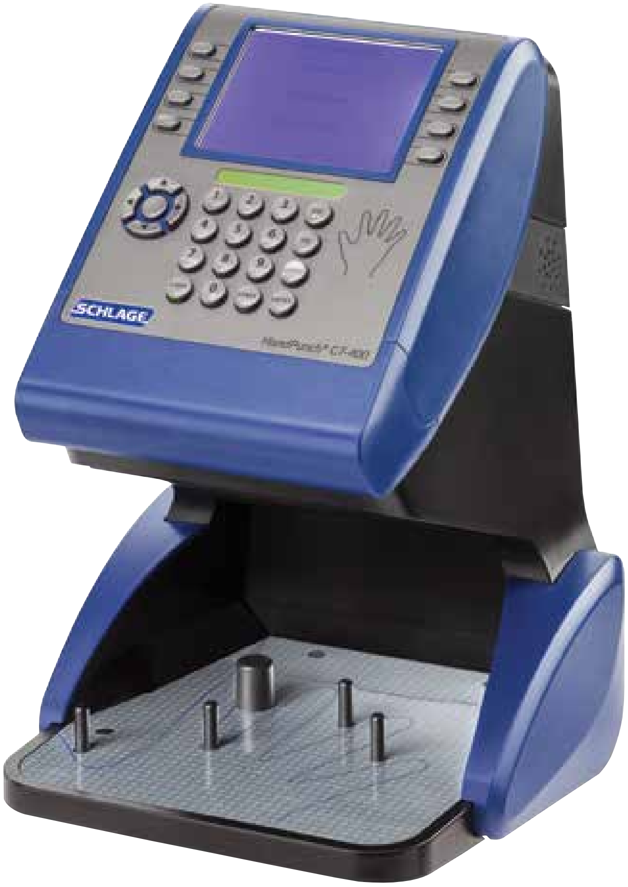
More productive and informed workforce
The verification process is fast and simple as the employee punches in and out. During the process, the communication panel can display relevant messages to employees, promoting communication with management.

Eliminates time fraud
Because every person's hand is unique, the HandPunch provides an accurate and reliable way to record punches for each employee. It eliminates "Buddy Punching", or employees inappropriately entering time and labor data for each other.



The Schlage HandPunch GT-400, partnered with a software provider, is the ultimate workforce management solution.

The HandPunch GT-400 is so efficient that, when used properly, most customers realize payback on the cost of hardware in less than nine months. So ... how about giving us a hand?



Take a look at the features, and you will see that the HandPunch GT-400 is the ideal solution for taking the work out of managing your workforce.

Flexible programming

- Linux based operating system enables maximum programming flexibility and differentiation.

Employee self-service kiosk

- Large display field allows information—such as lists and personal messages—to be displayed.
- Programmable ATM-style soft keys facilitate functionality.

Real-time communication

- Access information in real-time with push technology, making your system more efficient and productive.

Antimicrobial protection

- Antimicrobial coating embedded in platen, keypad, and plastics inhibits growth of bacteria.

Improved serviceability

- Remote diagnostic capability allows for troubleshooting and maintenance at the HandPunch without removing it from the wall.

Increased up-time

- Upgrade remotely—download new firmware and application functionality through an Ethernet connection, without removing the GT-400 from the wall and disrupting your productivity.

Easy Enrollment

- The blue hand outline provides a visual guide for quick and easy enrollment.

About Allegion

Allegion (NYSE: ALLE) creates peace of mind by pioneering safety and security. As a $2 billion provider of security solutions for homes and businesses, Allegion employs more than 8,000 people and sells products in more than 120 countries across the world. Allegion comprises more than 25 global brands, including strategic brands CISA®, Interflex®, LCN®, Schlage® and Von Duprin®.

For more, visit **www.allegion.com**

aptiQ ■ LCN ■ SCHLAGE ■ STEELCRAFT ■ VON DUPRIN

ALLEGION™

NUCLEUS
RESEARCH

GUIDEBOOK

ALLEGION: SCHLAGE HANDPUNCH GUIDEBOOK

July 2014
Document o170

Nucleus Research is the leading provider of value-focused technology research and advice.

NucleusResearch.com

THE BOTTOM LINE

Using biometrics to automate collection of time and attendance data can reduce buddy punching, manual data review, correction time, and payroll error. The Schlage HandPunch gives customers a reliable and industrial option over other biometrics, delivering additional operational benefits by using hand geometry to increase reliability and reduce privacy concerns. Customers maximizing the full potential of the technology can realize payback periods of less than 9 months facilitated through reduced errors, reduced or eliminated systems and materials costs, increased productivity, improved reporting and data visibility, along with reduced compliance risk.

THE SOLUTION

The Schlage HandPunch is a biometric terminal system for time punch entry and record generation used in conjunction with workforce management and human capital management software. The terminal uses hand geometry to verify an employee's identity, eliminating invasive measures such as fingerprint matching or facial recognition used by more conventional biometric terminals. The company's terminal gives customers the benefits associated with employee verification for records management.

To use the terminal, employees enter a PIN or code and place their hand to generate a recorded time punch associated with the time of day. Features of the HandPunch include:

- Employee messaging and self-service. The terminal can be configured to display messages and menus specific to each employee and referenced by their ID. Keys can also be defined to let employees view and enter requests and update information.
- Clock-based editing. Managers can enter a password to modify data entry points without the need to access a computer.
- Bell and door scheduling. Employers can manage shifts and breaks while controlling access to facilities.
- Data integration. Data stored and used in the terminals to identify and access employment records can integrate directly with other applications in HR and payroll to ensure accuracy and reduce manual data review.

WHY SCHLAGE HANDPUNCH

Payroll is a significant source of operating costs for all companies and a small percent change in payroll error can be the difference of finishing a pay period profitably or in the red. Companies have and are investing in workforce management systems (WFM) that improve payroll accuracy. While WFM traditionally mitigates the risk of errors in reporting and cost analysis, standalone enterprise software based on sign-in sheets, time punches, or schedule verifications can be error prone, slow, and incapable of reducing the risk associated with not validating an employee ID.

The Schlage HandPunch uses hand geometry to improve the accuracy of time and attendance, eliminating the possibility of productivity cost drains caused by actions such as buddy punching – the practice of one employee signing in or out for another. While other terminals identify users through palm prints, fingerprints, or iris scans, the HandPunch registers the size and shape of an employee's hand, stores it in the system, and runs a verification match from the database to match an employee to his or her corresponding user record. The technology's use of geometry removes the invasive and often unreliable genetic identification techniques used by other systems, opting instead for large-scale measurements that require less precision to produce a higher level of accuracy in verification.

KEY BENEFITS

Nucleus found that companies using the Schlage HandPunch realized several benefits that result in cost savings over the term of use. Key direct benefits include reduced errors and reduced materials costs, while key indirect benefits include increased productivity, increased data visibility, and reduced compliance risk.

REDUCED ERRORS

Reliable biometrics reduce the risk of employees altering time clock and payroll-related information. As a result, companies can drive down the potential of buddy punching, manipulation of rounding rules, and employee location disputes that arise around legal length of time for donning and doffing and permitted overtime. The average payroll error rate amounts to 1.2 percent of payroll and automating time and attendance and ensuing accuracy serves to reduce this rate. One customer found that moving from paper time cards that could not determine one user from another to the HandPunch system significantly reduced buddy punching. Other customers also found that moving from electronic badge systems to the new system reduced the risk that an employee would lose or forget a badge.

The average payroll error rate amounts to 1.2 percent of payroll and automating time and attendance and ensuring accuracy serves to reduce this rate.

Customers noted:

- *"People will use any excuse when they're late but because the HandPunch was more reliable than fingerprint scanning, I mandated the use of the HandPunch: You will prove to me in the system that you were here or you will not get paid. We still monitor the* *clocks but I know we've saved a fair amount on payroll overpayments because employees believe they will be caught."*

- *"We had problems monitoring time in and out accuracy. It used to take managers away from their other tasks to have to manage it. We tried different methods and ultimately the HandPunch made it so we didn't need a lot of direct oversight to reduce our cost of managing or eliminating errors. No one can punch in or out for another employee letting us see where, when, and how employees are on the clock and it is that simple."*

Customers also found that the HandPunch terminal's use of hand geometry proved more reliable than fingerprint scans, or handprints. Nucleus identified the following advantages of the increased reliability that contributed to fewer errors in timestamp reporting:

- The HandPunch takes an image from multiple angles and relies on visible details while a fingerprint relies on small-scale details that are subjected to environmental conditions such as dirty fingerprints or smudged scanners.
- The HandPunch updates itself based on a built-in biometric template for each user over, adjusting as users' change either from self-induced causes such as weight loss or gain, or from natural causes such as temperature changes or injuries.

One customer found that:

- *"We work in a manufacturing environment and dirt is not uncommon. It's very common for people to have dirty hands from working in the plant all day and with a fingerprint scanner, I had to stand out there every day because there were so many errors."*

REDUCED OR ELIMINATED SYSTEMS AND MATERIALS COSTS

Companies that moved from paper time cards or badge recognition systems to automated terminal units with biometrics eliminated the cost of time cards and badges that average 5 cents per card and 15 cents per badge. Additionally, they eliminated the cost of storing time cards for payroll records and supporting badge systems inclusive of the cost of replacing worn, lost, or stolen badges.

Companies that moved from paper time cards or badge recognition systems to automated terminal units with biometrics eliminated the cost of time cards and badges that average 5 cents per card and 15 cents per badge.

One customer commented:

- *"Employees would come to us having either lost, torn, or demagnetized their badges. We had gone to a new system from timecards because those would get lost, mishandled, or torn and we now had a more expensive resource to keep in inventory. The switch to the new terminal eliminated that without much risk of bad entries."*

INCREASED PRODUCTIVITY

Organizations using the HandPunch reduced the time required for employee identification and punching in and out. The system requires fewer materials to engage the system eliminating objects such as time cards and badges that stand between end users and accessing the terminal. It also reduces the time that HR spends in the back office matching schedules to time punches, supervising the time punch process, and verifying overtime ahead of signing off on payroll.

HandPunch users take advantage of the technology's benefits, realizing productivity increases in a number of areas including:

- Improved management productivity. Automated data entry eliminated the need for manual data reviews and individual amendments to employee records and time stamp entries. The biometric also increases the rate of accuracy in accessibility making it easier for managers to compile and review employee records, and for departmental heads to focus on actionable activities instead of spending time approving timecards.

One customer using a basic terminal noted:

- *"Even though the clock added the hours, they had to be scrutinized. It became an outdated thing."*

- Improved employee productivity. Rapid, reliable timekeeping ensured that employees spent more time on the job and less time entering timestamps. Basic, automated time clocks depended on employees keeping their personal ID cards accessible and in good form; characteristics that more often than not resulted in lost, forgotten, or damaged badges. Deploying the HandPunch accelerated the time punch process, decreasing the amount of time employees spent entering time and attendance data and increasing the amount of time they put into their primary role.

One customer found that:

- *"Most of the time when our people are leaving, it's all at the same time… and they would try to stop working to try to be first to punch out so they didn't have to wait. [The] HandPunch takes only 30 seconds a person, and most of that time is people remembering their ID number and entering it."*

- Improved administration. Automating payroll and time and attendance using biometrics also reduces overall payroll administration time. One organization found that it was able to redeploy more than one quarter of an HR staff member's time to other activities by eliminating management of paper time cards. Another organization reported that employees were able to save more than 30 hours per week reviewing time cards and processing timesheets.

Automated payroll and attendance with biometrics allowed redeployment of HR staff time to other activities by eliminating paper time cards at times by more than ¼. Employees could reduce the time needed to review and process timesheets by up to 30 hours per week.

INCREASED DATA ACCESSIBILITY

Automated data collection and timestamp entry with the HandPunch increased manager visibility into employee work habits and locations. As a result, organizations realized improved monitoring as well as improved audit capabilities. One company found that management could increase the rate at which they identified missing punches or punches where the start and finish locations did not match, establish the reasoning, and resolve the data conflict. Another company found that facilitating immediate access to all of the information in their HRIS system through the HandPunch let managers determine if an employee began their day in one department and finished in another.

One customer noted:

- *"In our organization, employees float between different departments. We would often find out after the fact that they were clocking in and out in departments they weren't scheduled to be working in that day. The HandPunch let us match the location to the punch to understand where employees were using the system to prompt us to find out why."*

The technology also lets managers perform weekly reviews of employee activity to see if staff members have erratic work hours or habits that can be detrimental to employee engagement, customer engagement, and employee-driven business outcomes. The system recorded more accurate and precise data that improved payroll budgeting projections, enabled managers to allocate employee resources more effectively, and decreased the time needed to resolve audits and discrepancies. Nucleus also found that greater visibility for both managers and employees reduced employee concerns about favoritism in scheduling and employee timestamp corrections.

REDUCED COMPLIANCE RISK

Companies found that using an accurate, auditable time and attendance tracking system reduced their risk of cost overages and fines caused by non-compliance measures. It also reduced the amount of time managers spent managing compliance risks and ensuring that internal labor practices in scheduling aligned with FLSA, FMLA, ACA, union, state, local, and other federal rules and regulations. Companies reported compliance to be the largest operational cost after labor, direct inventory and facilities. Compliance costs are not readily known up front and are subject to change throughout a calendar year leaving many HR departments in the dark about the size of their actual risk. While the HandPunch terminals do not report the cost of the risk, they enabled customers to manage individual employees' labor hours through unbiased reporting to ensure that designated, known rules were being followed. As a result, managers were able to access data to minimize the up-front risk of non-compliance and eligibility verification costs for irregularly scheduled employees.

One customer noted:

- *"To employees, a punch in or out is just adding time for pay. To us, we have to be careful about accuracy so we don't run into compliance risks. [The] HandPunch gave us that added layer against basic errors like buddy punching or slipping in some added time that could cause us big problems with government rules and pay amounts."*

KEY COST AREAS

The main cost area for the HandPunch was the initial hardware investment. Other areas reported by customers included:

- Integration. Schlage has several business partners that can integrate with the software forming the user interface in the technology but integration with other systems may be necessary to connect the time and attendance data to the central HRIS for payroll reporting. Customers typically run into added costs for this in the way of consulting provided by their existing HRIS or payroll provider when they are implementing the HandPunch after deploying their HRIS or payroll solutions.
- Personnel. Initial personnel time was required to support implementation of the technology and manage the integration with existing HRIS applications. In spite of reports of labor hours spent, Nucleus found that personnel time required was minimal.
- Training. Some basic, initial training was reported for employees and managers to be familiarized with the technology's user interface. Nucleus found that the HandPunch UI was intuitive and that the training time reported was also minimal.

BEST PRACTICES

Maximizing the return of any software or technology investment is up to the practices used to implement and maintain the solution while keeping internal staff fluent in its use. Nucleus found organizations followed a number of best practices to maximize their return on investment with the HandPunch and reduce the amount of time it took to recuperate the cost of the technology.

- Clear communications. Customers reported several concerns surrounding the HandPunch's implementation surrounding employee data privacy, government data sharing, and data use. The HandPunch does not collect fingerprints or palm data and cannot be used with systems such as the Automated Fingerprint Identification System (AFIS) that connects to law enforcement. Companies should communicate this to employees up front and further use it to segue into how hand geometry data will be collected and used inside the company. Implementing seemingly invasive means of tracking raises concerns among employees and manager need to keep the lines of communications open and include employees in the implementation as much as possible without hindering the deployment timeline.

- Test environment. Deploying to a select group of employees to show how the technology can streamline entering a timestamp and tracking absence and leave requests can help identify initial deployment problems, identify security issues, and create an advocacy panel of employees to increase adoptability among the greater workforce.
- Integration management. The more uses of the HandPunch and the data it generates and tracks, the greater the potential ROI. Integrating the system directly into back-end payroll and HR applications can reduce data management time, errors, omissions, and costs, leading to greater savings across multiple solutions and increasing the value of the implementation.

CONCLUSION

As companies look to reduce labor costs and improve operational efficiency, they need to be considering automating time and attendance to return visibility into labor data for more effective and productive management. While many organizations have automated some aspects of workforce management, many remain challenged to produce accuracy and eliminate employee-generated errors such as buddy punching. Nucleus has found that employees are less likely to attempt buddy punching or other fraud if they believe a system is accurate because they cannot argue with a data-driven outcome correlated with other solutions to deliver context for improved accuracy.

Deploying the HandPunch significantly reduces payroll errors associated with accidental and employee-induced errors, delivering significant returns by reducing the cost of payroll. Companjies supporting paper-based, badge-based, or invasive biometric-based systems can eliminate system error costs associated with failed scans, misread scans, lost, damaged, stolen, or forgotten badges, and timecard storage. Nucleus found that deployed properly, the HandPunch can deliver a payback period of less than 9 months, and companies moving from a paper or badge-based system are likely to see an even shorter period driven by elimination of higher materials costs.

HandPunch® concerns

When it comes to managing time and attendance systems no other biometric solution compares to the Schlage® HandPunch®. Time after time our customers report the reliability of the HandPunch because it accurately identifies employees in environments where dirt, dust, and wet conditions may limit the accuracy of other biometrics. The HandPunch has been known to pay for itself in less than 9 months, making it an ideal solution to businesses that are trying to control costs due to employee payroll fraud, manual data review and correction time, and payroll error. While the benefits of implementing Schlage HandReaders are many, employees may raise concerns about the way hand geometry technology could affect their privacy rights. Schlage Biometrics understands their concerns and would like to address the issues regarding biometrics that may come up.

HandReaders work by shining a light on the user's hand, taking a picture, and looking at the hand silhouette. The illumination is provided by LEDs similar to the remote control on a TV. Think of it as a flashlight casting a shadow of a hand.

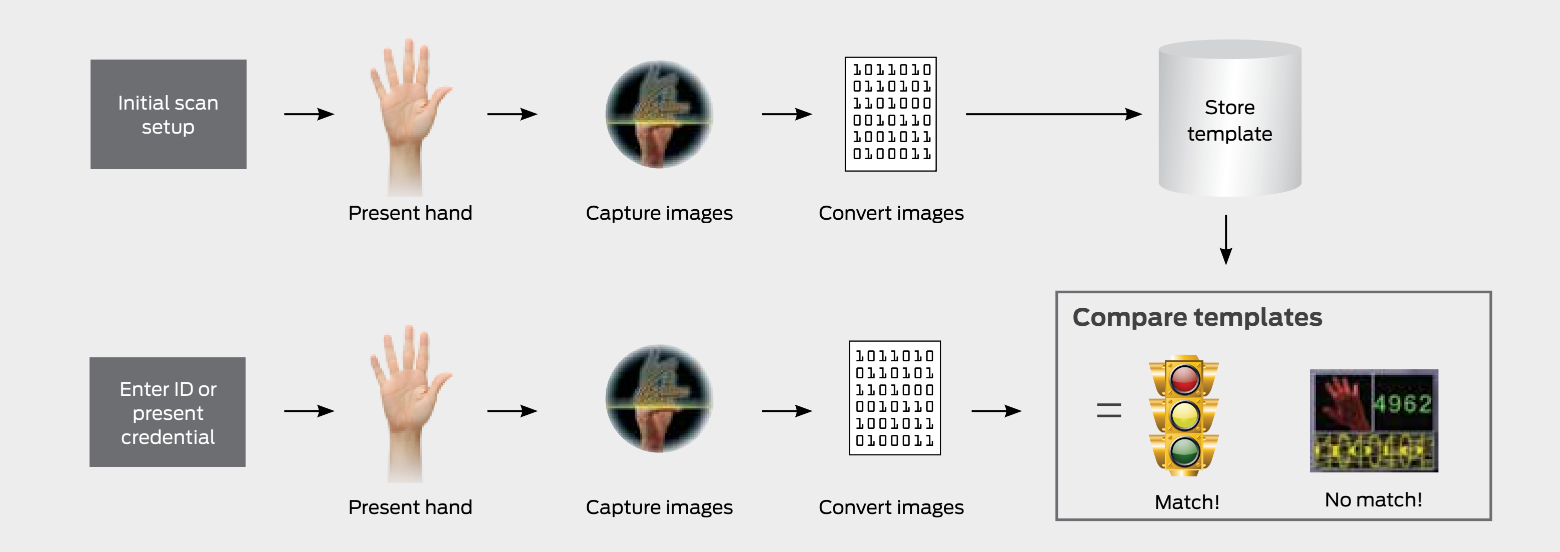
Technology

Geometric measurements of the hand (lengths, widths, areas, and heights) are calculated from the silhouette and then "compressed" by a mathematical formula into a 9-byte numerical template. Since the compression is so high, it is infeasible to reverse-engineer the 9-byte template into the hand image or even the raw geometric measurements of the person that used the HandReader.

Privacy

The HandReader terminal does not collect and store an image of the hand, but instead it converts the image to a 9-byte numerical template which is a mathematical representation of size and shape of the hand. Once this numerical template is developed it is stored in a memory location which is defined by the person's ID number.

To authenticate a user already verified in the database, the user's ID is entered and their hand is placed on the platen (surface area where users place their hand). An image of the hand is captured and then converted to a 9-byte numerical template. If the new template matches the stored template, the person's identity is verified and the transaction is recorded.



No personally-identifiable characteristics such as scars, marks, tattoos, fingerprints or palm prints are captured or detected by the terminal. According to Article 29 from the EU Advisory Body on Data Protection and Privacy: "biometric systems… which do not leave traces (e.g. shape of the hand but not fingerprints)… create less risks for the protection for fundamental rights and freedoms of individuals."

Religion

Since the HandReader is not capable of personally-identifiable characteristics, HandReaders do not in any way have the ability to place or detect the "Mark of the Beast" or any other mark on a person's hand. Many religious organizations and churches trust the HandReader every day to accurately and efficiently manage their time and attendance systems.

Safety

The infrared lights used in the HandReader are similar to those used in remote controls for TV's and VCR's. Internal testing concluded that the light intensity generated by the infrared lights in the HandReader is significantly less than the light intensity generated by direct sunlight. Using a HandReader for 30 seconds a day is comparable to standing in the sun for 0.2 seconds.

Schlage Biometrics has submitted HandReader information to the U.S. Occupational Safety and Health Administration (OSHA). OSHA did not report any hazards.

The Federal Communications Commission requires that computers meet sub-part J of Part 15 of FCC rules. This section details radiated energy. Schlage Biometrics has tested to these standards and meets the requirements of the European Community and is CE Certified.

Hygiene

Every HandReader contains antimicrobial technology which inhibits the growth of a broad spectrum of bacteria, mold, and fungi, making the platen's surface cleaner and more hygienic. This silver-based agent is embedded into the materials used to produce the platen during the manufacturing process. Therefore, the antimicrobial surface remains active for the life of the biometric reader.

Schlage Biometrics has been providing HandReaders for more than 20 years. Every day several hundred thousand hand geometry units are used by millions of people in applications like day care centers, athletic clubs, hotels, manufacturing facilities, government installations, education facilities, and long-term care facilities globally. Schlage Biometric HandReaders have a proven track record in the field and are the durable and reliable biometric you can count on.

About Allegion

Allegion (NYSE: ALLE) creates peace of mind by pioneering safety and security. As a $2 billion provider of security solutions for homes and businesses, Allegion employs more than 8,000 people and sells products in more than 120 countries across the world. Allegion comprises more than 25 global brands, including strategic brands CISA®, Interflex®, LCN®, Schlage® and Von Duprin®. For more, visit **www.allegion.com.**

aptiQ ■ LCN ■ SCHLAGE ■ STEELCRAFT ■ VON DUPRIN

ALLEGION™

ALLEGION™

SCHLAGE®

Effectiveness of hand geometry

HandPunch® increases reliability, eliminates buddy punching and reduces privacy concerns.

- Find out how HandPunch can deliver a payback in fewer than nine months.
- Discover why hand geometry provides more accurate verification than fingerprint technologies.
- Learn how implementing hand geometry biometrics can significantly reduce payroll errors.
- Find out how HandPunch verifies employees without invading their privacy.
- Learn why customers choose the HandPunch for their time and attendance needs.

Get your exclusive copy of the Nucleus Research white paper report on the effectiveness of hand geometry in time and attendance.

Visit us online at www.handreader.com or call 877-671-7011.

The Schlage HandPunch delivers a reliable and industrial option and provides additional benefits over other biometric technologies.

About Allegion

Allegion (NYSE: ALLE) creates peace of mind by pioneering safety and security. As a $2 billion provider of security solutions for homes and businesses, Allegion employs more than 8,000 people and sells products in more than 120 countries across the world. Allegion comprises more than 25 global brands, including strategic brands CISA®, Interflex®, LCN®, Schlage® and Von Duprin®. For more, visit **www.allegion.com.**

aptiQ ▪ LCN ▪ SCHLAGE ▪ STEELCRAFT ▪ VON DUPRIN

ALLEGION™

ALLEGION
PIONEERING SAFETY™

Schlage HandPunch Reader Cross-Reference Chart

Reader	GT-400	HP-4000	HP-3000-E	HP-3000	HP-2000	HP-1000E	HP-1000
User Capacity	Dependant upon partner terminal application	530 Standard Expandable to 51,516	512 Standard Expandable to 259,072	512 Standard Expandable to 259,072	512 Non-Expandable	100 Non-Expandable	50 Standard Expandable to 512
Transaction Buffer Capacity	Dependant upon partner terminal application	7680	5120 XL Model - 7680	5120 XL Model - 7680	5120 XL Model - 7680	5120 XL Model - 7680	5120 XL Model - 7680
Display Type	3.8 in 320X240 QVGA monochrome display	2 lines 16 characters per line	2 lines 16 characters per line	2 lines 16 characters per line	2 lines 16 characters per line	2 lines 16 characters per line	2 lines 16 characters per line
Low/High Resolution Templates	High	Low	Low	Low	Low	Low	Low
Alpha Numeric Keypad	●	-	-	-	-	-	-
Function Key Buttons	8	10	2	2	2	-	-
Dynamic and Static Labeling	Dynamic & Static	Static	Static	Static	Static	Static	Static
Field Encryption	●	-	-	-	-	-	-
Anti-microbial	Keypad, Housing and Platen surface	Platen surface	Platen surface	Platen surface	Platen surface	Platen surface	Platen surface

Communication	GT-400	HP-4000	HP-3000-E	HP-3000	HP-2000	HP-1000E	HP-1000
Ethernet	●	○	●	○	○	●	-
DHCP IP Address	●	-	-	-	-	-	-
Static IP Address	●	●	●	●	●	●	-
XML-RPC Interface to Host	●	-	-	-	-	-	-
RS-232 Host Coms	-	●	-	●	●	-	●
RS-422	-	●	-	●	-	-	-
Modem	-	○	-	○	○	-	○

I/O	GT-400	HP-4000	HP-3000-E	HP-3000	HP-2000	HP-1000E	HP-1000
Aux Inputs	-	2	2	2	-	-	-
Aux Outputs	Internal Relay	3	3	3	-	-	-
Printer Output	USB	●	●	●	○	●	○

Credential Inputs	GT-400	HP-4000	HP-3000-E	HP-3000	HP-2000	HP-1000E	HP-1000
PIN - ID (Digit Length)	Unlimited	10	10	10	10	10	10
Barcode Card Reader	○	●	External Option	External Option	-	-	-
Prox	♦	External Option	○	○	-	-	-
iCLASS (CSN read only)	♦	External Option	○	○	-	-	-
Mag stripe	♦	External Option	External Option	External Option	-	-	-
MIFARE/EV1 (CSN read only)	♦	External Option	○	○	-	-	-

Key: ● = Default ○ = Optional - = Not Available

♦ = Future phase External = Not Supplied by Schlage

ALLEGION

PIONEERING SAFETY™

Terminal Application	GT-400 (L4)	HP-4000	HP-3000-E	HP-3000	HP-2000	HP-1000E	HP-1000
Time Zone Restrictions	Dependant upon the partners terminal application	●	●	●	-	-	-
Bell Schedule		●	●	●	-	-	-
User Messages		●	-	-	-	-	-
Custom User Data Fields		●	-	-	-	-	-
User Name Display		●	-	-	-	-	-
Break Compliant		●	XL Model	XL Model	XL Model	XL Model	XL Model
Auto Print Booking Transactions		●	-	-	-	-	-
Supervisor Override Functions		●	●	●			
Schedules		● Individual	● Global	● Global	-	-	-

Support	GT-400	HP-4000	HP-3000-E	HP-3000	HP-2000	HP-1000E	HP-1000
Telnet Access to the Terminal	●	-	-	-	-	-	-
Remote Power-Off via telnet	●	-	-	-	-	-	-
Remote Reboot via telnet	●	-	-	-	-	-	-
Status Display	-	●	●	●	●	●	●

Key: ● = Default ○ = Optional - = Not Available

♦ = Future phase External = Not Supplied by Schlage

Schlage

Electronic security

Biometric Solutions

Installation Manuals

Master Index

SCHLAGE

HK-II

Terminal User's Guide

Ingersoll Rand
Security Technologies

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and, if not installed and used in accordance with the Installation Manual, may cause harmful interference to radio communications.

Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at the user's own expense. This Class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numerique de la classe A respecte toutes les exigences du Reglemente sure le materiel brouilleur du Canada.

Document Part Number: 70100-6001 – Revision 3.3 – July, 2011

HandKey and HandNet are trademarks of Schlage Biometrics, Inc.

Windows is a trademark of Microsoft Corporation.

The trademarks used in this Manual are the property of the trademark holders. The use of these trademarks in this Manual should not be regarded as infringing upon or affecting the validity of any of these trademarks.

Schlage Biometrics, Inc. reserves the right to change, without notice, product offerings or specifications.

Table of Contents

Introduction

HandKey II

The HandKey II is Schlage Biometrics' fourth generation biometric access control HandReader[1]. The HandReader records and stores the three-dimensional shape of the human hand for comparison and identity verification. Upon verification, the HandReader produces an output that can unlock a door, send card format data to an access control panel, or communicate with a host computer. The HandReader also has auxiliary inputs and outputs that can be used to control other systems such as CCTV cameras and alarms.

Biometrics

Biometric is a term describing the automatic measurement and comparison of human characteristics. While its origins are ancient, the evolution of advanced scanning and microprocessor technology brought biometrics into everyday life. Electronic hand geometry technology first appeared in the 1970s. Schlage Biometrics Inc., founded in 1986, built the first mass-produced hand geometry readers and made biometric technology affordable for the commercial market. Today, Schlage Biometrics' products are in use in every imaginable application from protecting cash vaults to verifying parents in obstetric wards.

Principle of Operation

The HandReader uses low-level infrared light, and a CMOS camera to capture a three-dimensional image of the hand. The HandReader then converts the image to a 9 byte electronic template, and stores the template in a database with the user's information.

To gain access, the user enters his or her ID number at the HandReader's keypad or uses an external card reader. The HandReader prompts the user to place his or her hand on the reader's platen[2]. The HandReader compares the hand on the platen with the user's unique template. If the images match, the HandReader unlocks the door or sends the user's ID number to a third-party access control panel for verification.

The HandKey II

The HandReader is an intelligent access control system that can operate as a stand-alone unit, in a network with other HandReaders, or in a network with a host computer. Refer to Figure 1-1 when reviewing the information in this section.

[1] For the sake of using a consistent name throughout the manual, the HandKey II is referred to as the HandReader for the remainder of this manual.

[2] The platen is the flat surface at the base of the HandReader (see Figure 1-1). This is where users place their hands for enrollment and verification. It has guide pins to position the fingers during use.

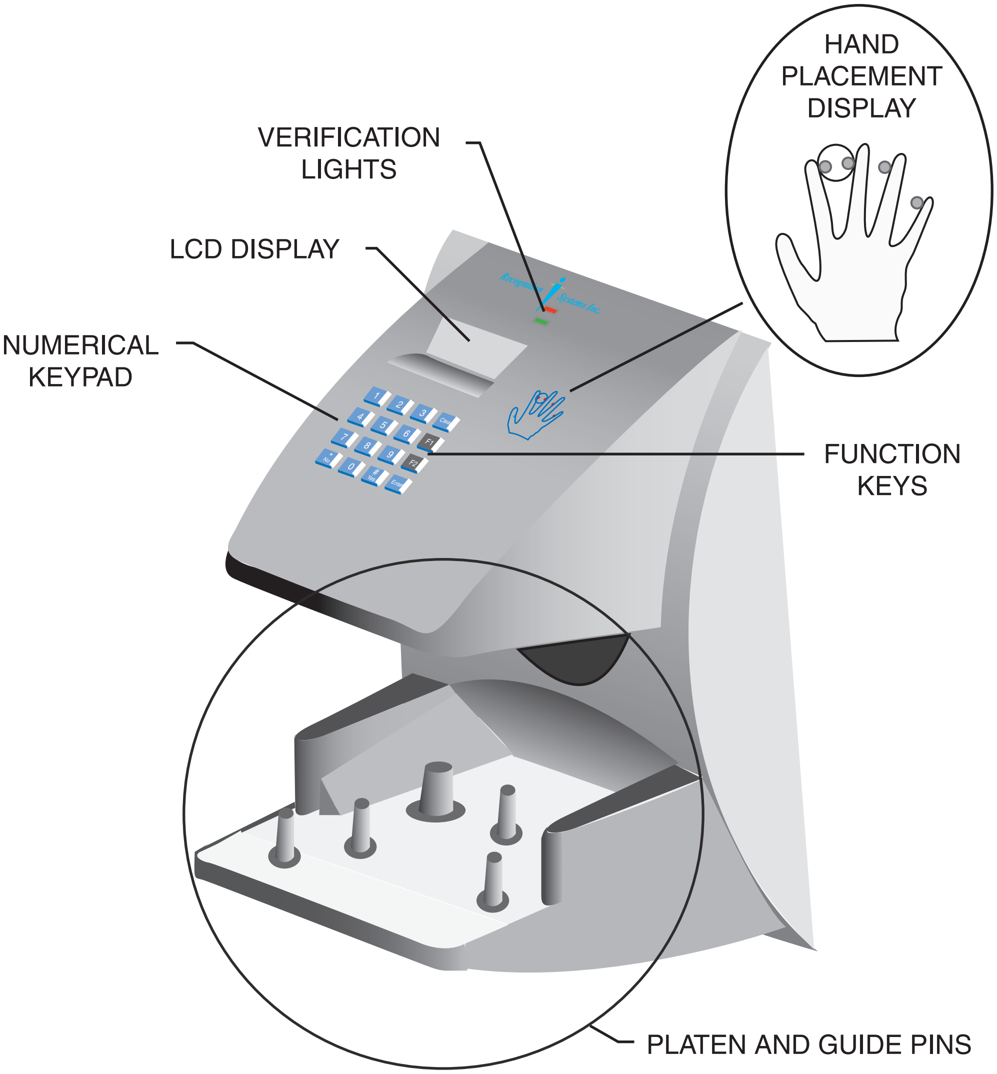


Figure 3-1: The HandKey II

The HandReader has an integrated keypad for ID entry and reader programming. It has two function keys (F1 and F2) that can be set to activate external devices such as a doorbell or an automatic door. The Clear and Enter keys assist in data entry and programming.

Four different features assist the user with hand placement and read verification.

A light emitting diode (LED) hand placement display on the HandReader's top panel assists users with hand placement on the platen.

A liquid crystal display (LCD) shows operational data and programming menus.

"Red light/green light" verification LEDs quickly inform users if their verification attempts were accepted or rejected.

An internal beeper provides audible feedback during keypad data entry and user verification.

Specifications

Size:	8.85 inches wide by 11.65 inches high by 8.55 inches deep (22.3 cm) 22.3 cm wide by 29.6 cm high by 21.7 cm deep
Power:	12 to 24 VDC or 12 to 24 VAC 50-60 Hz, 7 watts
Weight:	6 lbs (2.7 kg)
Wiring:	2 twisted-pair, shielded, AWG 22 or larger (such as Belden 82732)
Temperature:	-10C to +60C – non-operating/storage (14F to 140F) 0C to 45C – operating (32F to 113F)
Relative Humidity Non-Condensing:	5% to 85% – non-operating/storage 20% to 80% – operating
Verification Time:	1 second or less
Memory Retention:	5 years using a standard internal lithium battery
Transaction Buffer:	5120 transactions
ID Number Length:	1 to 10 digits
Baud Rate:	300 to 28.8 K bps
Communications:	RS-232, RS-422, RS-485 2-wire, optional Ethernet, optional Modem
User Capacity:	512 users expandable to 259,072
Card Reader Input:	Proximity, Wiegand, Magnetic Stripe, Bar Code (5 VDC provided by HandReader)
Card Reader Output:	Wiegand, Magnetic Stripe, Bar Code
Duress Code:	1 leading digit, user definable
Door Controls:	Request to Exit input, Door Switch input, Lock output (open collector, 5 VDC present, sinks to ground, 100 mA max)
Alarm Monitoring:	Tamper, Door Forced, Duress
Event Monitoring:	There is a variety of monitoring options including events such as: Invalid ID, Time Zone Violation, ID Refused, Try Again, Power Failure
Time Zones:	62 total – 2 fixed, 60 programmable
Auxiliary Outputs:	3 user definable (open collector, 5 VDC present, sinks to ground, 100 mA max)
Auxiliary Inputs:	Auxiliary Input 1 and 2 (open collector, 5 VDC present, sinks to ground, 100 mA max)

Options

HandKey units have the following options available.

• Backup Battery Support	See Technical Note 70200-0012 rev C
• Modem Communication	See Technical Note 70200-0013 rev C
• Ethernet Communication	See Technical Note 70200-0014 rev H

UL Compliance

Hand Readers are UL Listed as stand alone units only (i.e. the card reader function has not been evaluated by UL).

The HandKey II has not been tested for UL 294 in an Outdoor configuration.

Planning an Installation

Site Preparation

Before you begin installation, check the site blueprints, riser diagrams, and specifications for important information about the HandRreader's location and other systems that will connect to the HandReader. Look for any existing wall preparations and wiring that other contractors may have installed for the HandReaders.

HandReader Placement

The recommended height for the HandReader platen is 40 inches (102 cm) from the finished floor. The HandReader should be out of the path of pedestrian and vehicular traffic, and convenient too, but not behind the door it is controlling. Avoid placing the HandReader where users must cross the swing path of the door. The HandReader should be in an area where it is not exposed to excessive airborne dust, direct sunlight, water, or chemicals.

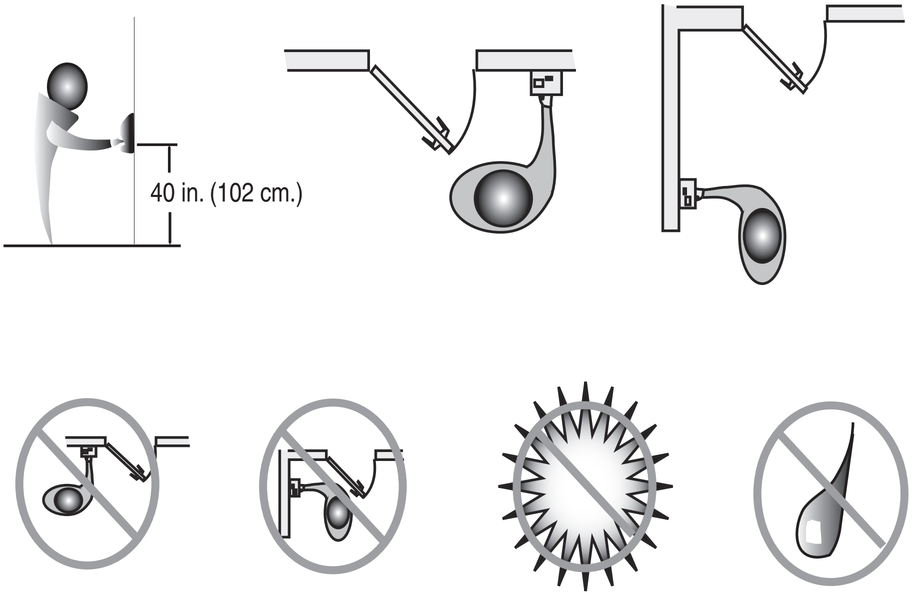


Figure 4-1: HandKey Placement Rules

! NOTE *For the following sections, Schlage Biometrics does not supply hardware items such as door control relays, door locks, switches, relays, communications or power wiring, or power supplies (a PS-110 or PS-220 power supply can be purchased from Schlage Biometrics to power the HandReader).*

Wiring

Four basic circuits typically connect to the HandReader:

- Power Input
- Door Control Inputs and Outputs
- Networking and Communications
- Card Reader Input and Emulation Output

Power Input

The HandReader requires 12 to 24 volts DC (600 mA) or 12 to 24 volts AC (7 watts). Power can be connected either to the power terminal pins 1 and 2 or through barrel jack J12.

! NOTE *Terminal 1 and the center pin of power jack J12 are connected together. Terminal 2 and the sleeve of power jack J12 are connected together.*

A full-wave bridge rectifier input structure is used in the power supply of the HandReader, making the polarity of terminals 1 and 2 irrelevant. Schlage Biometrics recommends using terminal 1 for positive (+) voltage and terminal 2 for common (-) for consistency. If J12 is used to attach power with the optional Schlage Biometrics wall-mount power supply, terminal 1 will reflect +13.8 VDC (unregulated) and terminal 2 will be power supply common.

! NOTE *Neither terminal 1 or terminal 2 is connected to the HandReader ground.*

! NOTE *Do not connect a HandKey's power supply to a switched duplex outlet. The HandKey must have a constant source of power for proper operation.*

Battery Backup

The HandReader uses an internal switching regulator to obtain internal operational power. It accepts input voltages from 12 to 24 VDC or 12 to 24 VAC at 50 to 60 Hz. An optional power-fail protection circuit board can be attached to the main circuit board to provide and control battery backup. The design of the internal power supply is such that any range of the above input voltages may be used and still provide proper battery charge voltage and battery backup operation. Switch-over to battery power is automatic and occurs when the input voltage falls to approximately 10.5 volts. At that time the internal battery charger is disabled to save power and uninterrupted operation continues on battery power.

When input power is restored, the HandReader switches off of battery operation and the battery charger is re-enabled to recharge the battery. Battery charge voltage is set at approximately 13.65 volts, and battery charge current is limited to approximately 50 mA. A fully discharged battery requires approximately 12 hours of charge to fully recover.

Additional options installed and specific configurations within the HandReader make it difficult to predict precisely how long battery support will last, but in general two hours of battery operation can be expected. While operating on battery backup due to loss of main input power, the battery output voltage is constantly monitored by internal circuitry. If the battery voltage reaches approximately 9.5 volts the HandReader automatically shuts down. This is done to prevent full exhaustion of the battery. A yellow indicator on the top panel illuminates to indicate that the HandReader is running off of battery power. This indicator extinguishes when main input power is restored.

Shunt J7 which is located immediately in front of the DIP switches on the main logic board (see Figure 5-1 on page 21) enables or disables battery operation on those HandReaders equipped with optional battery backup. If a HandReader does not have the optional battery backup package installed, J7 is not used. On HandReaders equipped with the battery backup option, J7 allows service personnel a mechanism for disabling battery backup operation before removal of main input power. To fully power down a HandReader equipped with battery backup, remove or reposition shunt J7 so that the two pins protruding up from the main logic board are not connected to each other. This effectively opens the circuit, removing the battery from any internal circuitry. Main input power can then be removed and the HandReader will fully shut down. Once the HandReader has fully shut down, shunt J7 may be reinstalled. The design of the power supply is such that main input power must be reapplied to re-enable the battery protection mechanism. If shunt J7 is not properly installed, the internal backup battery will not be charged, and in the event of a main input power loss, the HandReader will shut down.

The HandReader with the battery backup option uses a 12 volt 800 ma/hour sealed lead acid battery to provide backup battery power. This battery is located immediately inside the rear panel of the HandReader and plugs into jack J4 on the keypad control circuit board located in the top of the chassis.

Earth Ground and Shielding

Schlage Biometrics recommends that all HandReaders be grounded with a solid, reliable earth ground connection. This connection establishes a common ground return point used to protect internal semiconductor devices from ElectroStatic Discharge (ESD) and from external signal line transients. It also provides a common signal level reference point between externally networked HandPunchs. Schlage Biometrics recommends that the earth ground source be identified by a qualified electrician familiar with electrical codes as well as wiring and grounding techniques.

This is an extremely important and often overlooked aspect of hard-wired serial communication systems. If the sending and receiving stations do not agree on the ground reference for the signal voltages, communication errors or a total inability to communicate may be observed. If the voltages are very different, it is even possible to damage the units.

The subject of grounding can be complicated, and the full circuit of a system, including power supplies and often even the building line power wiring, must be understood. It is strongly recommended that a qualified electrician or electrical engineer familiar with this subject be consulted when designing the wiring of an HGU network installation. Always adhere to any applicable electrical codes for your area. Schlage Biometrics is not responsible for damage done to units due to improper wiring.

! NOTE *Use any one of the following ground terminals to make the earth ground connection: 4, 10, or 13. Do NOT use terminal 2 to establish the earth ground connection; terminal 2 is not directly connected to ground.*

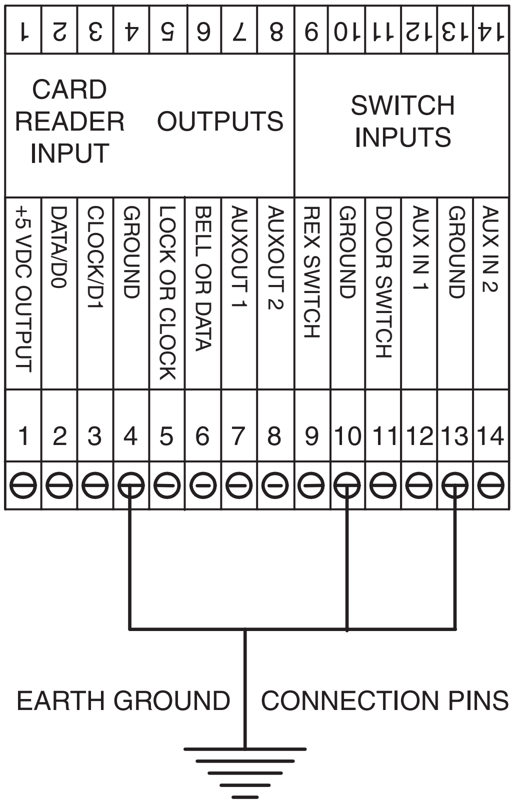


Figure 4-2: Earth Ground Connection Terminals

There are two standard methods for providing earth grounding to HandKey units:

- earth grounding all units (see figure 4-3 on page 11)
- carrying an earth ground to each unit (see figure 4-4 on page 11)

Earth ground all units when there is a good earth ground source near each unit and/or when there are very long cable runs between units.

Carry an earth ground to each unit when there are no earth grounds convenient to the unit and the unit's power supply is floating.

Earth Ground All Units

One method of establishing a ground reference is to connect each unit's main board ground to earth ground. Earth ground is found on the third pin on standard AC line sockets (in the United States, this is the round one in the middle). If the building wiring is functioning correctly, this should be a low-impedance path to a true ground, which then serves as a common reference point for the units.

If this method of grounding the units is used, it is not necessary to connect the units in the network together with a ground line in the communication cable. Indeed, doing so could create ground loops—large-area loops which provide a good coupling to external magnetic fields—which may actually compound communication problems. If a magnetic field, such as that from a lightning strike, induces a voltage in the ground loop, it is possible for large currents to flow around the loop, which can raise the ground potential of some units relative to others. When the shield or the cable is connected to any ground in this configuration, it should be connected only at one end to prevent the formation of ground loops.

For systems with multiple units on a network, there will be a series of cables daisy-chained between the units, and the shield of each leg of the network should be connected to ground at only one end. It does not matter which end. An example of this method of grounding is shown in Figure 2-3.

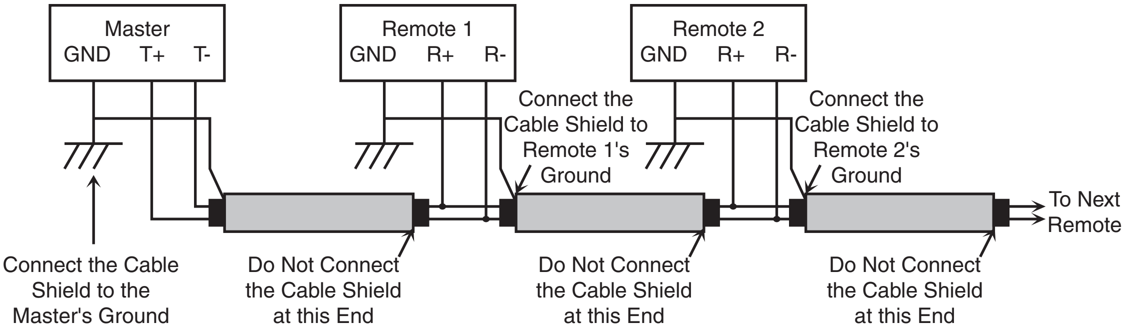

Master
GND T+ T-
Remote 1
GND R+ R-
Remote 2
GND R+ R-
Connect the Cable Shield to Remote 1's Ground
Connect the Cable Shield to Remote 2's Ground
To Next Remote
Connect the Cable Shield to the Master's Ground
Do Not Connect the Cable Shield at this End
Do Not Connect the Cable Shield at this End
Do Not Connect the Cable Shield at this End

Figure 4-3: Communication Shielding With All Units Earth Grounded

All units are connected to the same earth ground. Each shield ground is connected to only one unit, then interrupted to prevent the formation of ground loops. Two sets of lines are wired as shown in Figure 2-3. It does not matter significantly which unit's GND is used for a particular shield, as long as the path is broken from unit to unit.

Carry a Ground Line to Each Unit

The second method of establishing a ground reference in a system with floating power supplies is to use the ground line in the RS-422 cable to establish a common reference voltage for the communication signals. This line should be connected to the negative power terminal on the data converter or the ground line in the RS-232 port from the host PC system. It should then be carried to one of the ground terminals on the back of each unit in the network. An example of this method of grounding is shown in Figure 2-4.

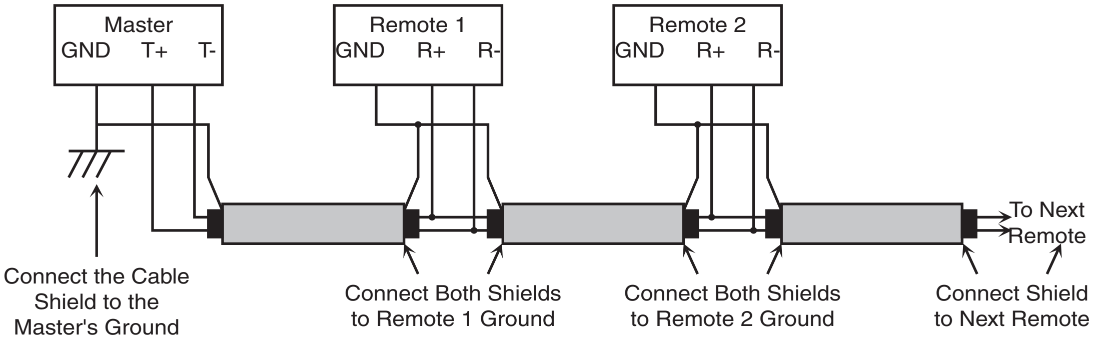

Master
GND T+ T-
Remote 1
GND R+ R-
Remote 2
GND R+ R-
To Next Remote
Connect the Cable Shield to the Master's Ground
Connect Both Shields to Remote 1 Ground
Connect Both Shields to Remote 2 Ground
Connect Shield to Next Remote

Figure 4-4: Communication Shielding Carrying a Single Ground to Each Unit

If no earth ground is available at the units, this is the only possible method of connecting the grounds. Even if an earth ground is available, depending on the building's power wiring and other environmental issues, this method may be superior to the previous one, since it establishes the ground of each unit independently of the building power lines. Local variations in grounds between buildings, or from one point to another in a very large building, (perhaps due to elevator motors or other large-current drawing machines) will have no effect on the communication network if this configuration is used.

However, the power supplies must be truly floating, with no hidden paths back to the high-voltage side of the transformers, or to earth ground. Since this is difficult to achieve (there is always some parasitic capacitance between the primary and secondary in any transformer), this method may be more susceptible to high-frequency transients in the high-voltage side of the power lines than the earth-grounded method.

The master unit's ground establishes the ground for the entire system. The main board ground points are connected to the shield ground at each unit, but are not connected to earth ground. The ground point on the master can be the data converter power supply negative terminal, or the GND pin on the RS-232 cable. If the master is an HGU, its main board ground can be used. This configuration should only be used if the power supplies to the units are truly floating, otherwise ground loops will be created, and differences in local grounds may cause large currents to flow through the cable shield.

Door Control Output

The HandReader can operate a door in two different modes: lock output and card reader emulation. The wiring for each mode is significantly different.

Lock Output Mode

In the lock output mode, the HandReader acts as an intelligent access reader signaling a lock relay or controller to unlock the door. It also monitors the status of the door. The decision to unlock the door is made by the HandReader after a valid verification. Users may be assigned time restrictions to limit access during specified hours or days.

Card Reader Emulation Mode

In card reader emulation mode, the HandReader outputs Wiegand (by default), magnetic stripe, or some other card reader signal, typically to an access control panel when a user successfully verifies. This mode makes integrating with existing access control systems fast and simple. On retrofit applications, the existing card reader wiring can be used to connect the HandReader to the panel if it has AWG 22 or larger conductors and is in good condition.

The standard HandReader emulation format is for a 26-bit Wiegand card using an 8-bit facility code. Other formats and card reader technology emulations are available. Consult the factory for formats other than 26-bit Wiegand.

The ID number may be entered via the integrated keypad or an external card reader.

If the user enters the ID number from the keypad, the HandReader sends the ID number to the access panel in the specified card format with a pre-programmed facility code.

If the ID number is entered via the card reader, the HandReader stores the card data and then sends the data, unmodified, to the access panel when the user successfully verifies.

Inputs and Outputs

In addition to the Lock and Auxiliary Output and the Card Reader Emulation Output, the HandReader has additional inputs and outputs for use with alarms and other controllers.

- Three Programmable Auxiliary Outputs
- Door Monitor Switch Input
- Request to Exit Input
- Card Reader Input for Wiegand or Magnetic Stripe
- Two Auxiliary Inputs

An open collector transistor driver drives each one of these outputs. Open collector refers to a transistor configuration capable of sinking current (by “pulling down” one side of a load to ground) but not able to source current – e.g. the transistor output is incapable of supplying current to drive up the output voltage and must rely on an external voltage source to accomplish this.

HandReader outputs, when measured to ground, generally show around 4.5 volts when they are inactive and no load is attached. This voltage is developed by a combination diode and series resistor pull up to the internal +5 volt supply of the HandReader. These outputs are pulled up internally to insure that they remain in a known condition if used to output Wiegand or magnetic stripe data to some external device.

If one of the outputs is shorted to ground, there will be approximately 5 mA of current flowing through the short, but no damage will occur. Because of the open collector structure of the outputs, each output is free to float to whatever external voltage is applied (when inactive). For example, if one side of a relay coil is connected to an external +12 volt power source and the other side of the relay coil is measured with respect to the ground of the external power source, the measurement will be +12 volts.

If the ground of the external power source (+12 volt return) is tied to the ground of the HandReader, and the free relay coil wire connected to the LOCK output, the LOCK output pin will read +12 volts also (when inactive). This is because the LOCK output is not active and free to “float” to whatever external voltage is applied. When a hand is verified, the LOCK output becomes active and essentially looks like a short to the HandReader ground. This “short” causes the full +12 volts of the external power source to be placed across the relay coil, energizing the relay. The ground of the external +12 volt source must be tied to the HandReader ground to make a complete circuit path.

All HandReader outputs are rated at +24 volts DC maximum with a maximum current draw of 100 mA. This means that it is acceptable to use up to a +24 volt DC external power supply to energize external devices. Whatever external relay is used should be chosen to match the external power supply voltage. For example, if the external relay coil is rated at 15 volts, a 15 volt external power supply should be used. In no case should the external voltage be higher than +24 VDC.

Each HandReader has a protection mechanism built in to protect against voltage transients (spikes) coming back into the HandReader from an external relay coil. Transients from an “opening” or de-energizing relay coil can reach several hundred volts. This protection is on all HandReader outputs and will limit reverse spikes to approximately 28 volts to protect the open collector transistor driver. HandReader outputs are NOT designed to switch AC voltages. DC voltages MUST be used and the correct polarities MUST be maintained.

! NOTE *Relays or devices connected to the lock and auxiliary outputs must not exceed 0.1 A current draw.*

Networking and Communications

HandReader networking and communications can be configured in one of five ways:

- as a stand-alone HandReader
- as a master or remote HandReader in a HandReader network
- as a remote HandReader in a HandReader network connected to a host PC
- as a remote network connected via optional Modem to host PC
- as a remote network connected via optional Ethernet to host PC

Stand-alone HandReader

When installed as a stand-alone access control system there is no communication wiring to other HandReaders or to a host computer. Power input and control output wiring are all that are required. An RS-232 serial printer output is available for event logging (refer to the Printer section on page 16). Schlage Biometrics highly recommends using Backhand™ software to backup template information stored in the HandReader.

Master or Remote HandReader in a HandReader Network

Multiple HandReaders can be linked together in a HandReader network.

- Up to 32 HandReaders can be linked together on a 2-wire RS-485 or 4-wire RS-422 network.
- Two twisted-pair, shielded, AWG 22 (or larger) wire should be used (Schlage Biometrics recommends Belden 82732 or its equivalent).
- The wiring must be a “daisy chain” network from HandReader to HandReader and must not exceed 4,000 feet (1220 meters) in total length.

The master/remote network requires user enrollment at the “master” HandReader. The master HandReader distributes hand template data with ID numbers and time restrictions (if any) to the other HandReaders in the network. Users removed at the master HandReader are automatically removed from the remote readers. A printer connected to the master HandReader will report transactions from all HandReaders on the network.

Remote HandReader in a HandReader Network Connected to a Host PC

Multiple HandReaders can be linked to a personal computer (PC) for an integrated access control network. Real time monitoring of door status and a variety of alarm types can be done with Schlage Biometrics’ HandNet for Windows™ (Schlage Biometrics model number HN-300) software. To run HandNet for Windows™ the computer must be PC compatible, using a Pentium™-166 or faster microprocessor and it must have a CD-ROM.

- The HandNet software can monitor over 1,000 HandReaders simultaneously.
- An unlimited number of sites can be created with up to 32 HandReaders per site.
- The HandReaders report all transactions to the PC. The HandNet software records all transactions and displays a variety of reports generated from this information.
- Template management is handled automatically.
- Users may enroll at any HandReader in the system. The PC collects the data and distributes it to other HandReaders in the network.
- Access may be restricted by time and by HandReader via HandNet’s access profiles and by the use of time zones.

Typically, HandReader networks link to a PC using an RS-422 connection. These networks have the following requirements.

- Two twisted pair, shielded, AWG 22 wire or larger should be used (Schlage Biometrics recommends Belden No. 82723 or equivalent cable).
- HandReaders must be wired together in a “daisy chain” network from HandReader to HandReader and then to the host PC. The total length of the wiring must not exceed 4,000 feet per network.
- The network requires an RS-422 to RS-232 converter (Schlage Biometrics P/N DC-102) at the PC.

Schlage Biometrics’ optional HandNet for Windows™ software allows programming of most of the remote HandReader setups from the computer. However, each HandReader on the network requires the setting of an address. HandReader addresses may be repeated, but only on different sites. Display language, date format changes, and the communication mode must also be set at the HandReader.

Remote HandReader Connected to a Host PC via Optional Modem

An optional, internal “answer only” 14.4 bps modem is available for HandReaders. This modem is designed for operation with United States phone systems. Site wiring should conform to standard telephone wiring standards and terminate at the HandReader with a standard RJ-11 modular phone jack. Each HandReader with a modem includes a 6’ modem cable for the final connection between the phone jack and the HandReader modem. Modem HandReaders may be networked with up to 31 non-modem HandReaders using RS-422 wiring. Refer to the Modem Application Note (available from Schlage Biometrics) for detailed information.

Remote HandReader Connected to a Host PC via Optional Ethernet

The HandReader is available with an optional, internal Ethernet communications module for TCP/IP communications. The wiring must conform to 10BaseT standards. Typically, network wiring terminates at the HandReader with a standard RJ-45 modular jack. The cable from the jack to the HandReader is not provided with the Ethernet option. The IP address, Gateway, and Host Bits are entered at the HandReader in the SET SERIAL menu. Ethernet HandReaders may be networked with up to 31 non-Ethernet HandReaders using RS-422 twisted pair cable. Refer to the Ethernet Application Note (available from Schlage Biometrics) for detailed information.

Printer

You can connect a serial printer to a HandReader. A printer connected to the master HandReader (in a master-remote application) will print every event as it occurs. A printer connected to a remote HandReader will print only the events that occur at that HandReader. Schlage Biometrics Inc. does not supply serial printers. Refer to the Printer String Application Note (available from Schlage Biometrics) for detailed information.

Mechanical Installation

Select an installation location based on the guidelines provided in the Planning an Installation section beginning on page 7.

Wall Plate Installation

! NOTE *For the following instructions protect the HandReader from the dust and debris generated during the wall plate installation process.*

1. Remove the wall plate from the packing carton. Refer to Figure 4-1 for all wall plate references in the following section.

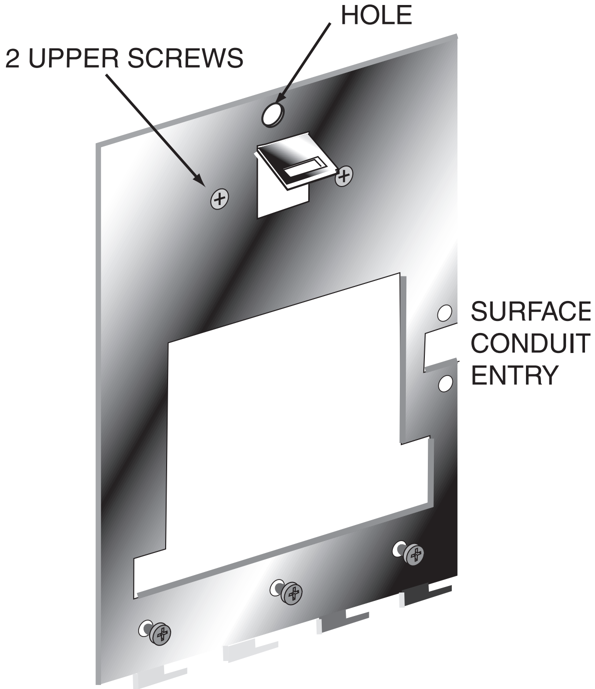


Figure 6-2: Wall Plate

3. Measure and mark a point 48 1/2 inches (123 cm) from the surface of the finished floor. This point will correspond to where the top-center point of the HandReader should be mounted.
4. For a hollow wall, drive a small nail into the wall at the mark and hang the wall plate from the leveling hole located near the top of the wall plate.

5. For a solid wall, hold the wall plate against the wall, centering the leveling hole over the mark in the wall.
6. Align a bubble level with the top edge of the wall plate and gently rotate the wall plate until the bubble level shows that the top edge of the wall plate is level.
7. Secure the plate to the wall using heavy masking tape.
8. Using the wall plate as a template, mark the locations of the two upper screw holes and the three lower screw holes.
9. For a concealed wiring connection, trace the outline of the open area in the center of the wall plate. Identify and mark a 1/2 inch hole through which the HandReader's wiring will be mounted.
10. For a surface conduit wiring connection, mark the two conduit clamp holes at the right side of the wall plate.
11. Remove the wall plate, masking tape, and the nail (if used).

Mounting the Wall Plate

1. For a hollow wall, use the provided hardware to mount the wall plate. Use the two auger style fasteners for the upper two mounting holes. Use the toggle bolts for the three lower mounting holes.
2. For a solid wall, use expansion bolts to mount the wall plate. For all five mounting holes, drill a 1/4 inch diameter hole, 1/4 of an inch deeper than the length of the expansion anchor.

Routing the Wiring

1. For a concealed wiring connection, drill a 1/2 inch hole in a convenient location within the open area of the wall plate. Pull the wiring to enter the HandReader through this hole in the open area.
2. For a surface conduit wiring connection, drill a 1/4 inch diameter hole, 1/4 of an inch deeper than the length of the expansion anchor for each of the two conduit clamp holes. Route 1/2 inch conduit to the HandReader, ending the conduit between the two conduit clamp holes. Pull the wiring to enter the HandReader through the conduit.

Attaching the HandReader

1. Remove the HandReader from its carton.
2. Align the sleeves of the back plate with the pins of the wall plate and slide the HandReader to the left as shown in figure 4-2.

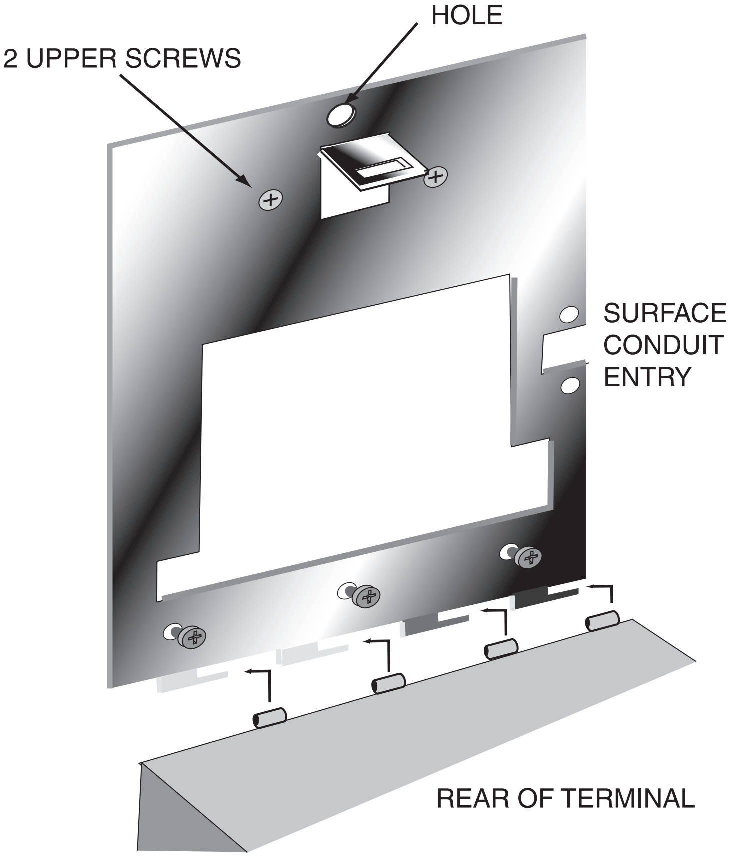


Figure 6-3: Attaching the HandReader to the Wall Plate

4. The HandReader is now ready for its wiring connections.

Closing the HandReader

With the wall mount latch in the unlocked position, swing the body of the HandReader up and rotate the key away from the wall. Hold the top of the HandReader firmly against the wall and rotate key towards wall, locking the latch into place (see Figure 4-3).

! NOTE *Do not force the HandReader onto the wall mount latch when the latch is in the locked (down) position.*

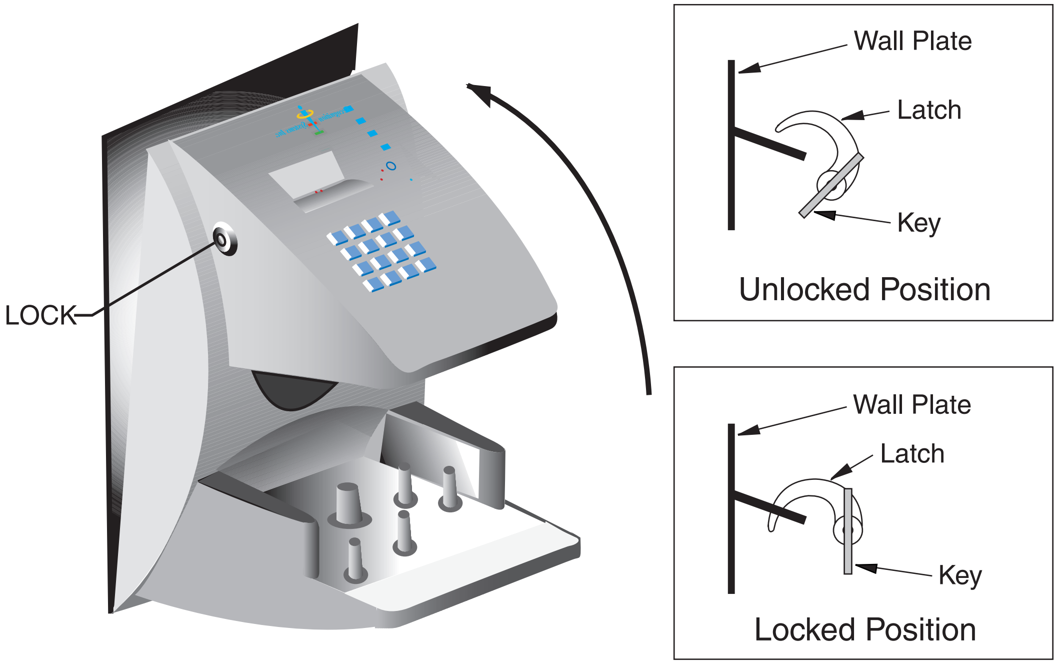


Figure 6-5: Closing the HandReader

Wiring Connections

Once the HandReader is attached to the wall plate the wiring connections to the HandReader can be made (see Figure 5-1).

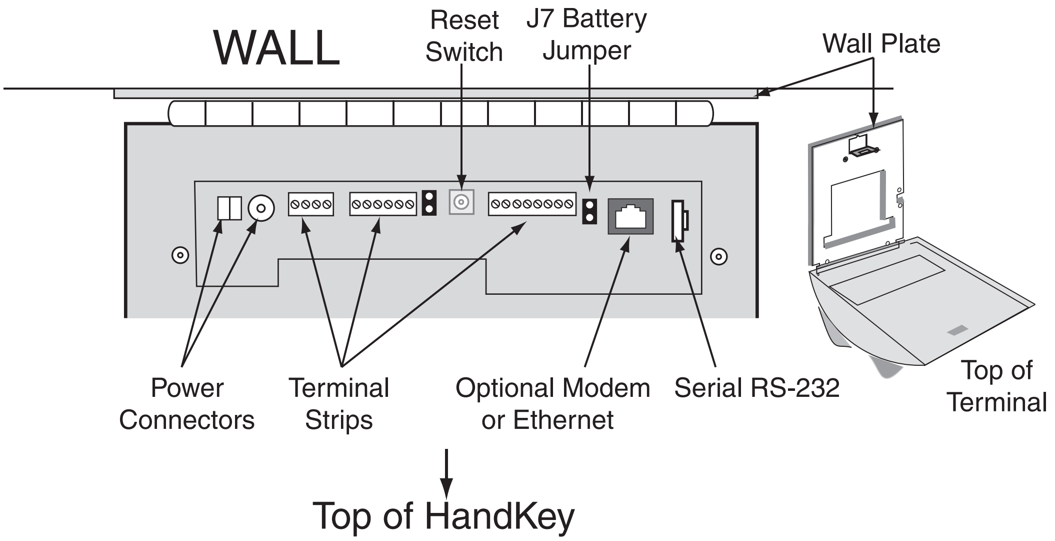


Figure 7-1: Wiring Connections

Wiring Examples

The following Tables provide the pin outs for the terminal strips on the HandReader.

- Table 5-1 on page 22 provides the pin outs for TS-1: Communication Connections.
- Table 5-2 on page 22 provides the pin outs for TS-2: Input Connections.
- Table 5-3 on page 22 provides the pin outs for TS-3: Output Connections.
- Table 5-4 on page 22 provides the pin outs for the Serial RS-232 Connection.

The following Figures provide typical HandReader wiring diagrams.

- Figure 5-2 on page 23 provides a typical Lock Output wiring diagram.
- Figure 5-3 on page 24 provides a typical Auxiliary Output wiring diagram.
- Figure 5-4 on page 25 provides a typical Card Reader Emulation Mode wiring diagram.
- Figure 5-5 on page 26 provides a typical RS-422 Master/Remote Network System wiring diagram.
- Figure 5-6 on page 27 provides a typical RS-485 2-Wire Master/Remote Network System wiring diagram.
- Figure 5-7 on page 28 provides a typical Host PC Network System wiring diagram.
- Figure 5-8 on page 29 provides a typical Printer to HandReader wiring diagram.

Table 7-1: TS-1 - Power and Communication Connections

Terminal	Connection
15	RS-422 Rx- or RS-485 Rx-/Tx-
16	RS-422 Tx- or RS-485 Rx+/Tx+
17	RS-422 Rx+
18	RS-422 Tx+

Table 7-2: TS-2 - Input Connections

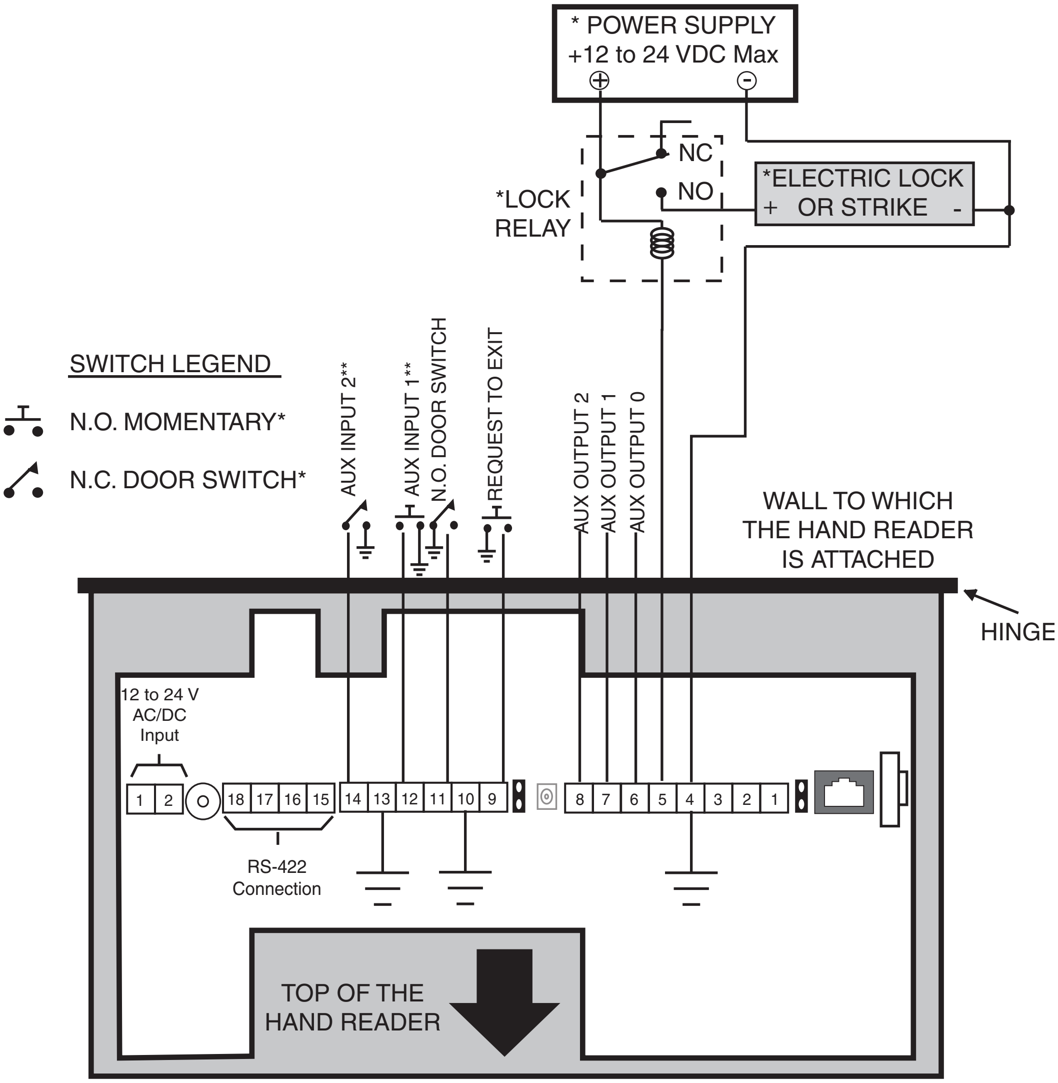
Terminal	Connection
9	Request to Exit Input
10	Ground
11	Door Monitor Switch Input (NC Standby)
12	Auxiliary Input 1
13	Ground
14	Auxiliary Input 2

Table 7-3: TS-3 - Output Connections

Terminal	Connection
1	+5 VDC @ 400mA Max. Output for External Card Reader
2	Card Reader: Wiegand D0 or Magnetic Stripe Data Input
3	Card Reader: Wiegand D1 or Magnetic Stripe Clock Input
4	Ground
5	Lock Output or Wiegand D1 or Magnetic Stripe Clock Output
6	Auxiliary Output 0 or Wiegand Data 0 or Magnetic Stripe Data Output
7	Auxiliary Output 1
8	Auxiliary Output 2

Table 7-4: RS-232 Connection

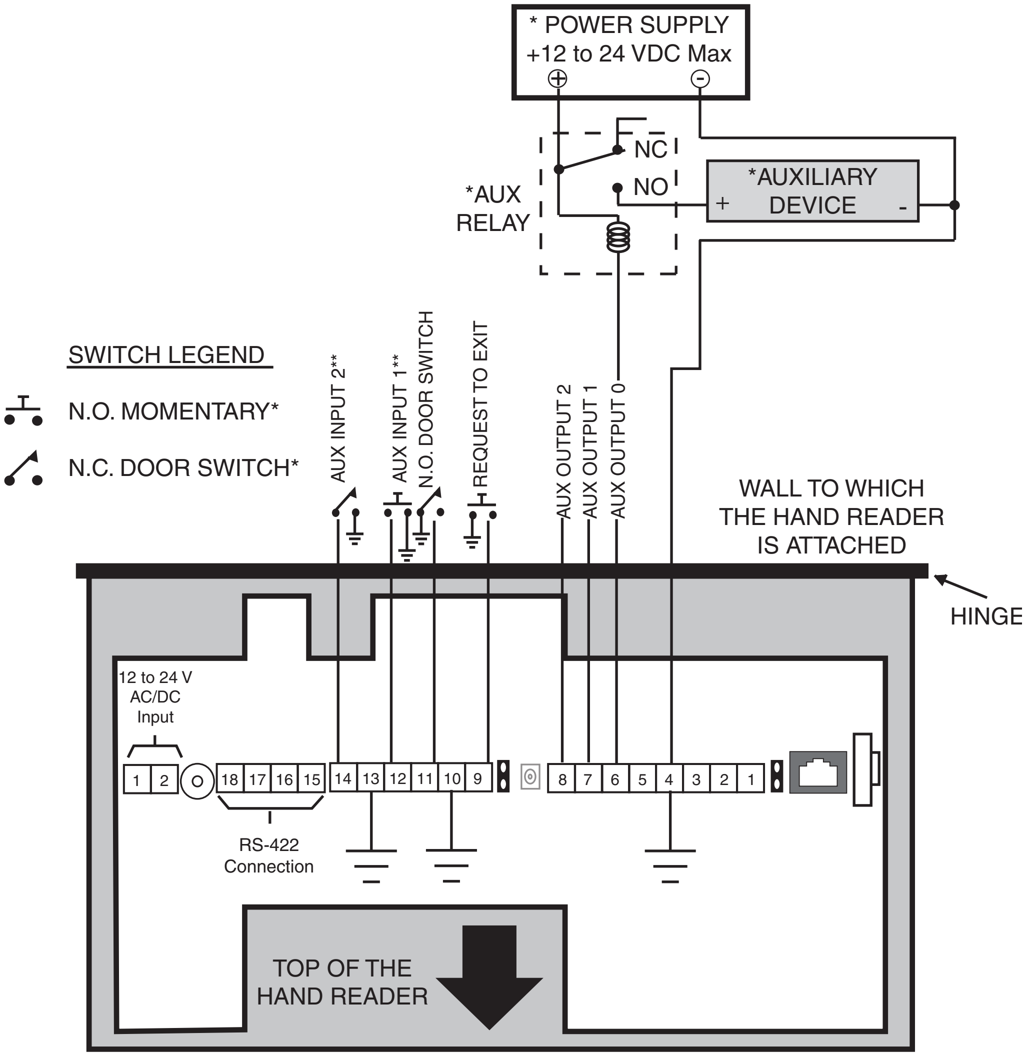
Pin	Signal	Connection
1	GND	Ground
2	RXD	Receive Data Input (from external device)
3	TXD	Transmit Data Output (to external device)
4	RTS	Ready to Send Output (to external device)



* These components are not supplied by Schlage Biometrics, Inc.

** The operation of the Auxiliary Inputs depend upon how the inputs have been configured.

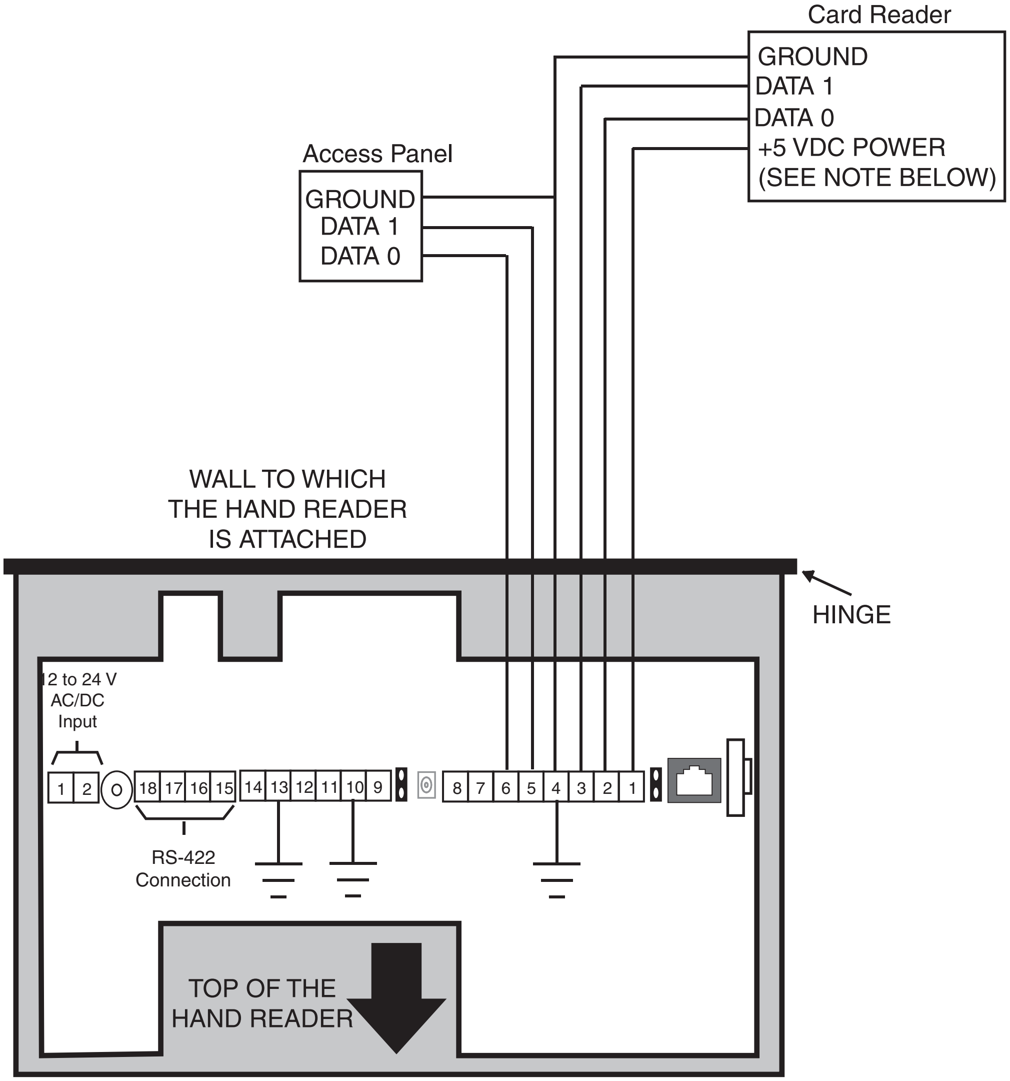
Figure 7-2: Lock Output Wiring Diagram



* These components are not supplied by Schlage Biometrics, Inc.

** The operation of the Auxiliary Inputs depend upon how the inputs have been configured.

Figure 7-3: Auxiliary Output Wiring Diagram



NOTE: For +12 VDC readers, connect power supply +12 VDC to card reader.

Figure 7-4: Card Reader Emulation Mode Wiring Diagram

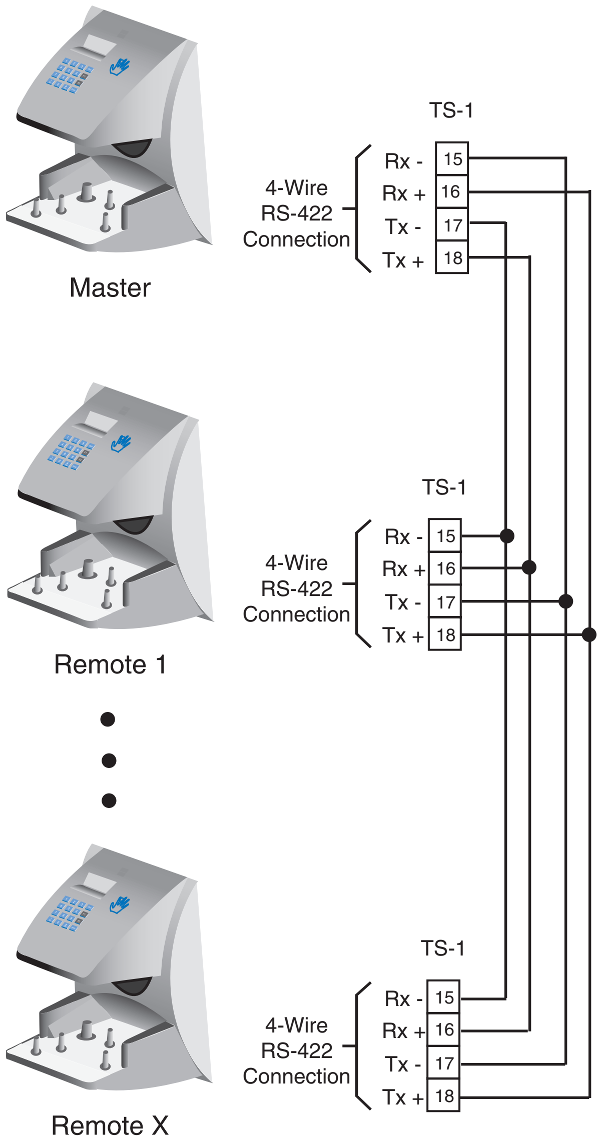


Figure 7-5: RS-422 4-Wire Master/Remote Network System Wiring Diagram

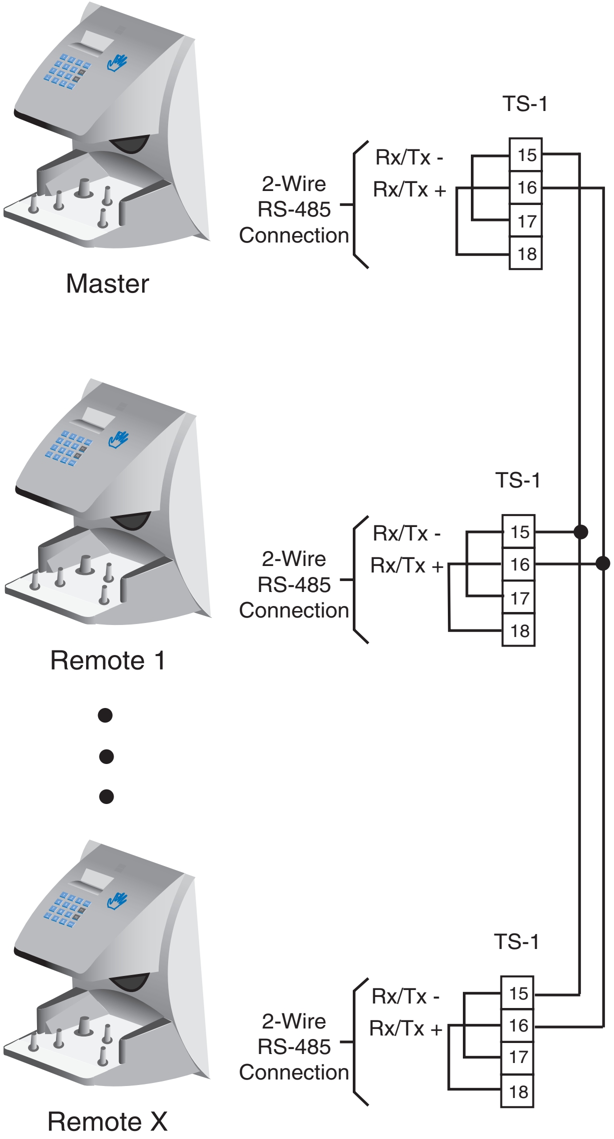


Figure 7-6: RS-485 2-Wire Master/Remote Network System Wiring Diagram

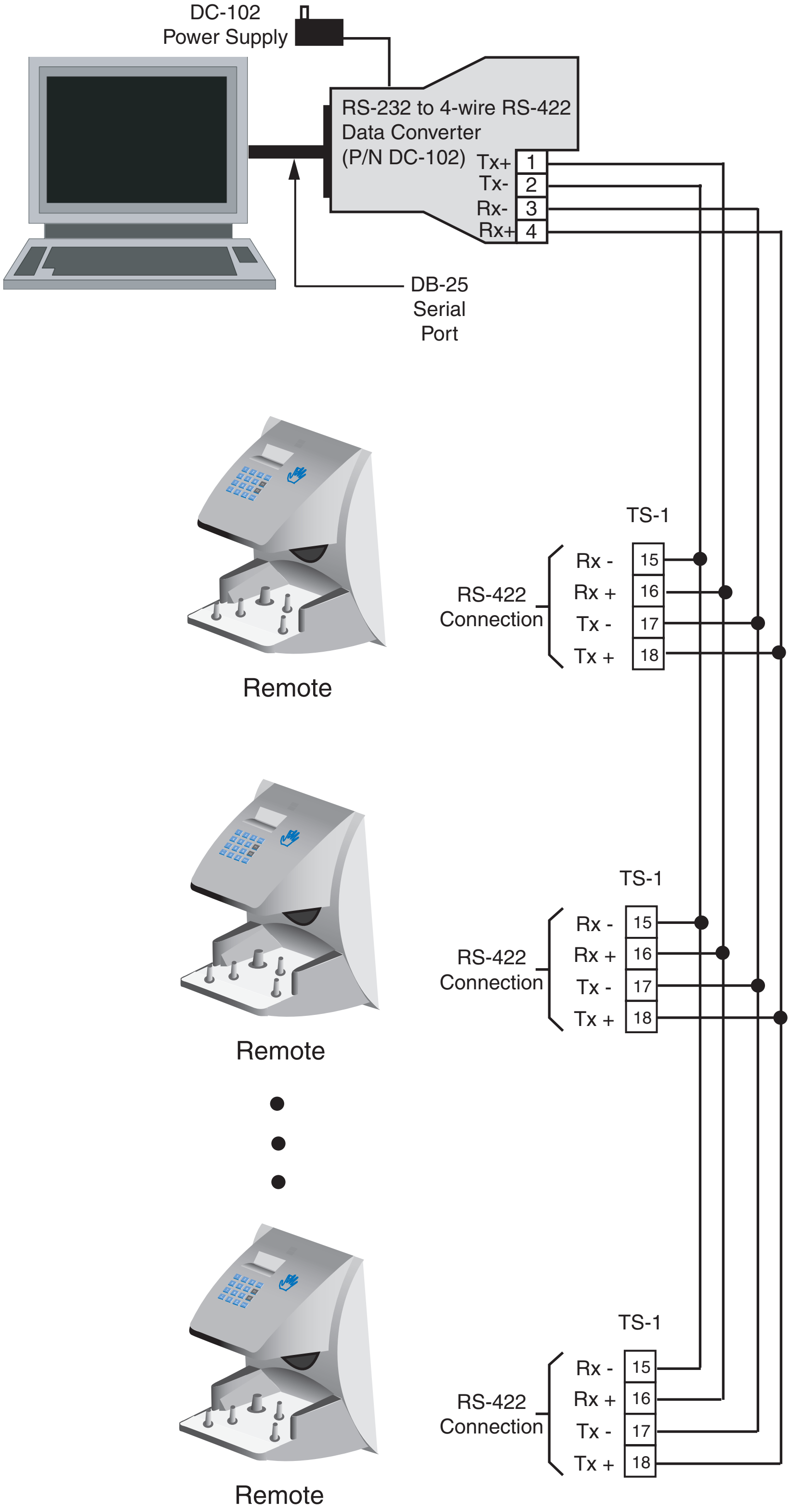
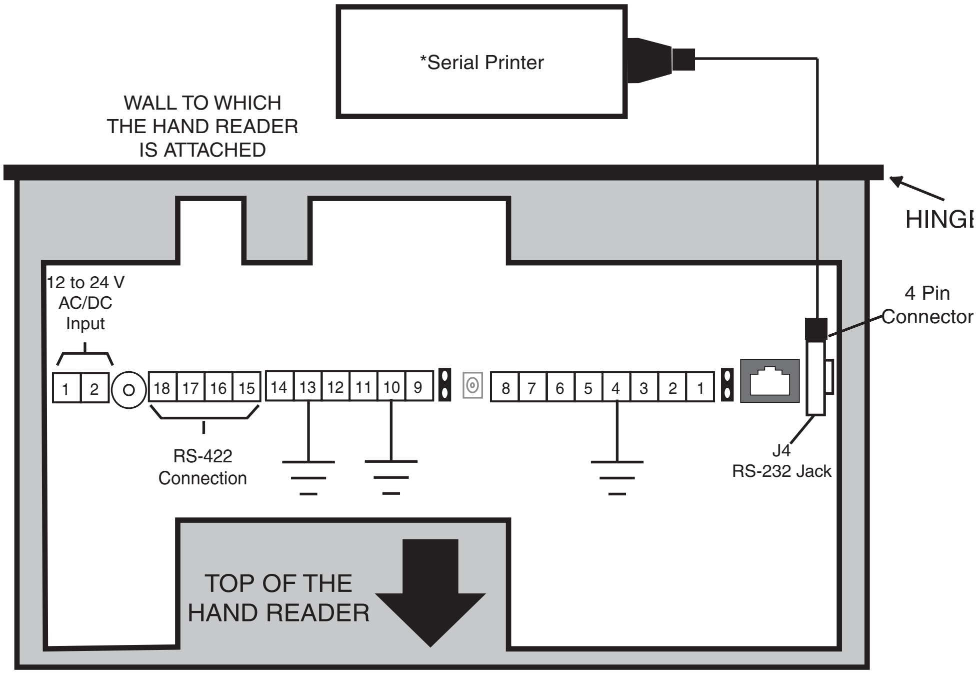


Figure 7-7: Host PC Network System Wiring Diagram



* These components are not supplied by Schlage Biometrics, Inc.

Figure 7-8: Printer to HandKey II Wiring Diagram

All HandReaders in a network must be set to the same communication method. Four-wire RS-422 cabling is required for HandNet for Windows™ network installations. Schlage Biometrics does not recommend two-wire RS-485 cabling for new network installations.

Erasing the Memory

There are two options when erasing the memory of the HandReader.

1. Setup
2. All

The erasing of the setup will set the HandReader's address, passwords, etc. back to factory defaults.

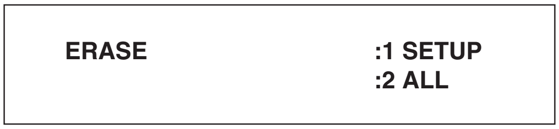
Choosing the All option will take the HandReader's setup back to factory defaults plus erase all user databases and datalogs. This action can not be undone. If there is a software that is managing the system then the users can be downloaded back to the HandReader if needed.

Erasing HandReader Memory

The erase memory function allows a HandReader's setup and/or user database to be erased.

Perform the following steps to erase the setup programs but retain the user database.

1. With system power OFF, depress reset switch.
2. Turn system power ON and wait 5 seconds.
3. LCD screen will display



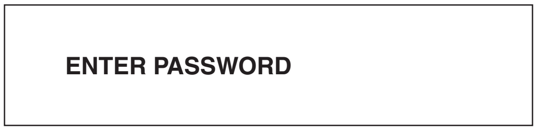
```
ERASE                    :1 SETUP
                         :2 ALL
```

Enter a Command Menu

Press the Clear and Enter keys simultaneously to enter a command menu.

If No One is Enrolled in the HandReader

1. The display appears as follows.



ENTER PASSWORD

2. Press the default password for the menu you wish to enter.

   Press 1 for the Service Menu.

   Press 2 for the Setup Menu.

   Press 3 for the Management Menu.

   Press 4 for the Enrollment Menu.

   Press 5 for the Security Menu.

3. Press Enter and the first command option in the selected menu appears.

If Users are Enrolled in the HandReader

1. The display appears as follows.

```
ENTER PASSWORD
```

2. Enter your ID number on the keypad and place your hand on the platen for verification.
3. If verification is successful, the display appears as follows.
4. Enter the password for the menu you wish to enter. The default passwords are as follows.

   Press 1 for the Service Menu.

   Press 2 for the Setup Menu.

   Press 3 for the Management Menu.

   Press 4 for the Enrollment Menu.

   Press 5 for the Security Menu.

5. Press Enter
6. If you are authorized to use this command the first command option in the selected menu appears.
7. If you are not authorized to enter this command the display appears as follows.

```
READY
*:
```

! NOTE *To access all five menus you must be the first person enrolled in a new system installation or you must have the highest authority level and the correct passwords for all five menus. If you are blocked from a menu to which you should have access, verify your access/password rights with management personnel. If authority levels or passwords have been incorrectly changed and you must have access to all menus, it is possible to reset the HandReader's memory. Resetting memory allows access to all five menus by the first person enrolled (as if it is a new system installation), but this means that any user information programmed into the HandReader must be re-entered (manually or by using HandNet software to restore the user information). Be sure you need to reset memory before performing this function. To reset memory, refer to Erasing HandReader Memory on page 31.*

Navigating Command Menus

Once an operator has entered a command menu, there are three options available for navigating the command menu system.

- Press # Yes to enter the command shown on the display.
- Press * No to step to the next command in the menu.
- Press Clear to exit the command menu (pressing any numeric key also exits the command menu). If the operator is in a command's sub-menu, the operator may have to press Clear multiple times to completely exit the command menu.

Programming the HandReader

The HandReader is programmed via a series of command menus. A summary of the menus and commands is given in Table 6.

Table 10-5: Basic Command Mode Structure

Service Menu	Setup Menu	Management Menu	Enrollment Menu	Security Menu
Password 1	**Password 2**	**Password 3**	**Password 4**	**Password 5**
Calibrate	Set Language	List Users	Add User	Set User Data
Status Display	Set Date Format	Data From Network*	Add/Remove User	Set TZ Table
Network Status*	Set Time and Date	Data to Network*		Reject Threshold
	Set Address			Set Passwords
	Set ID Length			Clear Memory
	Set Output Mode			Special Enroll
	Set Facility			
	Lock/Shunt Time			
	Aux Out Control			
	Set Reader Mode			
	Set Serial			
	Set Duress Code			
	Print Options			
	Set Beeper			
	Upgrade			

* These menu options only appear in HandReaders configured as a “Master” unit.

To control access to the command menus, each menu has a unique password. This password is requested as a part of the process for accessing each menu. A supervisor must enter the correct password for that menu to access that menu. The default menu passwords are given in Table 6.

To increase the security of the HandReader, Schlage Biometrics recommends changing the passwords for the command menus to new numbers. These password numbers can be up to 10 digits long. This is done with the Set Passwords command described on.

Authority Level

A second method for controlling access to the command menus is through the use of Authority Levels. Authority Levels control which command menus a user is allowed to access; the higher the authority level a user is granted, the greater the number of menus the user may access. Assign Authority Levels to users according to the types of tasks to which they are assigned.

- Level 0 is for a user who does not need access to any of the command menus.
- Level 1 provides access to the Service command menu.
- Level 2 adds access to the Setup command menu to all previous access levels.
- Level 3 adds access to the Management command menu to all previous access levels.
- Level 4 adds access to the Enrollment command menu to all previous access levels.
- Level 5 adds access to the Security command menu to all previous access levels.

The HandReader automatically assigns Authority Level 0 to each ID number enrolled. Until a user has been assigned to Authority Level 5, every user with Authority Level 0 can access every menu. This is done to ensure that the first person enrolled is able to access all the menus to perform all the programming required to support the HandReader. Once a user has been assigned to Authority Level 5, all other user authority levels are applied as per the list above.

! NOTE *The first person enrolled should be designated the System Administrator and should change his/her Authority Level to 5. This protects the integrity of the system by enacting the Authority Level rules described in the list above. Schlage Biometrics strongly recommends assigning at least two users to Authority Level 5 to ensure that more than one person has the authority to access all menus and all commands.*

Programming Order

When setting up HandReader operations there is a general programming/operations order that should be followed.

1. Design an ID Numbering System – Define the format for user ID assignments. A properly designed ID numbering system makes the HandReader easier and faster to use.
2. Enter a Command Menu – Enter a Command Menu and begin HandReader programming per the commands in that menu.
3. Enroll all Supervisory Staff – Enroll yourself and the supervisors who will have responsibility for HandReader management. This is done through the Enrollment Menu.
4. Set Supervisory Staff Authority Levels – Assign Authority Levels to the supervisors with specific HandReader management responsibilities. This is done through the Security Menu.
5. Set Reader Site Parameters – Set the reader's Operating Parameters to meet site specific needs and usage. This is done through the Setup Menu.
6. Train and Enroll Users – Train each user regarding HandReader usage and then Enroll each user. This is done through the Enrollment Menu.

System Management and Maintenance

Once a HandReader network is in operation the following commands are used to manage and maintain the HandReader network.

1. Set Reader Operating Thresholds – Set the Reject and Number-of-Tries HandReader operating thresholds to meet the site's security requirements. This is done through the Security Menu.
2. System Management – Backup or Restore HandReader data and List the Users authorized to use a HandReader. This is done through the Management Menu.
3. System Maintenance – Calibrate the HandReader, display HandReader Status, and display Network Status. This is done through the Service Menu.

! NOTE *For documentation clarity, instructions for operating each of the menu commands are presented in menu order, which is not necessarily programming order. Please keep this in mind as you review the commands for all of the menu options.*

Design an ID Numbering System

The ID numbering system helps identify the user about to use the HandReader. ID numbers are used when enrolling users. A properly designed ID numbering system allows for quicker user recognition (through the use of the Set ID Length command) and allows the assigning of a Duress code. A Duress code sends a silent alarm to a pre-defined location when entered by a user. Use the following guidelines when designing an ID numbering system.

! NOTE *Designing an ID numbering system is not necessary when using an external card reader to enter the ID number. All ID information is provided by the card.*

- Each user must have a unique ID number.
- ID numbers can be up to 10 digits long.
- For ease of memorization, make each number as short as possible. Generally speaking, 4 digit or fewer ID numbers are easy to remember.
- Make all ID numbers the same length. This allows the Set ID Length command to be used, automatically reading an ID number when the proper number of digits have been entered. If different ID number lengths are used, a user must press the # key to identify when the complete ID number has been entered.
- To use the Duress feature, ID numbers must begin with one specific digit that has been identified as the Duress code and this digit cannot be used as the first digit in any of the user ID numbers. This means that in normal use a user enters his/her ID number followed by the # key. To create a Duress alarm, the user enter the Duress code, the user's ID number, and the # key. The Set ID Length command cannot be used if the Duress feature is used.

Service Menu

The Service Menu commands provide information that helps you determine if the HandReader is operating properly and within normal operating parameters.

Navigating the Service Menu

Once you have entered the Service menu, there are three options available for navigating the command menu system.

- Press # Yes to enter the command shown on the display.
- Press * No to step to the next command in the menu.
- Press Clear to exit the command menu (pressing any numeric key also exits the command menu). If you are in a command's sub-menu, you may have to press Clear multiple times to completely exit the command menu.

Service Commands

There are three commands available from the Service command menu.

- Calibrate – Run calibration to check HandReader exposure values.
- Status Display – Check the status of HandReader inputs and outputs, the hand read score of the last user to verify on the system.
- Network Status – Check the network communication status of HandReaders in the HandKey system (master HandReader only).

Refer to and identify the commands you need to perform. Step through all previous commands until you reach the desired command. All commands are listed in menu order.

Table 11-6: Service Command Menu

Service Menu
Password = 1
Calibrate
Recal (N/Y)
Status Display
On/Off (Y/N)
Network Status
Status Information

Calibrate

The Calibrate command verify that the HandReader's exposure values are within normal operating parameters. The normal operating parameters are shown in Table 2.

Table 11-7: Normal Operating Parameters

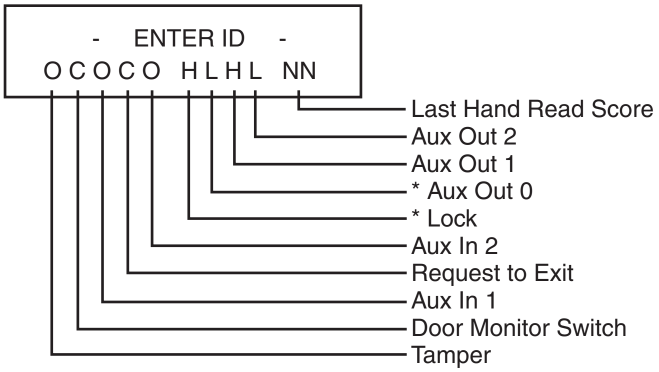
Parameter	Normal Range
Row "r"	0 +/- 2
Column "c"	0 +/- 2
Exposure	100 +/- 20

Status Display

The status display command allows you to enable or disable the displaying of the following information.

- the status values of HandReader inputs and outputs
- the hand read score of the last user to verify on the HandReader

Figure 11-1 on page 40 identifies each status display field value.



* These status values are inactive if the reader is in Card Reader Output Mode.

O = Circuit Open	H = Output is OFF (High)
C = Circuit Closed	L = Output is ON (Low)

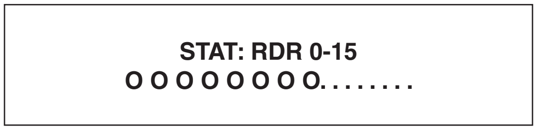
Figure 11-1: Status Display Chart

Network Status

The network status command allows you to check the network communication status of the HandReaders in the HandKey system.

! NOTE *You can check network status only from the Master HandReader in a master/remote HandReader network.*

Network status is displayed by reader address, 16 units at a time.



```
STAT: RDR 0-15
OOOOOOOO........
```

Each "O" and "." represents a HandReader address in the network. An "O" indicates that the HandReader corresponding to that address is communicating on the network. A "." indicates that the HandReader with that address is not communicating on the network.

Setup Menu

The Setup menu commands allow you to set the basic operating parameters for the HandReader.

! NOTE *Once in the Setup menu you can step through and set the parameters for each command sequentially. You do not have to exit command mode after setting any individual command.*

Navigating the Setup Menu

Once you have entered the Setup menu, there are three options available for navigating the command menu system.

Press # Yes to enter the command shown on the display.

Press * No to step to the next command in the menu.

Press Clear to exit the command menu (pressing any numeric key also exits the command menu). If you are in a command's sub-menu, you may have to press Clear multiple times to completely exit the command menu.

Setup Commands

There are 12 commands available from the Setup command menu.

- Set Language
- Set Date Format
- Set Time and Date
- Set Address
- Set ID Length
- Set Facility
- Aux Out Control
- Set Reader Mode
- Set Serial
- Set Duress Code
- Set Beeper
- Upgrade

Refer to and identify the command you need to perform. Step through all previous commands until you reach the desired command.

Table 12-8: Setup Command Menu

Setup Menu **Password = 2**
Set Language
Select Language
Set Date Format
Select Date Format
Set Time and Date
Month (MM)
Day (DD)
Year (YY)
Hour (HH)
Minute (MM)
Set Address
New Address
Set ID Length
New ID Length
Set Facility
Auxiliary Output Control
Select Auxiliary Output 1/2
Aux 1 Out Control
Aux 2 Out Control
Output Set by Tamper
Output Set by ID Refused
Output Set by Duress
Output Set by Try Again
Output Set by F1 Key
Output Set by F2 Key
Output Set on Battery Backup
Auxiliary Output Cleared by Timer
Aux Output Cleared by Valid Access
Set Reader Mode
To Master/Remote
Set Serial
RS-422 (Y/N)
Select Baud Rate
RS-232 (Y/N)
Select Baud Rate
Use RS-232 for Printer or Host
Set Seriala
Verify/Enter IP Address
Verify/Enter Gateway
Verify/Enter Host Bit
Set Duress Code
Enter Duress Code
Set Beeper
Turn Beeper On/Off (Y/N)
Upgrade
Enter Code

Set Language

The Set Language command allows the language shown on the HandReader's display to be "localized" for a variety of countries. The default language is English. The following languages are available.

English
French
German
Indonesian
Italian
Japanese
Polish
Portuguese
Russian
Spanish

Set Date Format

The Set Date Format command allows the date format shown on the HandReader's display to be "localized" for a variety of countries. The default date format is the U.S. standard date format – MM/DD/YY. The following date formats are available.

mm/dd/yy
dd-MMM-yy
dd-mm-yy
dd/mm/yy
mm-dd-yy
MMM dd,yy
ddMMMyyyy

Set Time and Date

The Set Time and Date command allows the HandReader's time and date to be set. If the HandReader is networked to a PC, this step is not necessary as the HandReader's time and date will be set by the host computer.

! NOTE *Stand-alone HandReaders and HandReaders on a master/remote HandReader network require adjustment for the daylight savings time changes. HandReaders networked to a host PC do not require adjustment as the host PC automatically makes the adjustment.*

Time is kept using a 24-hour clock. The time is set in the following format.
Hour: two digits – 00 to 23
Minute: two digits – 00 to 59

The date is set in the following format.
Month: two digits – January = 01, incrementing to December = 12
Day: two digits – 01 through 31
Year: two digits – enter the last two digits of the current year (i.e. 2001 = 01)

Set Address

The Set Address command allows a unique address to be set for each HandReader in a network. For proper operation, each HandReader in the network must have a unique address. Addresses 0 to 254 are available – address 255 is reserved for the master HandReader in a network. The default address is 0. An address does not need to be set for stand-alone HandReaders.

Set ID Length

The Set ID Length command allows you to reduce the number of keystrokes required to enter the ID number by eliminating the use of the key to complete an ID number entry. Once the ID Length is set, when a user enters an ID number the HandReader will automatically accept that number once the correct number of characters have been entered. Set ID Length does not apply when ID entry is made from a card reader. Set ID Length cannot be used if a Duress Code has been assigned.

Set the ID Length to the number of digits in the longest ID number. This command is unnecessary (and should be left at its default value) if ID entry is made from a card reader. The ID Length should not be set if a Duress Code is being assigned (see page 49). The default value for ID Length is 10.

! NOTE *Users assigned ID numbers shorter than the number of digits in the longest ID number must press following their ID entry to indicate the complete entry has been made.*

Set Facility

The Set Facility command allows the facility code to be entered in HandReaders configured for card reader emulation output mode. A facility code is not valid or required for HandReaders configured in Lock/Aux output mode.

Set the Facility Code to match the code expected by the access control panel. This command is unnecessary (and should be left at its default value) if the output mode is set to Lock and Auxiliary Output Mode. The default facility code value is 50.

! NOTE *When using a HandKey II on a Wiegand format access control panel and a keypad is used for ID entry, you must set the site code to the access control panel's facility code. Without a matching code the access control panel will deny access to HandKey users.*

Aux Out Control

The Aux Out Control command allows the Auxiliary Outputs in the HandReader to be set to trigger based on selected events. Alarms can be mapped to appropriate Auxiliary Outputs. Outputs are also cleared in this menu option.

Outputs 1, and 2 can be connected to a variety of peripheral devices such as audible or silent alarms, door locks, or lighting systems. Verify HandReader/peripheral wiring is correct and that the peripheral meets HandReader/system specifications before changing the output settings. Table 10 describes the Auxiliary Output choices.

Table 12-9: Auxiliary Output Choices

Auxiliary Output	Function
Auxiliary Output 1	Auxiliary 1 switched to ground
Auxiliary Output 2	Auxiliary 2 switched to ground
Tamper	HandReader opened, shaken, or removed.
ID Refused	User not verified after allowed number of tries.
Duress	User entered the duress code digit.
Try Again	User rejected.
F1 Key	F1 key pressed.
F2 Key	F2 key pressed.
On Battery Backup	AC power failure, HandReader switched to battery power.

Set Reader Mode

The Set Reader Mode command allows a HandReader to be set as the Master HandReader in a HandReader network. All user enrollment is done through the Master HandReader. The Master HandReader automatically downloads user data to all remote HandReaders on the network. The Reader Mode does not need to be set for stand-alone HandReaders and PC networks.

In HandReader networks, one HandReader must be set as a Master HandReader and all remaining HandReaders must be set as Remote HandReaders. The default Reader Mode is Remote mode. Reader Mode does not apply to stand-alone HandReaders or HandReaders in a PC network (the HandReader should be left in its default value).

! NOTE *All remote HandReaders on a HandReader network must have a unique address. Refer to the Set Reader Address section on page 43.*

The HandReader's display can tell you if a reader has been configured as a Master Reader or a Remote Reader.

A Master Reader has double-dashes surrounding the "READY" text.

```
=     READY     =
TIME       DATE
```

A Remote Reader has single-dashes surrounding the "READY" text.

```
-     READY     -
TIME       DATE
```

Set Serial

The Set Serial command allows you to select either the RS-485, RS-422 or RS-232 communication mode and to set the baud rate for the selected communication mode. The default baud rate is 9600 bps which is suitable for most network communication applications. If the HandReader uses the Ethernet communication option, the TCP/IP address, gateway, and host bit parameters are set instead of the baud rate.

Set Duress Code

The Set Duress Code command allows a special digit code to be defined that, when entered before a user's PIN entry, sends a silent alarm to security personnel using an auxiliary output. This function only works with keypad ID number entry systems – it does not work with Card Reader entry systems. If a Duress Code is set, an ID Length cannot be set by the Set ID Length command.

! NOTE *For this function to work properly the following must be true: an auxiliary output must be defined to activate on DURESS and assigned ID numbers cannot begin with the duress code number.*

Set Beeper

The Set Beeper command allows the beeper to be enabled or disabled. When enabled, the beeper sounds an audible response to key strokes and events.

Upgrade

For instructions on how to upgrade the memory of the HandReader please refer to the Memory Upgrade Note.

Management Menu

The Management menu commands allow you to manage employee data stored in a HandReader.

Navigating the Management Menu

Once you have entered the Management menu, there are three options available for navigating the command menu system.

- Press # Yes to enter the command shown on the display.
- Press * No to step to the next command in the menu.
- Press Clear to exit the command menu (pressing any numeric key also exits the command menu). If you are in a command's sub-menu, you may have to press Clear multiple times to completely exit the command menu.

Management Commands

There are three commands available from the Management command menu.

- List Users – display or print a list of all the users enrolled in a HandReader.
- Data From Network – upload data from the network to the master HandReader.
- Data To Network – download data from a master HandReader to the network.

Refer to Table 11 and identify the command you need to perform. Step through all previous commands until you reach the desired command.

Table 13-10: Management Command Menu

Management Menu **Password = 3**
List Users
Display or Print
Data from Network
Select Reader
Data to Networka
All Readers (Y/N)
Select Reader

List Users

The List Users command displays or prints a list of all the users enrolled in a HandReader. The list is shown, one user at a time, on the HandReader's display, or it is printed by a serial printer attached to the HandReader being polled or to a printer attached to the Master HandReader in a HandReader network. Before displaying the user list, the amount of memory available for enrolling more users is displayed.

Data From Network

The Data from Network command allows the master HandReader to receive information from a HandReader on the network. This is used to transmit user enrollment and system configuration information from an existing HandReader to the master HandReader.

Data To Network

The Data to Network command transmits all data held by the master HandReader to all HandReaders connected to the network. This is used to transmit user enrollment and system configuration information to all HandReaders on the network.

Enrollment Menu

Enrollment is the process of recording a hand image and associating it with an ID number. The first person to enroll in the HandReader has access to all command menus. This person should be considered the System Administrator and should retain the highest authority level to access all five menus at any time.[1]

As other users are enrolled they can be left as basic access users or they can be assigned varying degrees of authority depending upon the tasks for which they will be responsible.

Advance planning and training make enrollment fast and easy. Users should be informed on what to expect and how to place their hands on the HandReader before you enroll them.

Preparation

Here are a few guidelines to help you prepare for an enrollment session.

- You can enroll one person or a group of people during an enrollment session.
- Each user must have a unique personal identification (ID) number. It will save you considerable time if you assign the ID numbers in advance.[2]
- The HandReader will not accept two people with the same ID number.
- If you enroll people using the last four digits of their phone numbers or social security numbers, you may get duplicate numbers.
- If you plan to use the Duress function, do not enroll ID numbers that begin with the Duress code digit.[3]
- If you are enrolling large groups of people you may consider using an enrollment trainer. It is a replica of a platen that is available through your Schlage Biometrics dealer.

[1] Refer to the Set User Data > Set Authority Level command in the Security command menu on page 55.

[2] Refer to the Design an ID Numbering System section on page 37.

[3] Refer to the Set Duress Code command in the Setup command menu on page 45.

User Education

The HandReader is easy to use and non-threatening. However, most people have never used a biometric HandReader. Training users on how the HandReader works and how to use it will eliminate most fears and concerns before they occur. Inform the users of these facts.

- The HandReader reads the shape of the hand, not the fingerprints or palmprints.
- It does not identify people. It confirms people's identity.
- It scans with an invisible light of the type used in TV remote controls.
- It does not transfer germs any more than a doorknob or money.
- It does not invade privacy; it guarantees it.
- The enrollment process requires three or more reads to collect enough information to verify the user's identity.

Proper Hand Placement

For correct, consistent hand reads it is very important that your hand is placed on the platen in the same manner every time (see Figure 12-1). The following rules apply for proper hand placement on the platen.

- If you are wearing a ring, rotate the ring so the stone faces up in its normal position.
- Slide your right hand onto the platen rather like an airplane landing at the airport.
- Slide your hand forward until the web between your index and middle finger stops against the Web Pin.
- Keep your hand flat. You should feel the surface of the platen on your palm and the underside of your fingers.
- Close your fingers together until they touch the Finger Pins and watch the hand diagram light display on the top panel.
- The lights go out when you have properly placed your fingers. If a light remains on, a finger is not in proper contact with its Finger Pin.

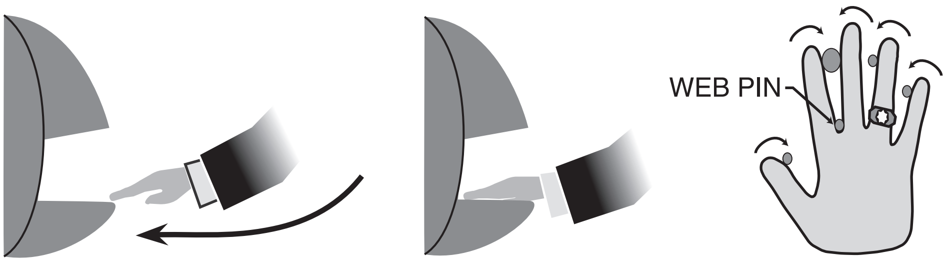


Figure 14-1: Placing Your Hand on the Platen

Left Hand Enrollment

Some right hands are not suitable for use in the HandReader due to disabilities such as missing fingers. You can enroll a user with the left hand facing palm side up. The techniques for left hand enrollment are the same as for standard enrollment. The user should keep the back of the hand flat against the platen and move the fingers against the web pin and the finger pins in the same manner as in standard enrollment. Users enrolled with the left hand must always verify with the left hand. Extra practice on placing the hand on the platen may be required to ensure correct, consistent hand reads.

Read Score

When a user uses the HandReader a number appears in the display.

ID VERIFIED
##

The number on the display reflects how accurately the user is placing his/her hand on the platen. Scores that vary greatly between low and high numbers are indicative of inconsistent hand placement. Scores above 50 are indicative of improper hand placement or of a drastic change in the physical appearance of the hand.

When this occurs, emphasize the importance of sliding the hand onto the platen and keeping the hand flat. Re-training and practice should lower a user's score. It might be necessary to change a user's sensitivity if the user has a mild disability. Re-enrollment might be necessary to create a new user template.

Navigating the Enrollment Menu

Once you have entered the Enrollment menu, there are three options available for navigating the command menu system.

- Press # Yes to enter the command shown on the display.
- Press * No to step to the next command in the menu.
- Press Clear to exit the command menu (pressing any numeric key also exits the command menu). If you are in a command's sub-menu, you may have to press Clear multiple times to completely exit the command menu.

Enrollment Commands

There are two commands available from the enrollment command menu.

- Add User
- Remove User

Refer to Table 12 and identify the command you need to perform. Step through all previous commands until you reach the desired command.

Table 14-11: Enrollment Command Menu

Enrollment Menu Password = 4
Add User
ID #
Remove User
ID #

Add User

The Add User command allows you to enroll a new employee into the HandReader.

Remove User

The Remove User command allows you to remove an employee from the HandReader.

! NOTE *Once a user has been removed from the HandReader, that user no longer has access through the door controlled by that HandReader. To be granted access again, that user must be re-enrolled.*

Security Menu

The commands in the Security menu control the security of the information within the HandReader and the sensitivity of the HandReader when reading hands.

Navigating the Security Menu

Once you have entered the Security menu, there are three options available for navigating the command menu system.

Press # Yes to enter the command shown on the display.

Press * No to step to the next command in the menu.

Press Clear to exit the command menu (pressing any numeric key also exits the command menu). If you are in a command's sub-menu, you may have to press Clear multiple times to completely exit the command menu.

Security Commands

The Security menu has six primary commands.

- Set User Data
- Set TZ Table
- Reject Threshold
- Set Passwords
- Clear Memory
- Special Enroll

Refer to table 13 and identify the command you need to perform. Step through all previous commands until you reach the desired command.

Table 15-12: Security Command Menu

Security Menu **Password = 5**
Set User Data
Set User Authority Level (Y/N)
ID #
Authority Level
Set User Reject Level
ID #
Reject at #
Set User Time Zone
ID #
New Time Zone?
Edit Time Zone
Time Zone #
Time Zone Data
Print Time Zone
Clear Time Zone
Time Zone #
Edit Holidays
Enter Month and Day
Print Holidays
Clear Holidays
Holiday Month
Set Unlock Time Zone
Time Zone #
Set Reject Threshold
Reject Threshold #
of Tries
Set Passwords
Security Password
Enroll Password
Management Password
Setup Password
Service Password
Clear Memory
Special Enroll
ID #
Time Zone #

Set User Data

The Set User Data command allows you to set the User Authority level, the User Reject Level, and the User Time Zone.

- The Authority Level controls which command menus a user is allowed to access; the higher the authority level, the greater the number of menus the user may access.
- The User Reject level allows you to set the number of failed hand read attempts for a user before rejecting further attempts by that user.
- The User Time Zone allows you to assign a time zone to a user, restricting the time-of-day that a user may be granted access.

Set TZ Table

The Set TZ Table command allows you to create or edit Time Zone and Holiday tables. A time zone is an identified period-of-time and days-of-the-week, during which a user is allowed access to an area secured by a HandReader. Once a user is assigned a Time Zone, access attempts outside of that time/date period are rejected by the HandReader.

A time zone may be "split." This means that a time zone may identify more than one set of period-of-time and days-of-the-week – up to four sets in one time zone. This provides a great deal of flexibility in providing secured access through a HandReader.

Time Zone information can also be printed for review or cleared if a time zone becomes unnecessary.

! **NOTE** *All time entries made for time zones are entered in 24-hour format. For example, 8 A.M. is entered as 08:00, 5 P.M. is entered as 17:00, and 11 P.M is entered as 23:00.*

The Holiday schedule for a calendar year can be entered. Once a holiday schedule is set, holidays are applied to time zones just like another day of the week (1 to 7 for the days of the week, 8 for holidays). Once entered, the holiday schedule can be printed for review and cleared.

! **NOTE** *Certain holidays, such as Easter and Thanksgiving, change their days from year to year. You must review and edit your holiday schedule each year to ensure the correct days are counted as holidays.*

An Unlock Time Zone can also be set. The unlock time zone is a special time zone that automatically unlocks the door associated with a HandReader when the time zone is active, and then automatically locks that door when the time zone becomes inactive. This can be used on doors where general access is allowed during specific times of the day (such as business hours).

Reject Threshold

Use the Reject Threshold command to set the HandReader's reject sensitivity level applied when reading hand data and to set the number of tries a user is allowed before being rejected by a HandReader.

The reject sensitivity level and number of tries are global values. This means that these values are applied to all users on all HandReaders on the network – except for those users who have been assigned an individual user reject level (refer to the Set User Reject Level command on page 54).

The default reject threshold is 100. This is the best threshold value for most applications.

- Raising the threshold level makes the HandReader less sensitive to variations in user hand placement on the platen.
- Lowering the threshold level might result in a greater number of rejected attempts, but also results in a more secure system.

The default number of tries is 3. If a user exceeds the number of tries without a valid hand read, the HandReader will refuse all subsequent attempts with that user ID number. This means the user will be locked out until another user is verified successfully.

Set Passwords

Use the Set Passwords command to change the passwords assigned to each of the five command menus. To increase the security of the HandReader, the password for any or all menus can be changed to a new number, up to 10 digits long. This means that to enter a command menu, a user must have the correct Authority Level (refer to page 54) and must enter the correct password.

Clear Memory

Use the Clear Memory command to clear the user data from the HandReader, but retain the setup data. This allows you to clear the HandReader's user database of all templates and ID numbers, but retain all HandReader setup information. Typically, this is done when moving the HandReader to a new location with different users but the same setup requirements.

! **NOTE** *Use this command with caution. Once user data is cleared from the HandReader's memory the user data is not recoverable.*

Special Enroll

Allows a user to be enrolled such that the ID number is the primary criteria for determining access. A hand read is required, but is not verified against any stored identification data. A time zone value can also be applied to the Special Enrollment ID number to increase access limits. The default is for no time zone to be applied.

! **NOTE** *Special Enrollment affects the integrity of the HandReader network and should only be used as a last resort. Anyone who knows a Special Enroll ID number is granted access when the ID number is used. Before specially enrolling a user, try to alleviate verification problems by adjusting the individual user's reject threshold (see page 55).*

HandReader Maintenance

A minimum amount of system maintenance is required to keep HandReaders fully functional. HandReaders should be cleaned periodically to prevent an accumulation of dust from affecting the HandReader's readability. User Scores should be reviewed periodically to ensure the HandReader is performing properly.

! NOTE *There are NO user serviceable parts inside the HandReader.*

Once a HandKey system is in operation there are three HandReader commands that can assist with system maintenance. These commands are performed through the Service Menu. The instructions for these commands begin on page 39.

- Calibrate – View Hand Reader exposure values.
- Status Display – Display Hand Reader input/output status, the hand read score of the last user to verify on the system.
- Network Status – Display the network communication status of Hand Readers in the HandKey system (master Hand Reader only).

Cleaning the Hand Reader

Inspect and clean the HandReader regularly to maintain optimum performance. Clean the platen, side mirror, reflector, and the window above the platen using a clean cloth dampened with ordinary, non-abrasive window cleaner (see Figure 14-1). Start at the rear corners of the platen and work your way forward.

! NOTE *DO NOT SPRAY CLEANING FLUID DIRECTLY INTO OR ON THE HAND READER.*

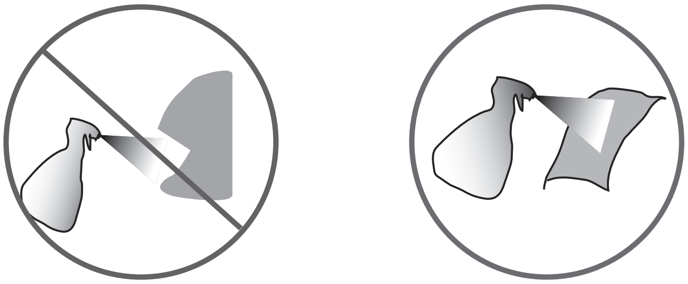


Figure 16-1: HandReader Cleaning

User Score

Periodically check users' scores (refer to the Read Score section on page 51). Scores should average under 30. Occasionally a user will score above 30. This is not necessarily an indication of poor performance. If a number of scores average over 30, clean the HandReader and check scores again. If scores remain high, or if users are experiencing frequent rejections, run the Calibration command (see page 40).

Appendix A: Tips for a Successful Installation

Unless the following tips are followed, the installation runs the risk of having some level of difficulties. These tips come from years of experience with thousands of sites installed around the world. By far the biggest problem tends to be that the HandReader is allowed to get dirty. Think of the HandReader as a camera, because that is exactly what it is. If a user takes a picture with a dirty camera, then what you get is a dirty picture.

Location and Installation

If a user would have to place their body in an awkward or dangerous position to use the HandReader then that probably is not the correct location for a HandReader.

- Mount all HandReaders in a network so that the top of the platen is 40" off of the floor
- If an enrollment HandReader is used make sure that it is placed with the top of the platen 40" off of the floor and not sitting directly on top of a desk, this will help to eliminate "bad enrollments"
- Mount the HandReader so that it is not difficult or dangerous to verify then open the door
- It is not recommended to mount the HandReader in an area where there is airborne dust, in the path of direct sunlight, or where the HandReader can be exposed to water or corrosive gasses
- Do not remove the foam backing from the wall mounting plate
- Seal any holes made in the wall for wire routing, so that dust will not blow into the HandReader. Walls act as billows as the pressure changes in a room (opening and closing a door can cause this).

HandReader

It is extremely important to keep the HandReader clean. If a HandReader is not kept clean verification issues will ensue. This is especially true in a networked environment, all HandReaders should be at the same level of cleanliness for optimum performance.

- Think of the HandReader as a camera
- Clean the HandReader before it gets dirty
- Use non-abrasive cleaners such as glass cleaners and non-abrasive cleaning cloths
- Make the cleaning of the HandReader part of the Janitorial program
- Never spray cleaner directly into the HandReader
- "Recalibrate" after cleaning the HandReader

Enrollment

Bad enrollments equal bad verification (meaning scores will be too high). The key to successful verification is education.

- Educate the Enrollee on Hand Geometry
- Explain enrollment process
- Train Enrollee on hand placement
    - Practice placing hand on platen
    - Rotate rings to be stone-up
    - Make sure hand is flat on platen
    - Close finger towards the center of hand
    - Fingers need only to gently touch finger pins
- Let the enrollee enter in their own ID number during the enrollment process, this forces the Enroller to step aside allowing the Enrollee to properly stand in front of the HandReader helping to eliminate “bad enrollments”
- If an enrollment HandReader is used make sure that it is placed with the top of the platen 40” off of the floor and not sitting directly on top of a desk, this will help to eliminate “bad enrollments”
- If an enrollment transaction fails:
    - Retrain the user on correct placement and ensure that rings are rotated to be stone-up then
    - Try again to enroll the same hand
    - Try to enroll the other hand (with the hand placed upside-down so the thumb still contacts the thumb-pin on the platen)
- After enrollment, it is a good idea to let the enrollee enter their ID number and practice a verification transaction to ensure that the enrollment was high-quality
- If a user consistently fails during verifications days/months/years later, re-enroll the user to ensure a high quality and up-to-date enrollment record

Communication

Direct

- Use shielded cable when installing direct networks. This will help reduce outside noise interference
- Do not lay cabling on top of fluorescent lighting. Make sure the Data Convertor is plugged in
- When starting a network for the first time bring one HandReader up at a time, this is a very easy way to find out where communication problems may exist

Modem

- Use default init string for modem first
- Do not set the baud rate of the HandReader down below 9600, unless communicating in a E series network (metal HandReaders), or risk over-running buffers
- In the init string set the line rate to 14400
- Use analog lines (POTS)
- Troubleshooting by plugging the HandReader on the fax machine’s phone line

Ethernet

- make sure network cable is plugged in to Ethernet card before powering up the HandReader
- Port 3001 must be set on all switches and routers in order to successfully communicate over WANs
- If the HandReader can be “pinged” but will not communicate with the software, power down the HandReader and run “ping” again

Appendix B: Noted Board Configuration Differences

Because of Schlage Biometrics' camera retrofit of the HandReader some changes have been made to the main PCB and they are listed as follows:

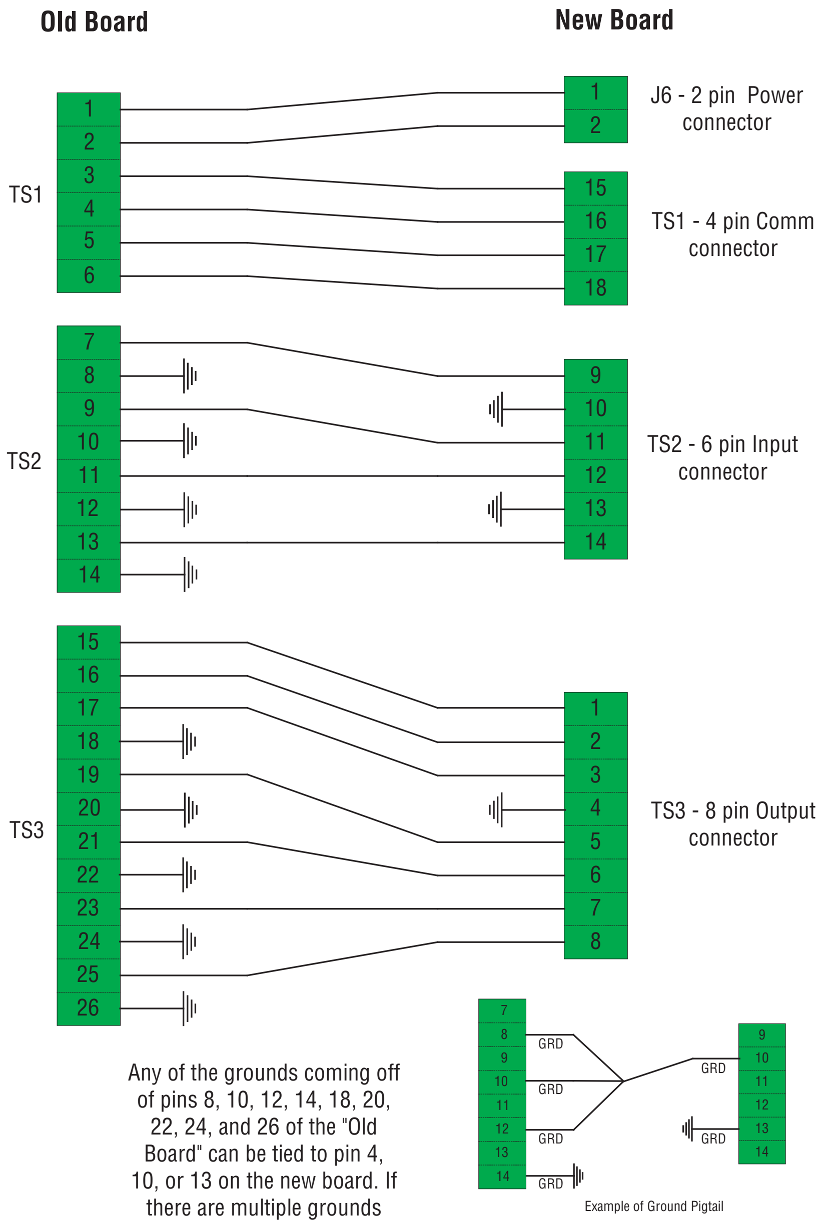
- Dipswitches have been removed
  - comm lines are terminated
  - RS-485 is set by wiring jumpers
  - memory is reset with a push-button reset and user interface with keypad and LCD
- The labeling of the terminal strips have changed. See Figure 16-1
- The configuration of the terminal strips have changed. See Figure 16-2
- Power has moved to the right side of the PCB
- The RSS-232 RJ-45 receptacle has been replaced with a 4 pin Molex connector on the left side of the PCB
- A 2 pin Molex connector (J5) has been added to the board, next to the reset button, to supply power for the LEDs. This connector should never be unplugged. unless a modem or Ethernet is added to the PCB
- The upgrading of the memory is now handled through software codes at the HandReader. Contact Order Entry for memory upgrades

Terminal Block Labeling

Number	OLD PCB	Number	NEW PCB
1	12-24 VDC (+) OR VAC	1	(+) 5 VDC OUTPUT
2	12-24 VDC (-) OR VAC	2	DATA/D0
3*	RX-	3	CLOCK/D1
4*	RX+	4	GROUND
5*	TX-	5	LOCK OR CLOCK OUTPUT
6*	TX+	6	BELL OR DATA OUTPUT
		7	AUXOUT 1
7	REX SWITCH	8	AUXOUT 2
8	GROUND		
9	DOOR SWITCH	9	REX SWITCH
10	GROUND	10	GROUND
11	AUX IN 1	11	DOOR SWITCH
12	GROUND	12	AUX IN 1
13	AUX IN 2	13	GROUND
14	GROUND	14	AUX IN 2
15	(+) 5 VDC OUTPUT	15	RX- *
16	DATA/D0	16	RX+ *
17	CLOCK/D1	17	TX- *
18	GROUND	18	TX+ *
19	LOCK OR CLOCK OUTPUT		
20	GROUND	1	12-24 VDC (+) OR VAC
21	BELL OR DATA OUTPUT	2	12-24 VDC (-) OR VAC
22	GROUND		
23	AUXOUT 1		
24	GROUND		
25	AUXOUT 2		
26	GROUND		

Figure 18-1: Terminal Block Labeling

Terminal Block Layout



Any of the grounds coming off of pins 8, 10, 12, 14, 18, 20, 22, 24, and 26 of the "Old Board" can be tied to pin 4, 10, or 13 on the new board. If there are multiple grounds create a pig tail so that there is only 1 wire going into the terminal block

Figure 18-2: Terminal Block Layout

Memory Reset

1. To reset the memory of the HandReader follow these steps-
2. Remove power and battery jumper, if a back up battery is installed
3. Press down on reset button and apply power
4. Release button
5. Reader will boot to
   - Press 1 to erase setup i.e. address, outputs, passwords, but retain user database and datalogs
   - Press 9 to erase everything i.e. HandReader goes back to factory defaults

Appendix C: Old Board Configuration Information

Wall Plate Installation

Attaching the HandReader

1. Loosen the three bottom mounting screws until there is approximately 1/8 inch (3 mm) clearance between the screw head and the wall plate.
2. Remove the HandReader from its carton.
3. At the base of the HandReader is a piano hinge with three keyhole shaped slots that correspond with the three lower mounting screws. Align and hang the HandReader from the three lower mounting screws (see Figure 17-1).

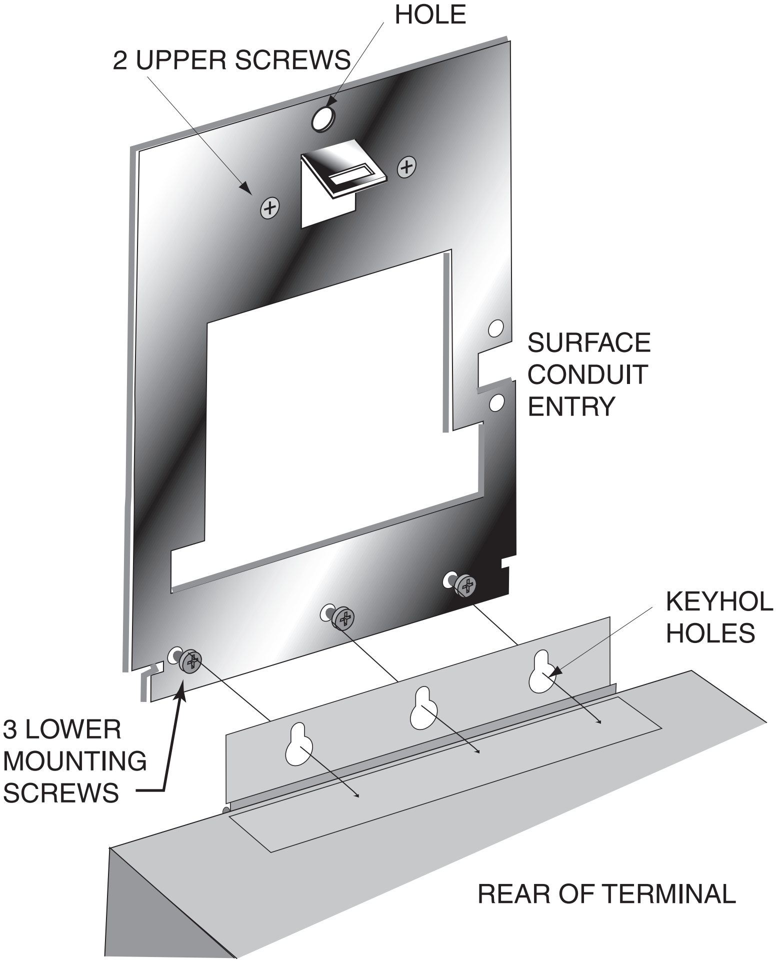


Figure 19-4: Attaching the Hand Reader to the Wall Plate

5. Tighten all three lower mounting screws.
6. The Hand Reader is now ready for its wiring connections.

Wiring Connections

Once the Hand Reader is attached to the wall plate the wiring connections to the Hand Reader can be made (see Figure 17-2).

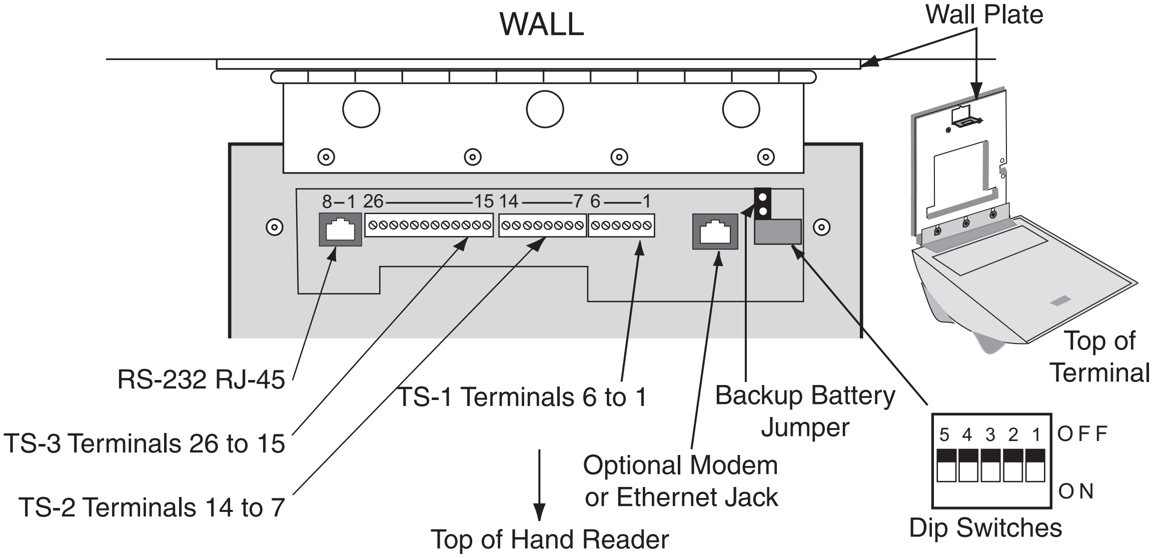


Figure 19-7: Wiring Connections and Dip Switches

Grounding

! NOTE *Terminal 1 and the center pin of jack J12 are connected together. Terminal 2 and the sleeve of jack J12 are connected together.*

! NOTE *Use any one of the following ground terminals to make the earth ground connection: 8, 10, 12, 14, 18, 20, 22, 24, or 26. Do NOT use terminal 2 to establish the earth ground connection; terminal 2 is not directly connected to ground.*

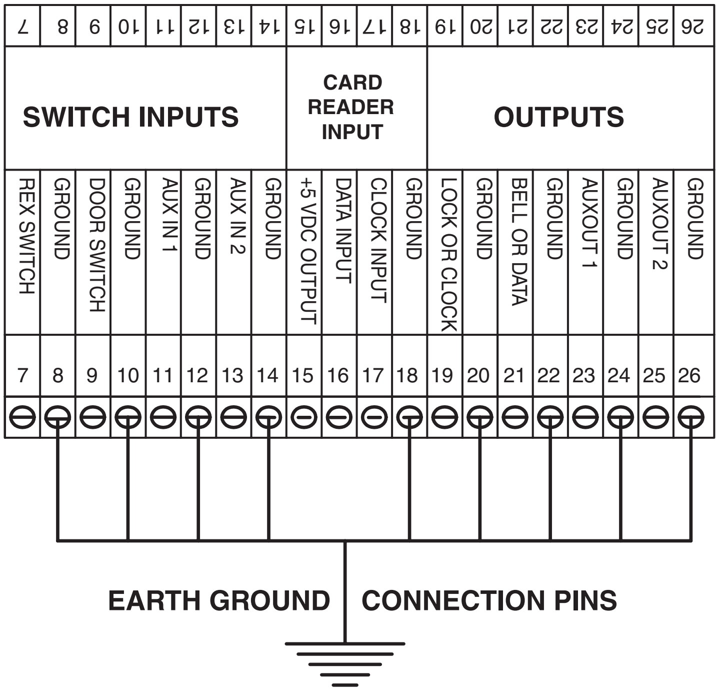


Figure 19-8: Earth Ground Connection Terminals

There are two standard methods for providing earth grounding to HandPunch units:

- earth grounding all units (see page 10)
- carrying an earth ground to each unit (see page 11)

Earth ground all units when there is a good earth ground source near each unit and/or when there are very long cable runs between units.

Carry an earth ground to each unit when there are no earth grounds convenient to the unit and the unit's power supply is floating.

Wiring Examples

The following Tables provide the pin outs for the terminal strips on the Hand Reader.

- Table 17-1 on page 68 provides the pin outs for TS-1: Power and Communication Connections.
- Table 17-2 on page 68 provides the pin outs for TS-2: Input Connections.
- Table 17-3 on page 68 provides the pin outs for TS-3: Card Reader and Output Connections.
- Table 17-4 on page 68 provides the pin outs for the RJ-45 Serial RS-232 Connection.

The following Figures provide typical Hand Reader wiring diagrams.

- Figure 17-3 on page 67 provides connection points for ground
- Figure 17-4 on page 69 provides a typical Lock Output wiring diagram.
- Figure 17-5 on page 70 provides a typical Auxiliary Output wiring diagram.
- Figure 17-6 on page 71 provides a typical Card Reader Emulation Mode wiring diagram.
- Figure 17-7 on page 72 provides a typical RS-422 Master/Remote Network System wiring diagram.
- Figure 17-8 on page 73 provides a typical RS-485 2-Wire Master/Remote Network System wiring diagram.
- Figure 17-9 on page 74 provides a typical Host PC Network System wiring diagram.
- Figure 17-10 on page 75 provides a typical Printer to Hand Reader wiring diagram.

Table 19-13: TS-1 - Power and Communication Connections

Terminal	Connection
1	Power Input 12 to 24 VDC/VAC
2	Power Return
3	RS-422 Rx- or RS-485 Rx-/Tx-
4	RS-422 Tx- or RS-485 Rx+/Tx+
5	RS-422 Rx+
6	RS-422 Tx+

Table 19-14: TS-2 - Input Connections

Terminal	Connection
7	Request to Exit Input
8	Ground
9	Door Monitor Switch Input (NC Standby)
10	Ground
11	Auxiliary Input 1
12	Ground
13	Auxiliary Input 2
14	Ground

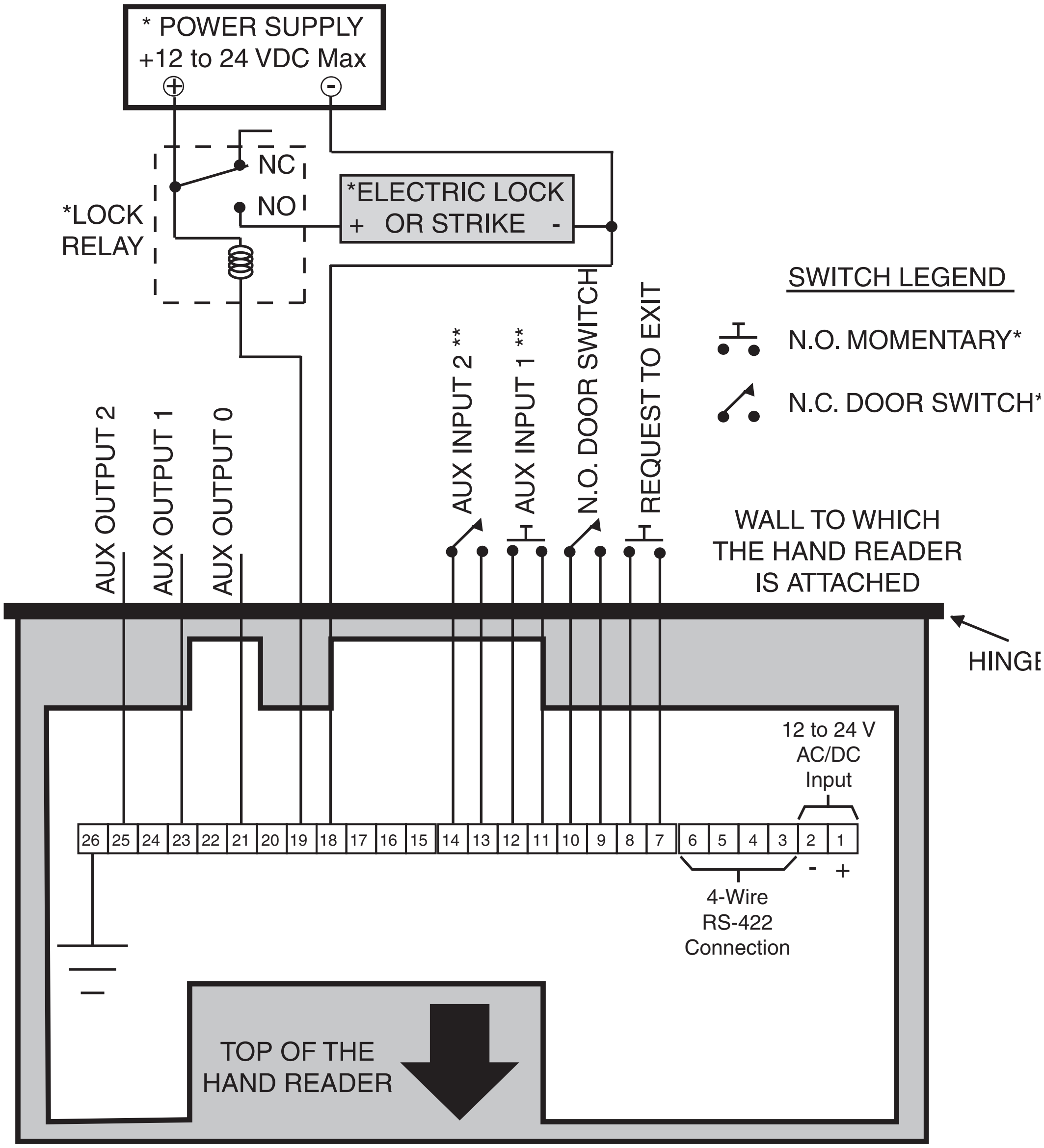
Table 19-15: TS-3 - Card Reader and Output Connections

Terminal	Connection
15	+5 VDC @ 400 mA Max. Output for External Card Reader
16	Card Reader: Wiegand D0 or Magnetic Stripe Data Input
17	Card Reader: Wiegand D1 or Magnetic Stripe Clock Input
18	Card Reader Ground
19	Lock Output or Wiegand D1 or Magnetic Stripe Clock Output
20	Ground
21	Auxiliary Output 0 or Wiegand Data 0 or Magnetic Stripe Data Output
22	Ground
23	Auxiliary Output 1
24	Ground
25	Auxiliary Output 2
26	Ground

Table 19-16: RJ-45 Serial RS-232 Connection

Pin	Signal	Connection
1	RI	* Ring Indicator Input (from external device)
2	CD	* Carrier Detect Input (from external device)
3	DTR	* Data Terminal Ready Output (to external device)
4	GND	Ground
5	Rx Data	Receive Data Input (from external device)
6	Tx Data	Transmit Data Output (to external device)
7	CTS	* Clear to Send Input (from external device)
8	RTS	* Ready to Send Output (to external device)

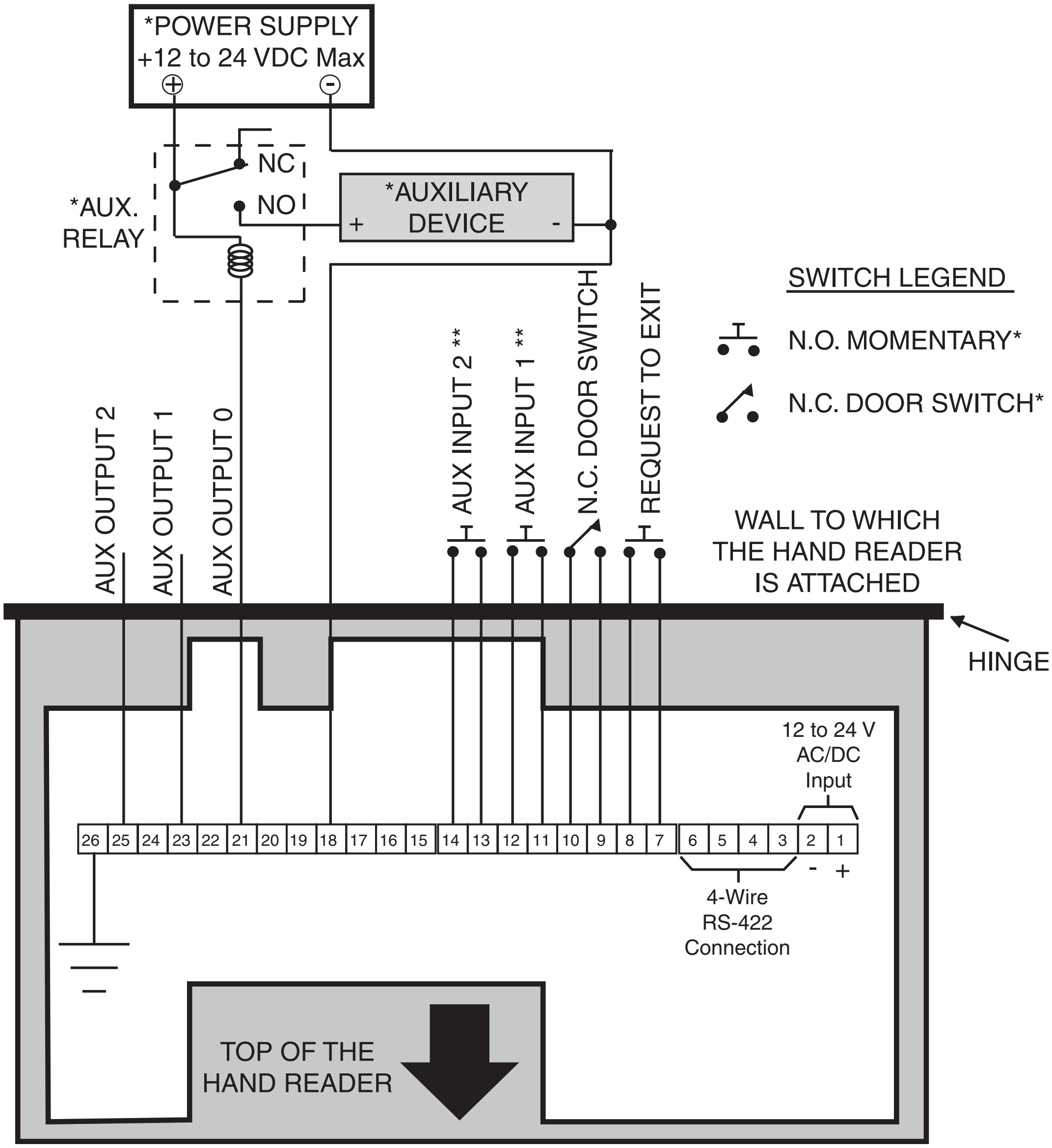
* These signals are not currently supported.



* These components are not supplied by Schlage Biometrics, Inc.

** The operation of the Auxiliary Inputs depend upon how the inputs have been configured

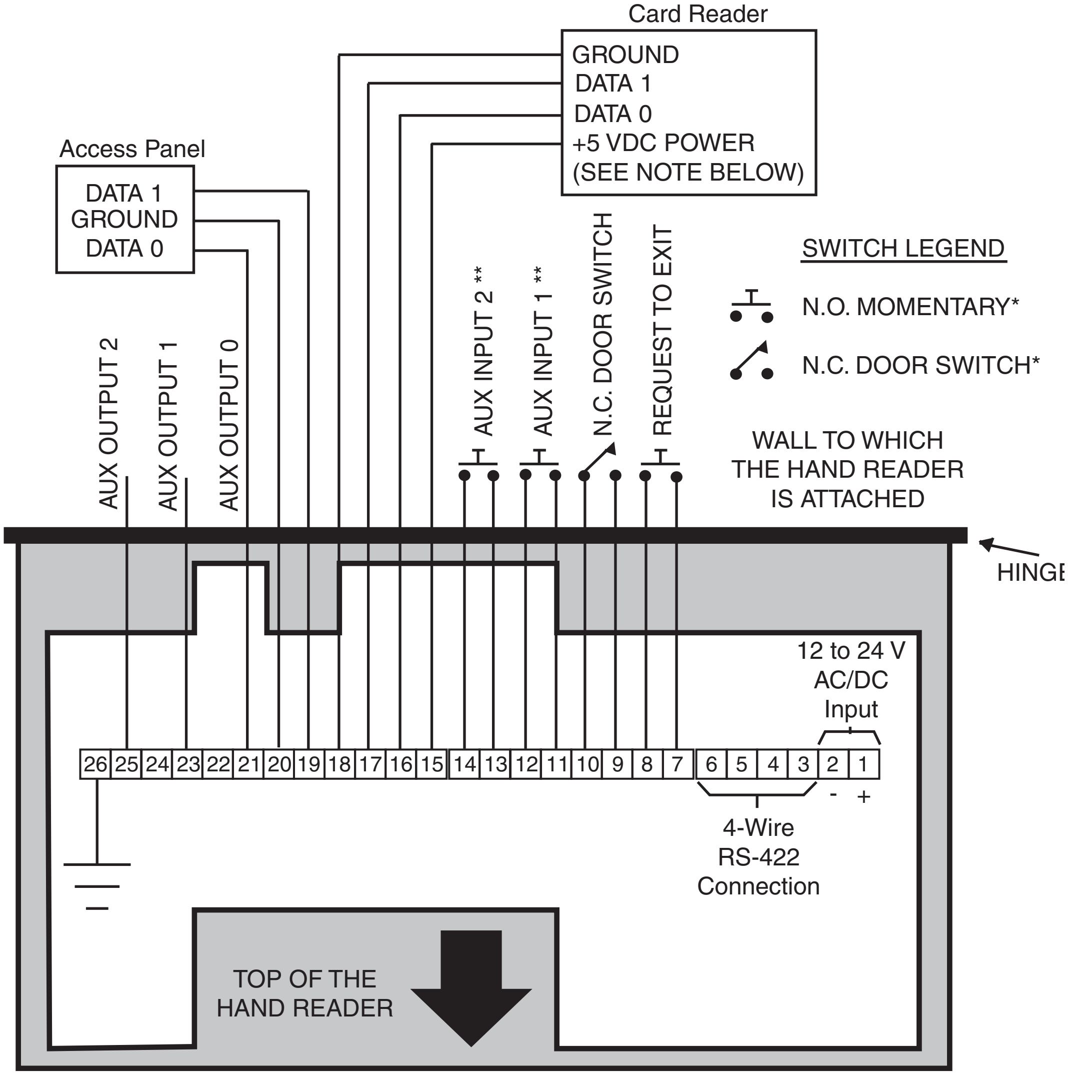
Figure 19-9: Lock Output Wiring Diagram



* These components are not supplied by Schlage Biometrics, Inc.

** The operation of the Auxiliary Inputs depends upon how the inputs have been configured

Figure 19-10: Auxiliary Output Wiring Diagram



* These components are not supplied by Schlage Biometrics, Inc.

** The operation of the Auxiliary Inputs depends upon how the inputs have been configured.

NOTE: For +12 VDC readers, connect power supply +12 VDC to card reader.

Figure 19-11: Card Reader Emulation Mode Wiring Diagram

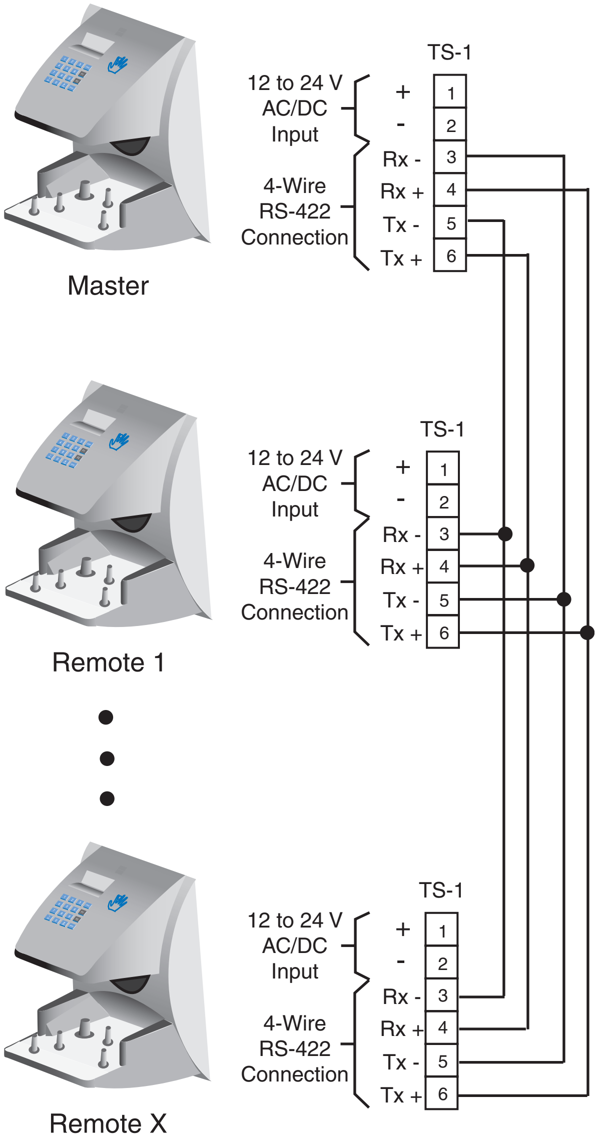


Figure 19-12: RS-422 4-Wire Master/Remote Network System Wiring Diagram

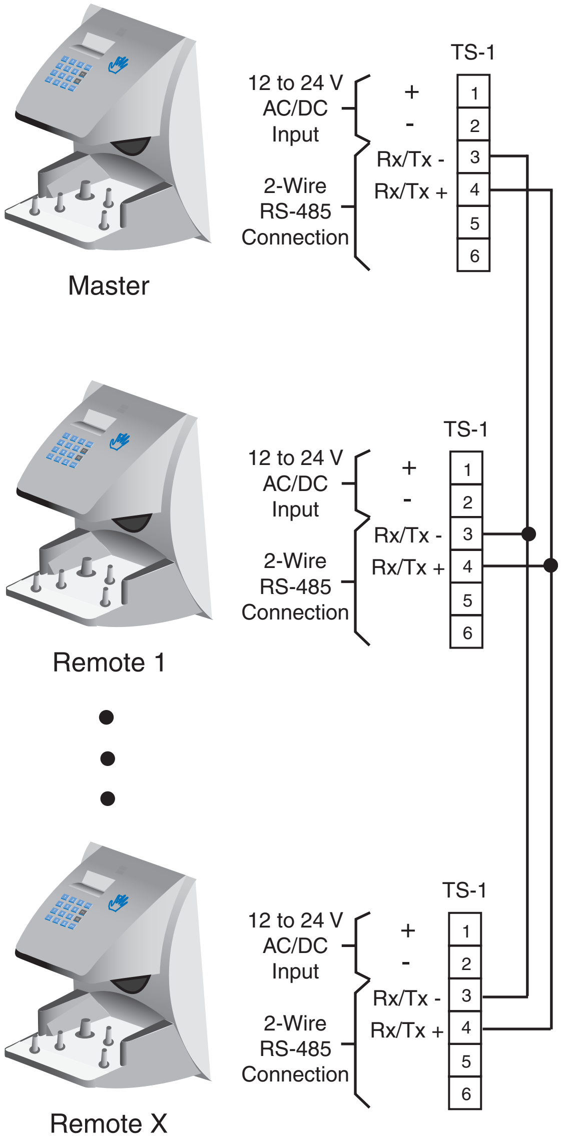


Figure 19-13: RS-485 2-Wire Master/Remote Network System Wiring Diagram

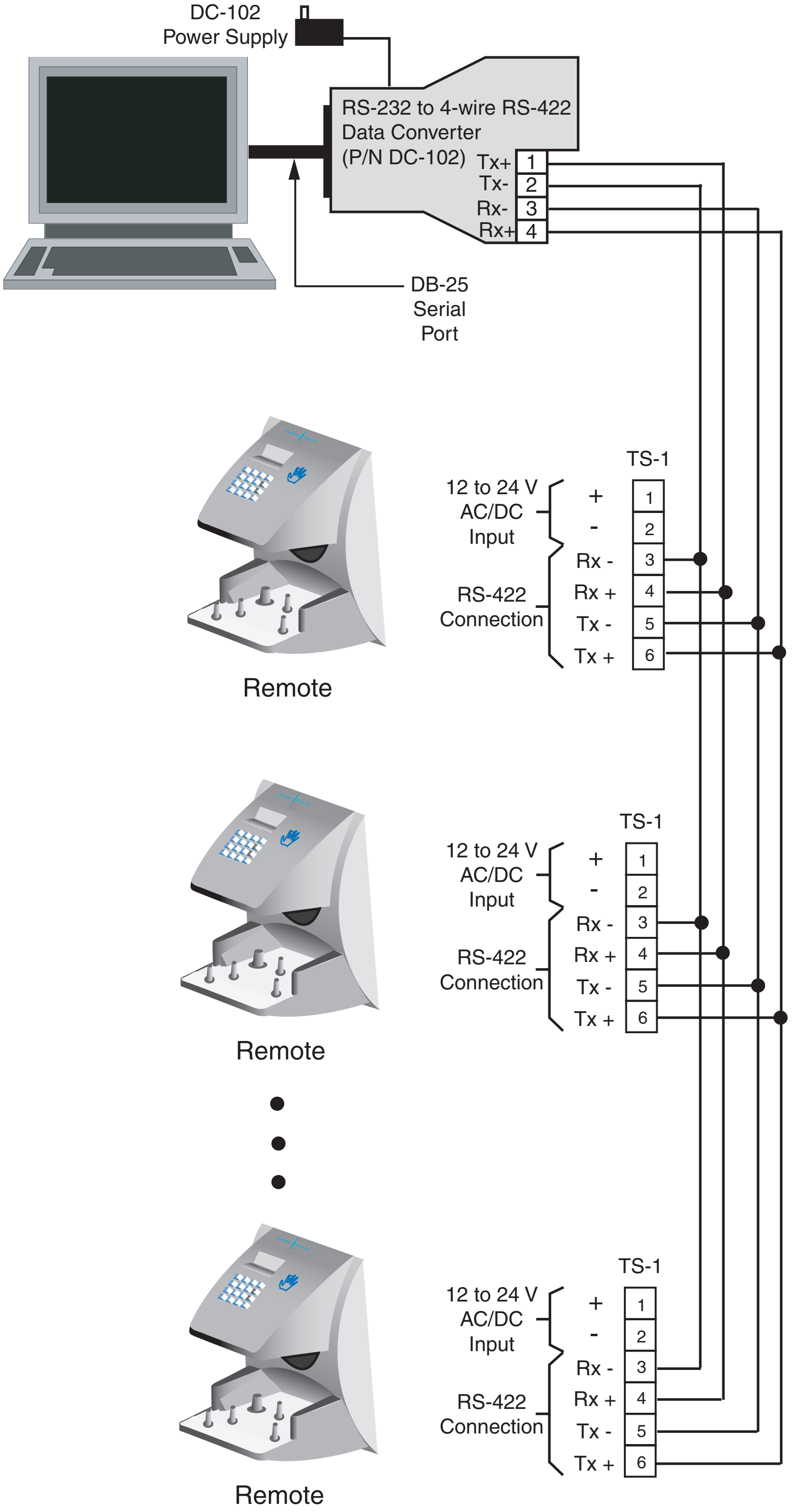
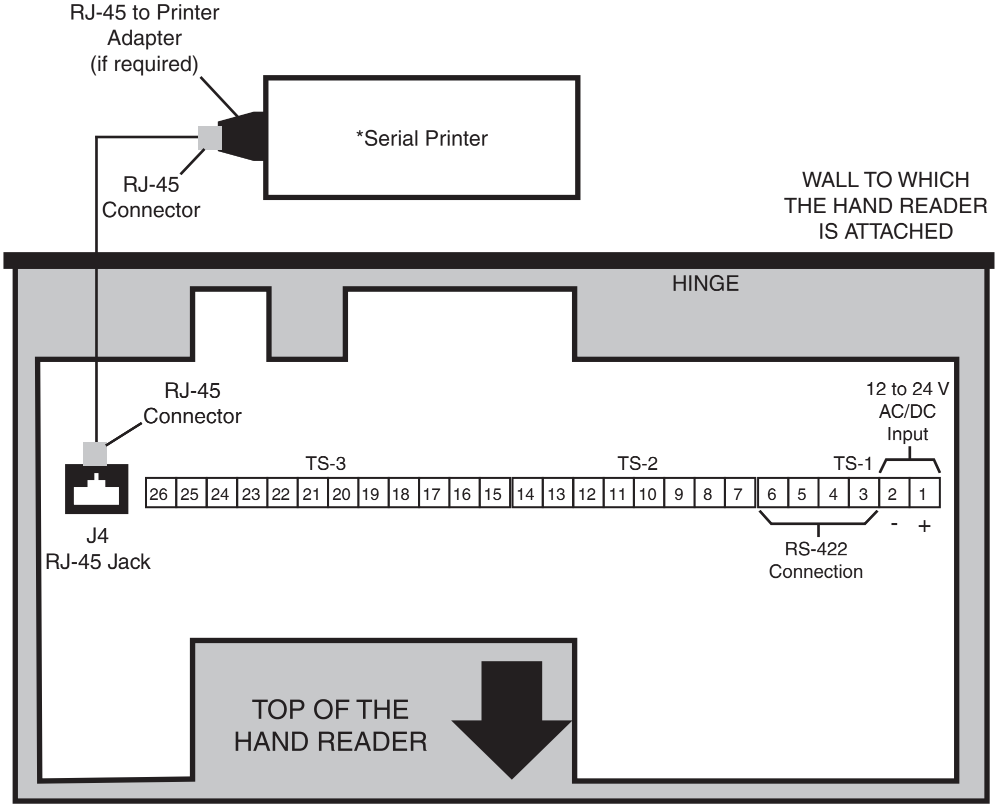


Figure 19-14: Host PC Network System Wiring Diagram



* These components are not supplied by Schlage Biometrics, Inc.

Figure 19-15: Printer to HandKey II Wiring Diagram

Setting the DIP Switches

DIP Switch settings perform three tasks for the Hand Reader (see Figure 17-11).

Set End of Line (EOL) Termination to match the type of termination the network being used needs.

- Set the Communication Method to match the type of network used.
- Erase Memory to clear Hand Reader memory to all factory default values and also clear all user memory.

Refer to Figure 17-2 on page 66 for the location of all DIP switches described in this section.

! NOTE *If a Hand Reader is used as a stand-alone Hand Reader, the End of Line (EOL) Termination and Communication Method dip switches are not used and should be left in their default positions.*

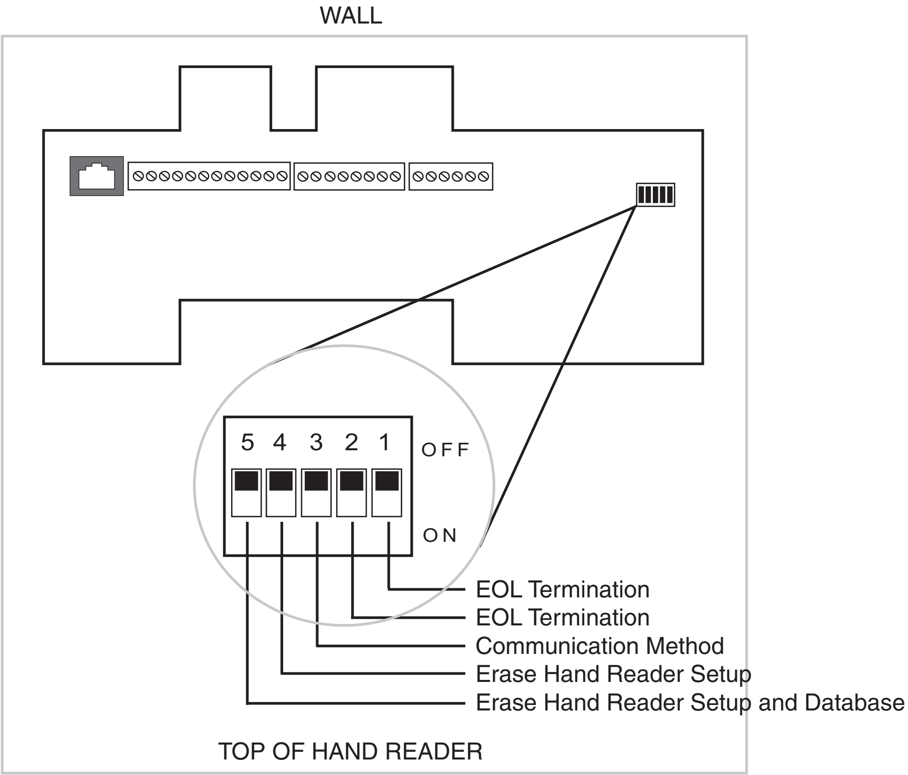


Figure 19-16: Hand Reader Dip Switches

End of Line Termination

The factory default setting is for EOL termination to be disabled – switches 1 and 2 OFF. Refer to Figure 17-11 for switch ON/OFF positioning.

- To enable EOL termination at a Hand Reader, both switches 1 and 2 must be ON.
- To disable EOL termination at a Hand Reader, both switches 1 and 2 must be OFF.
- In a Master/Remote Hand Reader network, the Master reader and the last Remote reader in the daisy-chain must have EOL termination turned ON. All other readers in the network must have EOL termination turned OFF.
- In a Hand Reader/host PC network, a modem/host PC network, the last Remote reader in the daisy-chain must have EOL termination turned ON.
- In an Ethernet / host PC network the EOLs must be turned OFF.

Communication Method

Communication can be done via an RS-232 direct connection, a 4-wire RS-422 network configuration. The factory default setting is for network communication via 4-wire RS-422 cabling – switch 3 OFF. Refer to Figure 17-11 for switch ON/OFF positioning.

- For network communication via RS-422 cabling, switch 3 must be OFF.
- For network communication via 2-wire RS-485 cabling, switch 3 must be ON.
- For network communication via RS-232, the switch 3 position does not apply. Leave switch 3 in the default OFF position.

! NOTE *All Hand Readers in a network must be set to the same communication method. Four-wire RS-422 cabling is required for HandNet for Windows™ network installations. Schlage Biometrics does not recommend two-wire RS-485 cabling for new network installations.*

Erasing HandReader Memory

The erase memory function allows a Hand Reader's setup and/or user database to be erased. The factory default setting (and normal operation setting) is for switches 4 and 5 to be OFF, retaining memory.

Erasing the HandReader Setup

Perform the following steps to erase the setup programs but retain the user database.

1. With system power OFF, set switch 4 ON.
2. Turn system power ON and wait 5 seconds.
3. Turn switch 4 OFF.

Erasing the HandReader Setup and User Database

Perform the following steps to erase both the setup programs and the user database.

1. With system power OFF, set both switches 4 and 5 ON.
2. Turn system power ON and wait 5 seconds.
3. Turn both switches 4 and 5 OFF.

! NOTE *Before putting the hand reader into service ensure DIP switches 4 and 5 are both OFF. If switches 4 and 5 are not off, the next time the Hand Reader's power is cycled the Hand Reader's memory will be erased.*

Closing the HandReader

Before closing the Hand Reader, ensure dip switches 4 and 5 are OFF (refer to Figure 17-11). With the wall mount latch in the unlocked position, swing the body of the Hand Reader up and lock the latch into place with the key provided with the Hand Reader (see Figure 17-12).

! NOTE *Do not force the Hand Reader onto the wall mount latch when the latch is in the locked position.*

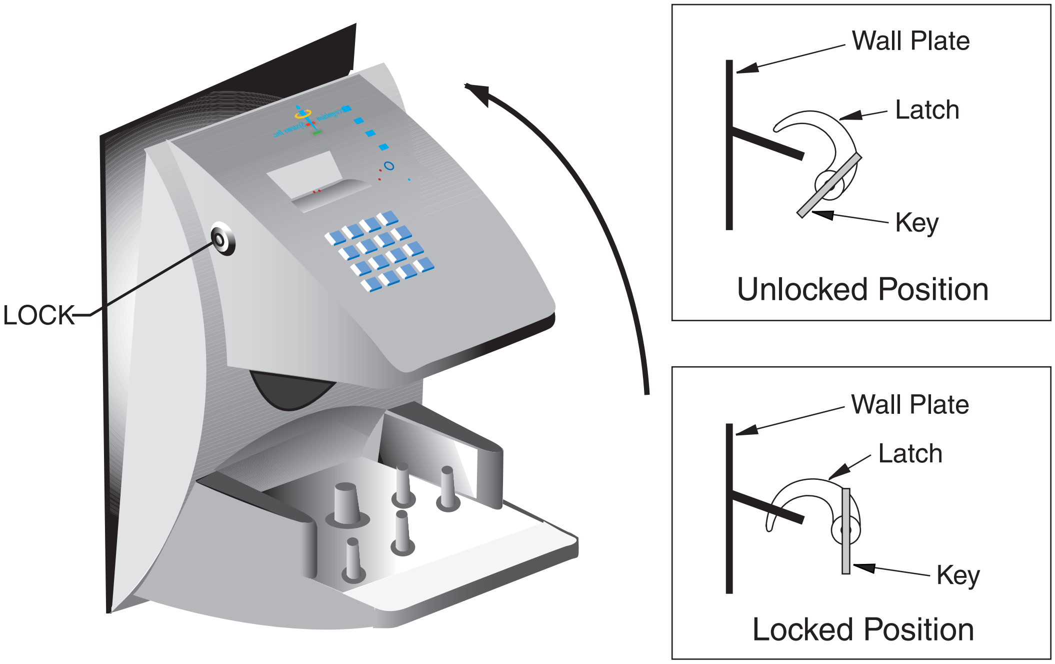


Figure 19-4: Closing the Hand Reader

Appendix D: Troubleshooting Guide

Display Messages During Verification

Various messages can appear on the HandPunch's display during hand verification. These messages are defined in.

Table 20-17: Display Messages During Verification

Message	Definition
PLACE HAND	The platen is ready to receive your hand for verification.
ID VERIFIED	You are verified, proceed.
REMOVE HAND	Remove your hand and place it on the platen again. Follow proper hand placement rules.
TRY AGAIN	Your attempt was rejected. Repeat verification following proper hand placement rules.
ID REFUSED	Your rejections exceeded the maximum number of tries allowed. Wait until another employee has verified and try again or call your supervisor.
ENTER ID	You entered your ID number incorrectly or your access time is restricted.

- If the display shows TRY AGAIN, you are not verified. You may have made an error in entering your ID number or in placing your hand on the platen. Re-enter your ID number and try again, taking care to follow proper hand placement rules (see page 50).
- If the display shows TIME RESTRICTION, you are not authorized to punch in at this time. If this seems to be in error, contact your supervisor about time restrictions.
- After a pre-programmed number of denied attempts, an ID number will no longer be accepted and the display will appear as follows.
- This is called a "lockout." Before the rejected ID number can be used again, another employee or a supervisor must successfully verify at the HandPunch.
- If you enter your ID number, but do not place your hand on the platen, the HandPunch will time-out in about 25 seconds. You can immediately end this time-out by pressing the key.

Beeper and LED Status During Verification

The HandPunch's beeper and LED status display also display hand verification information. This information is defined in.

Table 20-18: Beeper and LED Status During Verification

Operation	Beeps	LED	Meaning
During Keypad Entry	1 per Keystroke	–	Keystroke Accepted
After ID Entry	–	–	OK - Proceed
After ID Entry	2	–	ID Number Not in Database
After Hand Placement	1	Green	ID Verified
After Hand Placement	2	Red	ID Not Verified - Try Again
After Hand Placement	1 Long		
Continuous	Red	ID Refused	

Glossary

Address, IP – An Internet Protocol address is a unique address assigned to a computer for communicating over the Internet. It is made up of 4 sets of numbers, separated by periods (for example, 123.245.78.901).

Address, Reader – A Hand Reader Address is a unique identification number assigned to a Hand Reader. Each Hand Reader on a network must be assigned a unique address.

AWG – American Wire Gauge is a U.S. standard set of wire conductor sizes. The "gauge" refers to the diameter of the wire. The higher the gauge number, the smaller the diameter, the thinner the wire, and the greater the electrical resistance. Thicker, smaller gauge wire carries more current because it has less electrical resistance over a given length. Thicker wire is better for long wire distances.

Card Reader Emulation Mode – In Card Reader Emulation Mode, the Hand Reader outputs hand read data in a card reader format, typically to an access control panel. The data is outputted when user's hand is successfully read. This mode is commonly used when a Hand Reader is being added to an existing access control network. By configuring the Hand Reader in card emulation mode, it can easily replace an existing access control reader in the network. The Hand Reader can be configured to output data in a variety of card reader formats – such as Wiegand, ABA Track-II magnetic stripe, or bar code.

Daisy-Chain – A Daisy-Chain is a method of wiring together Hand Readers on a network, where the first Hand Reader is connected to the second Hand Reader, which is connected to the third Hand Reader, and so on until the last Hand Reader is reached.

End-of-Line (EOL) Termination – EOL Termination is a set of resistors attached to the data lines at the last Hand Reader physically connected to a network. These resistors prevent data signal distortion and reflection back across the data lines, improving the integrity of the network connection.

IP Address – see Address, IP

Platen – The Platen is the flat surface at the base of the HandKey, on which a user places his/her hand for enrollment and verification. The platen has guide pins to ensure the user's fingers are consistently positioned correctly.

Reader Address – see Address, Reader

Template – A Template is a set of data generated for a user. It is made up of the user's enrollment information and any system configuration parameters that are assigned to the user. The template is stored at each Hand Reader and can be stored at a host computer when the HandNet™ for Windows™ software is used.

Time Zone – A Time Zone is an identified period of time, during which a user is allowed access to an area secured by a Hand Reader. Access attempts outside of that time period are rejected by the Hand Reader.

Transaction – A Transaction is any kind of event recorded at a Hand Reader. Transactions may include actions such as accepted or denied hand reads, input and output events, and doors opening and closing.

Wiegand™ Reader – The term “Wiegand Reader” has two meanings depending upon its application. A true Wiegand reader reads a specially constructed card made up of small pieces of magnetic wire. As the card is swiped through the reader, the individual bits of wire generate a unique data signal. This data signal is made up of a Facility Code field (typically 8 bits), an ID Number field (typically 16 bits), and parity bits (typically 2 bits) for a total of 26 bits of data. Now this 26-bit Wiegand data format has been adopted by a variety of access reader devices and access control panels for transferring user access data.

Limited Warranty

Schlage Biometrics, Inc. (the “Company”) warrants to the original user the products manufactured by the Company (the “Product”) to be free of defects in material and workmanship for a period of one year from the date of purchase by such user or 15 months from the date of shipment from the factory, whichever is sooner, provided:

The Company has been notified within such period by return of any alleged defective product, free and clear of all liens and encumbrances, to the Company or its authorized dealer, transportation prepaid; and

The Product has not been abused, misused, or improperly maintained and/or repaired during such period; and

Such defect has not been caused by ordinary wear and tear; and

Such defect is not the result of voltage surges/brownouts, lightning, water damage/ flooding, fire, explosion, earthquakes, tornadoes, acts of aggression/war, or similar phenomenon; and

Accessories used as integral to the Product have been approved by the Company.

The Company shall, at its option, either repair or replace, free of charge, the Product found, upon the Company’s inspection, to be so defective, or if agreed upon, refund the purchase price, less a reasonable allowance for depreciation, in exchange for the Product.

THE COMPANY MAKES NO OTHER WARRANTY AND ALL IMPLIED WARRANTIES INCLUDING ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE ARE LIMITED TO THE DURATION OF THE EXPRESSED WARRANTY PERIOD AS SET FORTH ABOVE.

THE COMPANY’S MAXIMUM LIABILITY THEREUNDER IS LIMITED TO THE PURCHASE PRICE OF THE PRODUCT. IN NO EVENT SHALL THE COMPANY BE LIABLE FOR ANY CONSEQUENTIAL, INDIRECT, INCIDENTAL, OR SPECIAL DAMAGES OF ANY NATURE ARISING FROM THE SAME OR THE USE OF THE PRODUCT.

Schlage Biometrics Inc. reserves the right to make changes in the design of any of its products without incurring any obligation to make the same change on units previously purchased.

Ingersoll Rand
Security Technologies

Ingersoll Rand's Security Technologies Sector is a leading global provider of products and services that make environments safe, secure, and productive. The Sector's market-leading products include electronic and biometric access control systems; time and attendance and personnel scheduling systems; mechanical locks and portable security, door closures and exit devices, steel doors and frames, architectural hardware and technologies and services for global security markets.

866.861.2480

www.schlage.com www.ingersollrand.com

Schlage
Biometric Solutions
Ingersoll Rand Security Technologies
538 Oakmead Parkway
Sunnyvale, CA 94085
Office: 866-861-2480/512-712-1413 (international)
Fax: 866-303-1794/408-341-4101
E-mail: sbssupport@irco.com

HandNet for Windows

Terminal User's Guide

Ingersoll Rand
Security Technologies

Table of Contents

Getting Started

Introduction

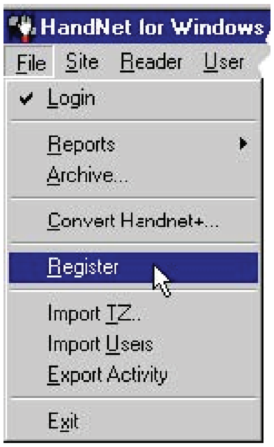
What HandNet Does

HandNet for Windows lets you control and monitor many connected HandKey readers. In this one program, you can control who can use each reader and when. You can also monitor activity and alarms for all readers at once.

Registering HandNet

After the first time you use this Version of HandNet, you have fourteen days to register it. You must register it even if you registered your previous Version of HandNet. If you do not register it within fourteen days, you will not be able to log into the program. The process should only take a minute.

1. If you have not logged into HandNet yet, log in; see page 4.
2. If the registration screen is not shown, pick *Register* from the *File* menu, and click the *Print the registration form* button on that screen.
3. Fill the form out and fax it to the number at the top of the form. Once we receive your completed form, we will fax an activation code back to you within two business days (since it could take two days for us to send your code back, please print and send the registration form now; do not wait until day fourteen).
4. Pick *Register* from the *File* menu, enter the activation code we sent, and click the *Activate* button. Once you do this, HandNet is permanently functional.



New Features in Version 2.0

HandNet for Windows Version 2.0 provides a number of new features, but these are only available to you if you purchased the upgrade to the full feature set. If you did not purchase this upgrade and you would like to, please contact your dealer; once you pay for the upgrade, we will send you a new access code to enter on the *Registration* screen. Once you enter this code, all the new features are immediately available to you.

How to tell if I have access to the new features

1. From the main menu bar, click the *Help* menu, and then click *About HandNet for Windows*.
2. Check the bottom of the box that pops up. To be able to use the new features, the last line must say *You may use all features of this software*. If this line says *Your current license does not let you use the enroll*..., you must contact your dealer and upgrade your license before you can use the new features (once you upgrade, we willsend you an access code that makes these feature available).

The new features

Enrolling Users from HandNet: Previously, to enroll a user you had to go to a features reader, enter command mode on the reader, and enroll the user. Now, if you have a reader that is near the computer, you can add the user in HandNet, select the reader to enroll at, and pick *Enroll* from the *Reader* menu without ever having to deal with command mode on the reader; see page 87.

User Access for a Limited Time Period: HandNet now lets you specify that a user's access should start and stop at certain days or times. For example, if a contractor needs access to your facility, you can now set the access to expire on the day that the contract ends. This gives you more complete control of who can access readers and when; see page 93.

Import/Export Users: If you have more than one computer system running HandNet and you want users added on one system to be available to the others, HandNet now lets you export user information from one program and import it into another; see page 99.

Exporting Activity for External Report Generation: If you want to create custom activity reports using some external report tool, *Export Activity* on the *File* menu sends all of your current activity to an access database file called expactvt.mdb; see page 116. While the main HandNet database files are password protected for security reasons, this file is not so you can open it and access any information in it at will. You can also set HandNet up to automatically export activity whenever you archive activity.

* * * * *

Getting Help in HandNet

The online help has the same information that is in this manual. To get help in HandNet, press F1. This brings up help for the screen you are on. From there, you can use the contents, index, or search tabs at the left of the help window to find any topic.

For Basic Topics

Click the *Contents* tab at the top of the left pane, click a book to open and click a topic. Not every topic is in the *Contents* tab, so if you do not find what you need, try the *Index* or *Search* tabs.

For Groups of Topics on a Single Theme

In addition to the contents you can also click on the pull-down list right under the *Previous/Next* buttons (in the bottom middle of the header). This list contains a number of important groups of topics. Once you are on one of these topics, the *Next* and *Previous* buttons work as well.

Screens and Menus

On menus and screens in this help, click any option on the screen to jump to help on that item.

When to Use the Index and When to Search

Use the index for main themes like adding a reader or enrolling a user. Use the search for minor points. For example, if you type *enroll* on the *Index* tab, you get three main topics that deal with enrolling users. On the *Search* tab, *enroll* gets you nearly thirty topics where *enroll* appears somewhere in the text. For main topics, the index gets you to what you want more directly. On the other hand, if you remembered that a screen somewhere said something about the number of tries a user gets before having access denied, the *Search* tab would check the entire text and find this detail for you. Use the *Index* tab to find items that are likely to be a main topic; use the search tab to find minor points.

Marking a Topic to Return to

To mark a topic in the help that you want to come back to:

1. Go to the topic that you want to mark.
2. Click the *Favorites* tab at the top of the left pane.
3. Click the *Add* button at the bottom of the pane. This adds the topic to your favorites list.

To get back to any marked topic later:

1. Click the *Favorites* tab at the top of the left pane of the help window.
2. Double-click the topic.

Getting In and Getting Out

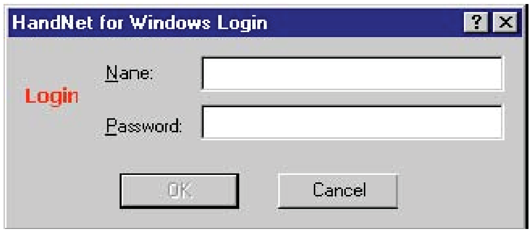
Starting HandNet

To start HandNet, either click the HandNet icon on your Windows desktop, or click the *Start* menu on your Windows taskbar, highlight *Programs*, and highlight and click *HandNet for Windows*.

Logging into HandNet

HandNet requires you to log in before you can make any changes; this prevents unauthorized people from changing information. If you are not logged in, you can look at the lists of activity, users, and readers (network), but you cannot change any information and cannot use any other options.

1. Click *Login* on the *Toolbar,* or pick *Login* from the *File* menu. The program brings up this box:



2. Type your name and password, and click *OK*.

If this is a new system: Use a name of *1234* and a password of *new* (change this name and password immediately so unauthorized people cannot user the program).

After initial setup: If you forget your name or password, see your supervisor or security administrator.

Passwords are NOT case sensitive. For example, if your password is *narnia*, then *Narnia* and *NARNIA* would also work.

After you are done using HandNet, be sure to log out again so unauthorized operators will not be able to use the program.

Changing the Initial Login Name and Password

HandNet comes set up with a login name of *1234* with a password of *NEW*. This lets you get into HandNet when you first start using it, but this is not secure; anyone may read this manual and find this name and password. To keep unauthorized users from using HandNet, change this password before you add any other information.

1. Click the *View* menu.
2. Click *Settings*.
3. Click the *Operators* tab.
4. Click the operator named *1234* and then click *Edit*. This takes you to the *Operator Definition* screen, which has settings for this user.
5. Change the *Name* to your name, and change the *Password* to something you will remember but that no one else will be able to guess. Click *OK* to return to the list of operators.

Remember the name and password you enter; if you forget it, you will not be able to get into HandNet. Do not change any other settings; this user is set up to use any option in HandNet; if you uncheck any boxes, you will not be able to use the corresponding options.

6. Click the *Close* button at the bottom of the box to close *System Settings*.

Logging out of HandNet

Log out of HandNet when you are done using it. This prevents unauthorized people from changing information. Someone who is not logged in can look at the lists of activity (including alarms), users, and readers, but cannot change any information or use any other options.

To log out, click the *Logout* button on the *Toolbar* or pick *Login* again from the *File* menu to uncheck it.

Exiting HandNet

For security purposes, you should generally log out of HandNet when you are done making changes so unauthorized people cannot add users or make changes. However, unless you are going to install a new Version of the HandNet software, or you need to restart the computer HandNet is running on, you do not typically want to exit from the HandNet program. If you exit (that is, shut down the program), you disconnect it from all readers. While all readers will continue to record activity and give access as appropriate, the program will not receive any information from the readers or process any alarms during the time that HandNet is not running. Because of this, you would usually leave HandNet running all the time.

* * * * *

Getting Started Overview

Procedure for Getting Started and Setting Up

QUICK STEPS

Getting Started with HandNet for Windows

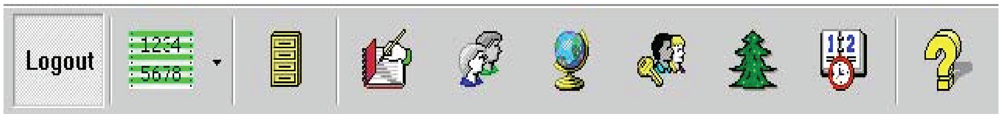
1. Log in; see page 4.
2. If you have not done so yet, register HandNet. HandNet will not let you log in after fourteen days if you do not register it; see page 1.
3. Change the initial password so unauthorized users will not be able to use the program; see page 4.
4. If you have been using readers without HandNet and you want to get the users from the reader(s):
    1. Pick *Settings* from the *View* menu.
    2. Click the *Security* tab.
    3. Check the box by *Do not delete unauthorized enrollments.*

    This prevents HandNet from deleting the users from the readers when you enable them (you will import the users from the reader later, after setting up the readers and sites). If you did not change this setting, when you enabled the site and reader, HandNet would regard all of the users in the reader as unauthorized (because they were not in HandNet yet), and it would delete them from the reader.
5. Set up site(s), that is, groups of connected readers; see page 33.
6. Set up readers; see page 42.
7. If you want to control which days and times users can access readers, set up time zones (see page 61) and holidays (see page 65).
8. If you have set up time zones and holidays, or if you want to give some users access through some readers but not others, set up access profiles; see page 67.
9. If you have previously been using one of our older MS-DOS products (HandNet Plus or HandNet), convert the users; see page 98 (if you have been using HandNet for Windows 1.09 or later, you do not need to convert anything; this Version of HandNet automatically updates information for the new Version).
10. If you have been previously using readers without one of the HandNet products and you need to get users from the reader(s), upload users from the reader(s); see *Getting User Information from a Reader* on page 99.
11. Add users; see page 74.
12. Enroll the users; see page 87.
13. When you are done using HandNet, be sure to log out so unauthorized people will not be able to add or change anything; see page 5.

Menus and Navigation

Toolbar

The toolbar looks like this:



If you are not logged in yet, the first button will be a login button and a number of the other will be disabled.

Turning the Toolbar On and Off

Toolbar on the *View* menu turns it on or off.

Options on the Toolbar

Login	You see this button if you are not logged in yet. Click this button to login to HandNet; see page 4. Without logging in, you cannot make any changes or do anything other than look at basic information.
Logout	Once you log in, the first button changes to the *Logout* button. If you are going away from the computer, logging out prevents making unauthorized changes. If anyone could possibly get access to the computer in your absence, logging out is an important security precaution.
1234 5678 ▾	The main button lets you generate a custom activity report; see *Creating a Custom Activity Report from the Reports* Menu on page 105. The small arrow to the right pulls down the *Reports* menu; see page 13.
🗄	This lets you archive older activity; see page 113.
📝	This opens the *Activity* window; see page 101. The *Activity* window lists all actions you take in HandNet, and actions or alarms from each reader. If the *Activity* window is already open and behind another window, this brings it to the front.
👤	This opens the *Users* window; see page 71. This lists everyone who is potentially able to access readers. If the *Users* window is already open and behind another window, this brings it to the front.
🌐	This opens the *Network* window; see page 31. The *Network* window lists all of your sites, readers, and their current status. If the network window is already open and behind another window, this brings it to the front.

🔑	This takes you to the access profile settings; see page 67. Access profiles let you control which readers different types of users have access to and when.
🌲	This takes you to the holidays settings; see page 65. If users have different access on holidays than on other days, the holidays settings identify when those days are.
1 2	This takes you to the settings that let you define different periods of time when users can have access; see page 61 (in HandNet, we call these time zones, but there is no connection to the time zones we usually think of that have to do with different times around the world).
?	This pops up the online help for HandNet. The help contains the same information as this manual but arranged in a slightly different format. To get help for the screen you are on, you can also press F1 anywhere in HandNet. The help has a complete index and also lets you search for specific text; see page 3.

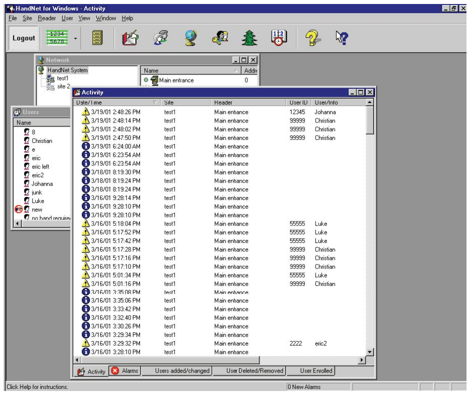
* * * * *

Tiling the Display Windows

HandNet lets you keep open the *Activity* window, the *Users* window, and the *Network* window (which shows sites and readers). If you have more than one window open, *Tile Horizontally* on the *Window* menu adjusts the open windows so they fill the Handnet window from side to side, and so they do not overlap and cover each other up.

Example of Windows that are NOT Tiled

Notice that the front windows cover up parts of the windows behind them and that the windows do not fill up the screen from side to side.



Name	Addr
Main entrance	0

HandNet System
test1
site 2

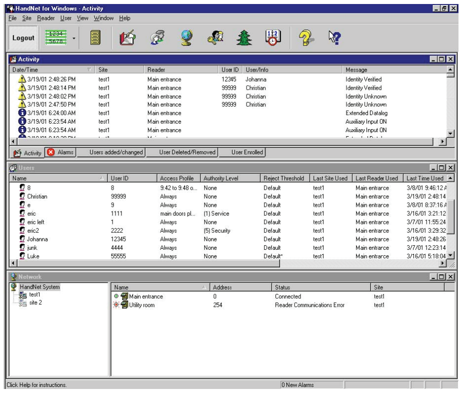
Name
8
Christian
e
eric
eric left
eric2
Johanna
junk
Luke
new
no hand require

Date/Time	Site	Reader	User ID	User/Info
3/19/01 2:48:26 PM	test1	Main entrance	12345	Johanna
3/19/01 2:48:14 PM	test1	Main entrance	99999	Christian
3/19/01 2:48:02 PM	test1	Main entrance	99999	Christian
3/19/01 2:47:50 PM	test1	Main entrance	99999	Christian
3/19/01 6:24:00 AM	test1	Main entrance		
3/19/01 6:23:54 AM	test1	Main entrance		
3/19/01 6:23:54 AM	test1	Main entrance		
3/18/01 8:19:30 PM	test1	Main entrance		
3/18/01 8:19:24 PM	test1	Main entrance		
3/18/01 8:19:24 PM	test1	Main entrance		
3/16/01 9:28:14 PM	test1	Main entrance		
3/16/01 9:28:10 PM	test1	Main entrance		
3/16/01 9:28:10 PM	test1	Main entrance		
3/16/01 5:18:04 PM	test1	Main entrance	55555	Luke
3/16/01 5:17:52 PM	test1	Main entrance	55555	Luke
3/16/01 5:17:42 PM	test1	Main entrance	55555	Luke
3/16/01 5:17:28 PM	test1	Main entrance	99999	Christian
3/16/01 5:17:16 PM	test1	Main entrance	99999	Christian
3/16/01 5:17:10 PM	test1	Main entrance	99999	Christian
3/16/01 5:01:34 PM	test1	Main entrance	55555	Luke
3/16/01 5:01:16 PM	test1	Main entrance	99999	Christian
3/16/01 3:35:08 PM	test1	Main entrance		
3/16/01 3:35:06 PM	test1	Main entrance		
3/16/01 3:33:42 PM	test1	Main entrance		
3/16/01 3:32:40 PM	test1	Main entrance		
3/16/01 3:30:26 PM	test1	Main entrance		
3/16/01 3:29:34 PM	test1	Main entrance		
3/16/01 3:29:32 PM	test1	Main entrance	2222	eric2
3/16/01 3:28:10 PM	test1	Main entrance		

Click Help for instructions.
0 New Alarms

Example of Windows that ARE Tiled

Notice that none of these windows cover any parts of the other, and that the windows now fill up the screen from side to side.



Date/Time	Site	Reader	User ID	User/Info	Message
3/19/01 2:48:26 PM	test1	Main entrance	12345	Johanna	Identity Verified
3/19/01 2:48:14 PM	test1	Main entrance	99999	Christian	Identity Verified
3/19/01 2:48:02 PM	test1	Main entrance	99999	Christian	Identity Unknown
3/19/01 2:47:50 PM	test1	Main entrance	99999	Christian	Identity Unknown
3/19/01 6:24:00 AM	test1	Main entrance			Extended Datalog
3/19/01 6:23:54 AM	test1	Main entrance			Auxiliary Input ON
3/19/01 6:23:54 AM	test1	Main entrance			Auxiliary Input ON

Name	User ID	Access Profile	Authority Level	Reject Threshold	Last Site Used	Last Reader Used	Last Time Used
8	8	9:42 to 9:48 o...	None	Default	test1	Main entrance	3/8/01 9:46:12 A
Christian	99999	Always	None	Default	test1	Main entrance	3/19/01 2:48:14
e	9	Always	None	Default	test1	Main entrance	3/8/01 8:37:16 A
eric	1111	main doors pl...	(1) Service	Default	test1	Main entrance	3/16/01 3:21:12
eric left	1	Always	None	Default	test1	Main entrance	3/7/01 11:55:24
eric2	2222	Always	(5) Security	Default	test1	Main entrance	3/16/01 3:29:32
Johanna	12345	Always	None	Default	test1	Main entrance	3/19/01 2:48:26
junk	4444	Always	None	Default	test1	Main entrance	3/7/01 12:23:14
Luke	55555	Always	None	Default*	test1	Main entrance	3/16/01 5:18:04

HandNet System
test1
site 2

Name	Address	Status	Site
Main entrance	0	Connected	test1
Utility room	254	Reader Communications Error	test1

Click Help for instructions.
0 New Alarms

* * * * *

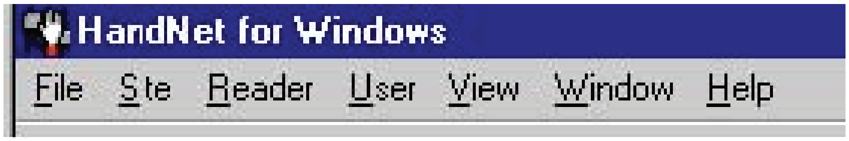
Menu Overviews

Pulling Down Menus with the Keyboard instead of the Mouse

If you prefer working from the keyboard rather than clicking with the mouse, you can hold the *ALT* key down and then type the underlined letter in the choice. For example, to open the *View* menu, you would hold *ALT* down and type *V* (this is often the first letter in the option, but not always).

Main Menu Bar

The main menu bar looks like this:



These menu options are briefly summarized below. The following pages contain more detail on the options on these menus.

File: The *File* menu lets you log in and out, generate reports, archive older activity, import setup information, and shut the program down; see page 11.

Site: The *Site* menu lets you add and change settings for sites (groups of connected readers); see page 14.

Reader: The *Reader* menu lets you add new readers, delete readers, and rename readers in the HandNet network. You can also unlock, relock, and lockup the selected reader, enroll a user at the selected reader, activate and deactivate an auxiliary device, and send (download) time, time zones, users, and setup configuration to selected readers; see page 15.

User: The *User* menu lets you add users, delete users, rename users, change information for a selected user, and create custom entries to collect additional information about users; see page 17.

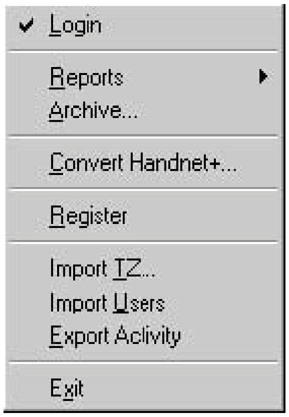
View: The *View* menu lets you open the *Users, Activity, and Network* windows (the *Activity* window lists both activity and alarms; the *Network* window lists all of your sites and readers). The *View* menu also lets you turn the toolbar on or off. And it lets you get to access profiles, holidays, activity filters, time zones, and system settings (you do not need these options on an ongoing basis; these are normally only used when setting the program up); see page 18.

Window: The *Window* menu lets you switch between open windows, tile open windows horizontally on the screen, or switch panes within the *Network* window; see page 20.

Help: The *Help* menu lets you pop up the help system you are looking at now (you can also press F1 to pop up *Help*); see page 21.

File Menu

The *File* menu lets you log in and out, generate reports, archive older activity, import setup information, and shut the program down.



Login: You must log in to HandNet before you can do anything other than look at information; see page 4. You must log in to acknowledge alarms, add sites and readers, add or change users. When you are done using the program, click this same option again to log out so unauthorized operators cannot use the program.

Reports: This brings up another menu that lists several standard reports, and that lets you create custom reports based on the activity that you see in the *Activity* window; see page 13.

Archive: This takes older information from the current activity file and stores it in a separate file. Once you archive information, the activity is no longer visible in the *Activity* window, but you can still generate reports based on the archives.

Convert Handnet+: If you have been using HandNet+ or HandNet (our older MS-DOS programs), and are just switching to HandNet for Windows, this converts user information from HandNet+ and adds it to the user list in HandNet for Windows. Information imported includes: user name, user ID number, authority level, and reject threshold; see page 98.

Register: After the first time you use this Version of HandNet, you have fourteen days to register it. You must register it even if you registered your previous Version of HandNet. If you do not register it within fourteen days, you will not be able to log into the program. The process should only take a minute. To register HandNet:

1. If the registration screen is not shown, pick *Register* from the *File* menu, and print the registration form.

2. Fill the form out and fax it to the number at the top of the form. Once we receive your completed form, we will fax an activation code back to you within two business days (since this could take two days for us to send your code back, please print and send the registration form now; do not wait until day fourteen).

3. Pick *Register* from the *File* menu, enter the activation code we sent, and click the *Activate* button. Once you do this, HandNet is permanently functional.

Import TZ: This lets you change the access profile to *Always* or *Never* for many users based on information in a text file; see *Changing Access for Many Users at Once* on page 95.

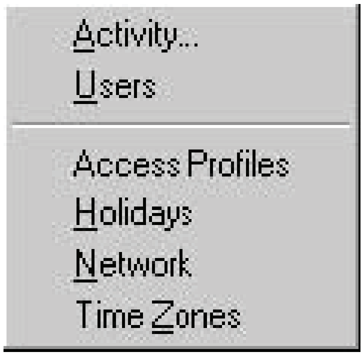
Import Users: If you have readers connected to several different computers (each with its own copy of HandNet) and if users added to one system need to be available on the others, *Import Users* lets you bring in users that were added or changed in another copy of HandNet; see page 99. If all of your readers are connected to a single copy of HandNet, you do not need this feature.

Export Activity: If you want to create custom activity reports using some external report tool, *Export Activity* sends all of your current activity to an access database file called *expactvt.mdb*; see page 115. The main HandNet database files are password protected for security reasons, but this file is not, so you can open it and access any information in it. If you are only going to generate reports with *Activity Reports* on the *File* menu, you do not need this option; using it would only create a file that you do not need.

Exit: This closes the HandNet program, disconnecting it from all readers. All readers will continue to be able to open doors, but the program will not receive any information from the readers or process any alarms while HandNet is not running. Unless you are going to install a new Version of the HandNet software, or you need to restart the computer that HandNet is running on, you do not want to exit the HandNet program. For security purposes, you would generally logout so unauthorized people cannot add users or make changes, but you would leave the HandNet program running all the time.

Reports Menu

To get to the reports menu, click *Reports* on the *File* menu. This menu lets you create custom activity reports and print several stock reports.



Activity: This lets you create reports based on any activity recorded by HandNet. This includes any information in the *Activity* window and any activity that you have chosen to archive. You can customize these reports to include only the information you need; see *Creating and Printing Custom Activity Views* on page 105.

Users: This lists all of the users in the system. The report includes each user's name, ID number, authority level, reject level, and access profile. It also indicates the last reader used, the last access time, and whether the user is enrolled. You can use this report to see if a user is enrolled and to make sure one user is not enrolled with multiple ID numbers. If you have created custom user entries, this report does NOT show any of them.

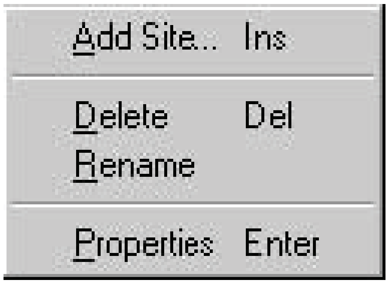
Access Profiles: If you have set up different access profiles to give different types of users access to different readers or at different times, then this report can help you see whether you have set your access profiles up the way you wanted. This report lists each access profile, sites and readers the profile gets access to, and the time zone that users can access each reader; see page 67 for more about setting up access profiles.

Holidays: This list all of the holidays you have set up in HandNet. It lists the name of each holiday, the month, and the date. This report helps you make sure you have correctly added all holidays for the year (if you have set up any time zones to prevent access on holidays, or to give different access on holidays than on other days, the *Holidays* list identifies when those holidays are. If you do not give different access on holidays than on other days, you do not need to set holidays up or print this report); see page 65 for more about setting up holidays.

Network: This report tells whether each site is enabled and connection information (communications port, baud rate, phone number or IP address, time adjustment, and modem speaker status). It also lists readers at the site, whether they are enabled, and their addresses. This report is used during setup to make sure the network is set up properly.

Time Zones: This lists all of the different user access period that you have set up (though we call these access periods *time zones*, they have no connection to the time zones we usually think of that have to do with different times around the world). The report includes the name of each time zone, the time periods it includes, and the days of the week those time periods apply. During setup, this report helps you see if you have set up all of the necessary time zones and configured them correctly (if you do not need to limit access by day or time -that is, if all users may use the readers twenty-four hours a day, seven days a week if they wanted- then you do not need time zones); see page 61 for more about setting up time zones.

Site Menu



In HandNet, a site refers to a group of up to thirty-two connected readers. Put another way, one reader is physically connected to the computer (by network, serial cable, or modem), and up to thirty-one additional readers can be daisy chained to that first reader; that is, a cable runs from the first reader to the second, another cable runs from the second to the third, and so on. We call this chain of readers a site. A site does not have any connection to a particular building or location; these readers could be in one building or in more than one building (if the buildings are close enough to run a cable from one to the other), and one building could have one or many sites.

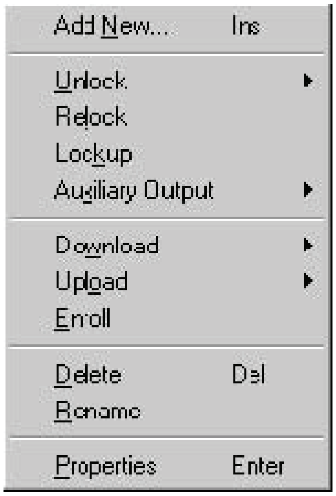
Add Site: This adds a new site to the HandNet network; see page 34. You must set up a site in HandNet before you can set up readers.

Delete: If you have selected a site in the Network window, *Delete* removes the site and all readers assigned to it. HandNet will ask you to confirm that you want to delete the site. Make sure that you have selected the appropriate site since, if you continue, you will not be able to undo the deletion unless you have made a backup of the files that contain your site and reader information (see page 126 for more about making backups).

Rename: If you have selected a site in the *Network* window, this lets you rename that site (you can also just click once on the site name in the *Network* window and rename it there without using this option). Renaming a site does not change any of its properties, and does not require you to set anything up again; it only changes the name that appears in the lists on the screen and in reports that you generate. You might want to rename a site if you discovered that the original name is not clear.

Properties: This takes you to a window with three tabs that let you look at or change settings related to how the site is connected to the computer with the HandNet software; see *Changing a Site* on page 34 for further detail.

Reader Menu



The *Reader* menu lets you add new readers, delete readers, and rename readers in the HandNet network. You can also unlock, relock, and lockup the selected reader, enroll a user at the selected reader, activate and deactivate auxiliary output, and send (download) time, time zones, users, and setup configuration to selected readers.

To do anything here, except add a reader, you must select one or more readers first.

Add Reader: This lets you add and configure a reader to the HandNet network; see page 42 (you must set up a site before you can add readers in HandNet).

Unlock: When you highlight *Unlock* on the *Reader* menu, you see another menu with two choices: *Indefinite* and *Timed*.

Indefinite unlocks the door connected to that reader and leaves it unlocked until you choose *Relock* on the *Reader* menu to lock it again. If you regularly want a door unlocked during certain hours, pick properties from the *Reader* menu and go to the *Configuration* screen. In the *Auto Unlock Time Zone* you can indicate when the door should be automatically unlocked. The program will automatically lock the door again at the end of the time zone.

Timed unlocks the door connected to that reader and leaves it unlocked only for the number of seconds specified on the *Configuration* page in the *Reader Properties* (that is, it unlocks the door for the same number of seconds that the door would be unlocked if it were opened by a reader).

See *Locking and Unlocking Doors* on page 130 for more about these options.

Relock: If you have unlocked a door with *Unlock, Indefinite* option, this locks it again; see page 128.

Lockup: This disables the lock on the door for the selected reader. The reader will still let users enter their ID numbers and still verify hands, but the door will stay locked even for valid users. The door will stay locked until you choose *Unlock* or *Relock*; see page 128.

Auxiliary Output: If an auxiliary device is connected to a reader, this lets you turn that device on or off for the selected reader; see page 129. *Auxiliary Output* can control local lighting, trigger a third party alarm system, activate a bell, and so on.

Download: This lets you send information to the selected readers. While HandNet automatically sends the appropriate information to readers, occasionally you will need to use this when correcting a problem with a reader; see *Resending Information to a Reader* on page 60.

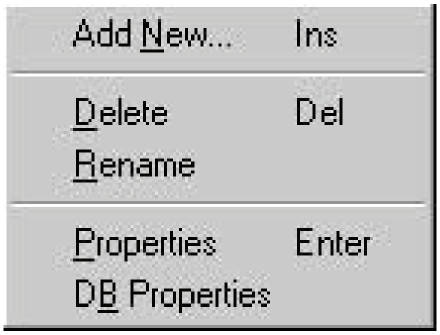
Upload (Users): This lets you get user information from the selected readers. You would do this if you had been using a reader independent of the HandNet program and now wanted to add all of the users stored in that reader to the program; see *Getting User Information from a Reader* on page 99.

Delete: This removes the selected readers from the HandNet network.

Rename: This renames the selected reader. Renaming the reader does not change any of its properties and does not require you to set anything up again; it only changes the name that appears in the lists on the screen and in reports that you generate. You might rename a reader if you discovered that the original name was not clear or if you changed the purpose of the areas the reader gave access to.

Properties: This takes you to a window with a number of tabs that let you look at or change a number of settings related to the reader; see *Changing Reader Settings with Reader Properties* on page 45.

User Menu



The *User* menu lets you add users, delete users, rename users, change information for a selected user, and create custom entries to collect additional information about users (if you have already set up users in a reader that you are connecting to HandNet, do not recreate those users; you can *Upload Users* from the reader; see *Getting User Information from a Reader* on page 99).

To change, delete, or rename users, select a user first on the list of users (for the list of users, pick *Users* from the *View* menu, or press *CTRL-U*).

Add New: This lets you add new users; see page 74. After you add the user, you must enroll the user (see page 87) before the user will have access through the readers.

Delete: This lets you remove a user from the program. You would do this if you never wanted that user to be able to use any of the readers in the HandNet network (if you might need the user again but want to keep the user from using any of the readers, you can also change the user's access profile to *Never*).

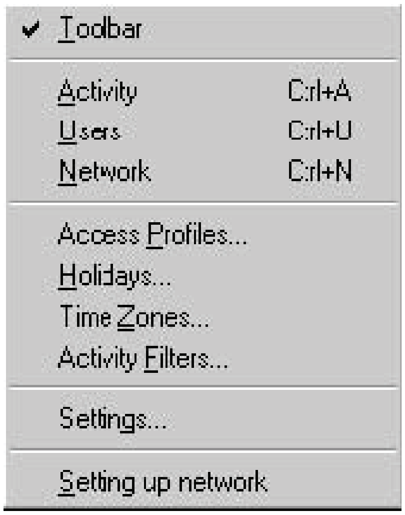
Rename: This lets you rename the selected user. You would use this if you entered the user's name incorrectly. You would also use this if you added multiple users at once. When you use *Add multiple new users* to add a number of users automatically, the program uses the ID number for the name. You would want to rename these users so you could identify which ID is for which user.

Properties: This lets you look at or change information for the selected user; see *Changing Users* on page 90.

DB Properties: This gives you a summary of the total numbers of enrolled and unenrolled users. It also lets you add custom entries so you can collect additional information about users. For example, depending on your needs, you might collect emergency phone numbers, birthdays, employment start dates, or any other information you needed about your users; see *Adding Custom User Entries* on page 97.

View Menu

The *View* menu lets you open the *Users, Activity,* and *Network* windows (the *Activity* window lists both activity and alarms; the *Network* window lists all of your sites and readers). The *View* menu also lets you turn the toolbar on or off.



It also lets you get to access profiles, holidays, activity filters, time zones, and system settings. You do not need these options on an ongoing basis; they are normally only used when setting HandNet up.

Toolbar: This turns the toolbar off if it is on and turns it on if it is off. The toolbar has icons that help you quickly get to common options; see page 7. The toolbar is shown when you start HandNet. A check is shown by this option when the toolbar is displayed.

Activity: This opens the *Activity* window (or brings it to the front if it is already open and behind other windows). This lets you see recent activity and alarms. If you have created any activity filters to create lists of specific types of activities, these views are also available here. The tabs at the bottom of this window let you switch between the activity list, the alarm list, and any custom views you have created; see page 101 for more about the *Activity* window.

Users: This opens the *Users* window (or brings it to the front if it is already open and behind other windows). This window lists everyone who could potentially gain access through a hand reader; see page 71 for more about the users window (there is no connection between this list and the operators authorized to use HandNet; for people who can use HandNet, see the *Operators* tab in *System Settings* on page 24).

Network: This opens the *Network* window (or brings it to the front if it is already open and behind other windows). This window lists all of your sites and readers; see page 31 for more about the *Network* window.

Access Profiles: If some users can only use certain hand readers and/or only use them at certain times or on certain days, access profiles define when each type of user can use each reader. For example, suppose your maintenance staff should have access to the maintenance rooms seven days a week, your office staff should have access to the office but only during business hours, and your supervisors should have access to everything at any time. You would create three access profiles: one for supervisors, one for office staff, and one for maintenance personnel. These profiles would identify which readers each group could use. In these profiles you would also identify which time periods each group could use the different readers (you would set up these time periods first using time zones). After creating these different profiles, whenever you added a user, you would just identify which group the user was a part of, and the access profile for that group would automatically give the appropriate access; see page 67 for more on setting up access profiles.

To limit access to certain days or times, you must set up time zones before creating access profiles.

If you want all users to be able to use every reader any time, you do not need to set up access profiles. HandNet comes set up with an *Always* profile that lets users use any reader in the system twenty-four hours per day, seven days per week. It also has a *Never* profile that does not let the user verify at any reader at any time.

Holidays: If you have set up any time zones to prevent access on holidays or to give different access on holidays than on other days, the holidays list identifies when those holidays are. If you do not give different access on holidays than on other days, you do not need to use this option; see page 65 for more on setting up holidays.

Time Zones: If you want some users to be able to use certain readers only during certain hours or on certain days of the week, time zones let you identify when access is available. For example, suppose some users should only to be able to gain access through certain readers between 8:00 AM and 5:00 PM, Monday through Friday. You would create a time zone that identified these times and days, associate that time zone with appropriate readers using an access profile, and then assign that access profile to the users. After you did this, users with that access profile would only have access during the times you identified in the time zone; see page 61 for more on setting up time zones.

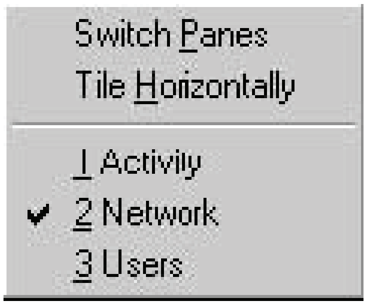
If you do not need to limit access by day or time (that is, if users could use the readers twenty-four hours a day, seven days a week if they wanted), then you do not need to set up time zones.

Activity Filters: This lets you customize the information you see in an activity window by letting you identify the dates, times, sites, readers, users, message types, and messages you want to see. For example, suppose you want to see who's come in through the main entrance without having to wade through messages related to activity at other readers. You could create an activity profile that listed activity only from the main entrance reader and only if the activity was *Identity verified* (the message you get when someone enters an ID and the hand is recognized). You would then be able to choose this view and see only this activity. Activity filters can be much more complex than this; they can filter or limit an activity list to include any subset of information you need (after you create an activity filter, a tab at the bottom of the activity window will list the name of the filter; just click that tab for the corresponding information); see *Creating a Custom Activity View* on page 105 for more information.

Settings: This lets you look at or change system-wide settings; see page 22. This includes the name of the system, security, who can use HandNet, which messages trigger alarms, when old messages should be archived, and settings for importing and exporting users.

Window Menu

The *Window* menu lets you switch between open windows, tile open windows horizontally on the screen, or switch panes within the *Network* window.



You will see a check mark to the left of the window that is currently active.

Switch Panes: If the *Network* window is open, *Switch Panes* switches you back and forth between the list of sites in the left pane of the window, and the list of readers in the right pane of the window. This is primarily useful for users who cannot use a mouse; if you can use a mouse, it is easier to just click the pane you want. If the *Network* window is not open, this choice does not do anything.

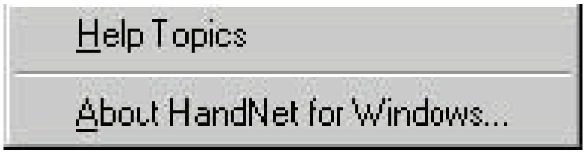
Tile Horizontally: This adjusts any open windows so they fill the HandNet window from side to side and so they do not overlap and cover each other up. If you are not sure what tiling is, see the example on page 9.

Activity: This choice is only here if you have the *Activity* window open. This makes the *Activity* window the active window (if the *Activity* window is not open, open it by typing *CTRL-A* or by picking *Activity* from the *View* menu). The *Activity* window shows the activity log, error messages, and any custom activity views you have created; see page 101 for more about the *Activity* window.

Network: This choice is only here if you have the *Network* window open. This makes the *Network* window the active window. The *Network* window lists sites and readers (if the *Network* window is not open, open it by typing *CTRL-N* or by picking *Network* from the *View* menu); see page 31 for more about the *Network* window.

Users: This choice is only here if you have the *Users* window open. This makes the *Users* window the active window (if the *Users* window is not open, open it by typing *CTRL-U* or by picking *Users* from the *View* menu); see page 71 for more about the *Users* window.

Help Menu



Instead of going to the *Help* menu, you can press *F1* from any screen in HandNet. This takes you to help for the screen you are on. If you need help on something else, you can use the *Contents, Index*, or *Search* tabs at the left of the window to find what you need.

Help Topics: This brings you into the help for HandNet. The *Help* menu contains the same information as this manual, but it lets you more easily search and jump from topic to topic; see page 3.

About HandNet for Windows: This brings up a screen with copyright information, the Version of the program, the product serial number, and the name of the person or company the product is licensed to (unless you need to give your serial number or the program Version number to one our support representatives, or unless you need to check to see if you are licensed to use all the features of the program, you probably will not need to come to this screen).

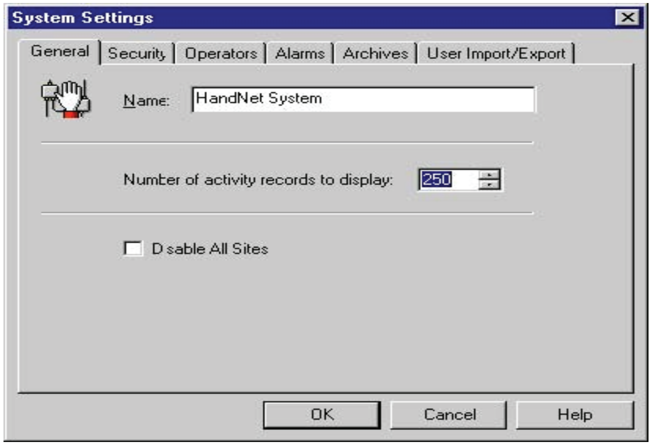
* * * * *

System Wide Settings

Settings on the *View* menu lets you control setup issues that are not related to specific sites or readers. This includes the name of the system, what user changes should be allowed at readers, who can use Handnet, which messages trigger alarms, when old messages should be archived, and settings for importing and exporting users.

General System Settings

To get to the *General* tab, pick *Settings* from the *View* menu.



System Settings

Name: HandNet System

Number of activity records to display: 250

□ D sable All Sites

Name of System

Name: This shows the name that appears above the list of sites in the *Network* window.

Amount of Activity to Show

Number of Activity Records to Display: This shows how many of the most recent activities to list in the *Activity* window. HandNet stores activities even after they are no longer listed in the *Activity* window; those that are no longer shown are still stored and still included if you print a report.

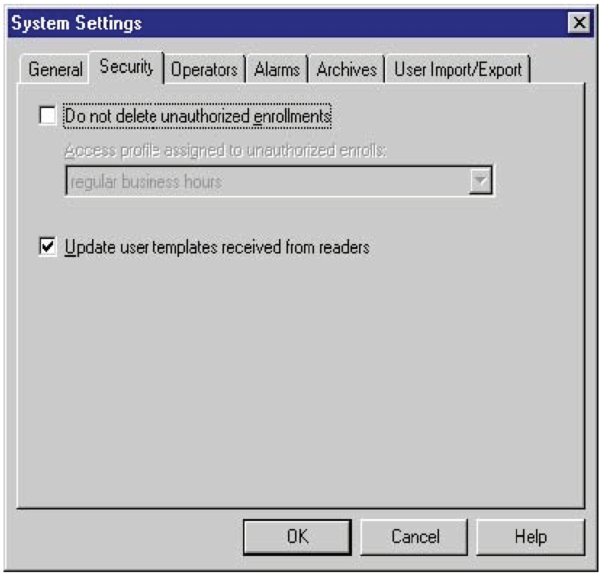
Disable All Sites

Disable All Sites: Check this box if you need to quickly prevent HandNet from trying to communicate with any site. You might check this if you were servicing a number of sites at once.

* * * * *

What User Changes Can Come from Readers

To get to the *Security* tab, pick *Settings* from the *View* menu, and then click the *Security* tab.



□ Do not delete unauthorized enrollments

Access profile assigned to unauthorized enrolls: regular business hours

☑ Update user templates received from readers

Whether Users can be Added at the Reader

Do not delete unauthorized enrollments: When this is not checked (HandNet's initial setting) you can only add new users in HandNet; you cannot add a new user directly at the reader (you can add a user at a reader if the user is in HandNet so you can enroll the user, but if you add a user at the reader that has not been added in HandNet, HandNet will delete the new user). If you want to be able to add and enroll a new user at a reader without adding the user in HandNet first, check this box. If you allow this, and if you add a new user from the reader, the user will be given the access profile selected in the entry below (you can change the access profile on the *Security* tab in *User Properties*; see page 92).

Access profile assigned to unauthorized enrolls: Indicate what access profile should be given to a user who is added at a reader (if you do not want the user to be able to access any readers until you change them in HandNet, choose *Never*).

Whether to Revise the Stored Images of Users' Hands

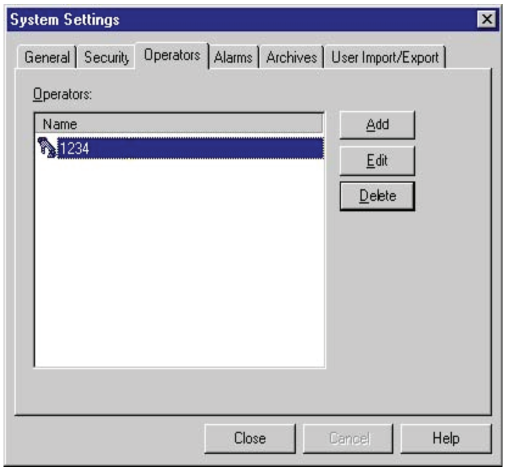
Update user templates received from readers: When you enroll a user, HandNet stores a template that contains information about the shape of the user's hand. If this box is checked, then each time a user gains access, HandNet updates this template. This means that if the user's hand changes gradually (for example, if the user gains or loses a significant amount of weight over time), the image of the user's hand in HandNet will automatically be gradually adjusted as well. If there are gradual changes, checking this prevents users from having access problems as their hands become increasingly different from the original image. If you do not check this, then readers will always compare the user's hand to the original image created when you enrolled the user. We recommend having this checked.

* * * * *

Who Can Use HandNet

The *Operators* tab lists those people who are authorized to use the HandNet program. When you click *Add* or *Edit*, the program brings up the *Operator Definition* box where you control which tasks the operator is allowed to do in HandNet.

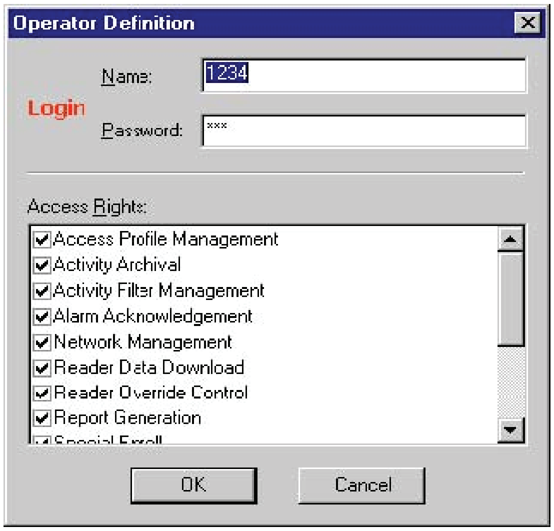
To get to this screen, pick *Settings* from the *View* menu, and then click the *Operators* tab.



1234

Adding or Changing an Operator

You see this box when you add or edit an operator. It has the name and password the operator must use to log into HandNet. The boxes that are checked control which types of activities the operator can do.



Name: 1234

Password: ***

☑ Access Profile Management
☑ Activity Archival
☑ Activity Filter Management
☑ Alarm Acknowledgement
☑ Network Management
☑ Reader Data Download
☑ Reader Override Control
☑ Report Generation
☑ Special Enroll

Name: Enter the name that the operator will enter on the *Login* screen; see page 4. If the operator is also a user in HandNet (so s/he can gain access through readers), the name you enter here does NOT have be the same as the name in *User Properties*.

Password: Enter the password that the operator will enter on the *Login* screen. Passwords are NOT case sensitive. For example, if the password is *narnia, Narnia* and *NARNIA* would work identically.

Which Options the Operator Can Use

Access Rights: Check the corresponding boxes to determine which tasks the operator can do in HandNet. When you add a new operator, all of the boxes are unchecked; unless you check them, the operator will be able to do little more than look at information on the screen.

Click OK to save your changes and return to the list of operators.

Deleting an Operator

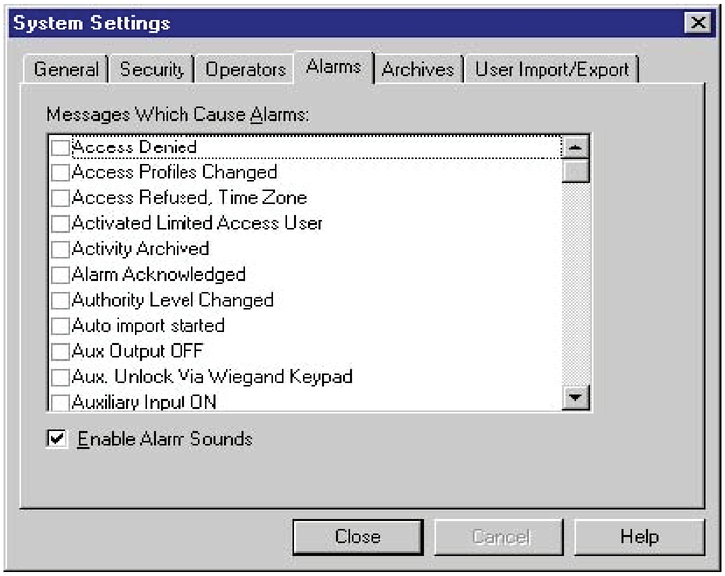
To delete an operator so that person will no longer have access to HandNet, click the operator in the list and click *Delete*. HandNet does NOT ask you to confirm this deletion, so make sure you have highlighted the right operator before you click delete.

If the operator is also a user and if you do not want the user to have access to readers anymore, you must also delete the person from the user list.

* * * * *

Which Messages Trigger Alarms

The *Alarms* tab controls which activities generate alarms in HandNet. To get to this screen, pick *Settings* from the *View* menu, and then click the *Alarms* tab.



Messages Which Cause Alarms:

□ Access Denied
□ Access Profiles Changed
□ Access Refused, Time Zone
□ Activated Limited Access User
□ Activity Archived
□ Alarm Acknowledged
□ Authority Level Changed
□ Auto import started
□ Aux Output OFF
□ Aux. Unlock Via Wiegand Keypad
□ Auxiliary Input ON

☑ Enable Alarm Sounds

Messages That Cause Alarms

Messages Which Cause Alarms: Check each message that should generate an alarm. What you check here only determines what triggers an alarm in the HandNet program; if you are connected to an auxiliary or external alarm system, actions that trigger external alarms are controlled by the *Auxiliary (AUX) Settings* (see page 48) and *Extended Setup* (see page 51) tabs in *Reader Properties*.

Alarms Sounds

Enable Alarm Sounds: If this is checked, then when an alarm situation occurs, a loud, siren-like alarm sound will begin and continue until you acknowledge the alarm. If this is not checked, when an alarm situation occurs, you will see a red flashing message at the bottom of the screen but will not hear any sound.

* * * * *

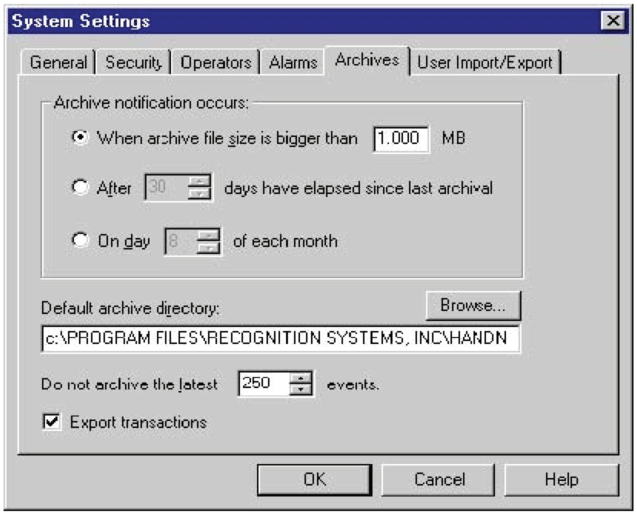
When Past Activity Gets Archived

What Archiving Is

Archiving is moving past activity from the current activity file to a separate file. This keeps the activity file smaller and faster while still keeping the information available for reports if needed. The *Archive* tab controls when HandNet reminds you to archive past activity, where it will make the archive file if you do not choose another location, and the minimum amount of activity to keep available in the current activity file.

You can make an archive at any time use *Archive* on the *File* menu; see page 113.

To get to the *Archives* tab, pick *Settings* from the *View* menu, and then click the *Archives* tab.



Archive notification occurs:

● When archive file size is bigger than 1.000 MB

○ After 30 days have elapsed since last archival

○ On day 8 of each month

Default archive directory: c:\PROGRAM FILES\RECOGNITION SYSTEMS, INC\HANDN

Do not archive the latest 250 events.

☑ Export transactions

When HandNet Reminds You to Make and Archive

Archive Notification Occurs: This controls when HandNet reminds you to make an archive.

When archive file size is bigger than... reminds you only when there is enough activity for the archive file to reach the size you enter. How long it will take depends on the amount of activity.

After ___ days... reminds you make an archive on a regular basis regardless of the amount of activity during that period. For example, if you wanted to make an archive once a year, you could select this option and enter 365 for the number of days.

On day ___of each month reminds you make an archive once a month. If you want to include all activity from a particular month in the archive, and you also want to keep a number of days worth of recent activity available in the activity window, then you might want to do this later than the first of the month and change the *To* date to the last day of the previous month when you make the archive. For example, if you wanted to keep activity from the past week in the current activity, then you might not make your monthly archive until the 8th of the month. That way, when you have made your archive through the end of the previous month, the past week would still be in the current activity.

Default Archive Directory: This shows the drive and directory (folder) that is automatically filled in for the file location when you make the archive. This is initially set to the same folder that the HandNet program is in, but you can change this if you wish.

What NOT to Archive

Do Not Archive the Latest __ Events: This indicates how many events or activities to keep in the current activity file. You can choose from 1-500. When you make an archive, HandNet this number of the most recent events in the activity file. If you want to keep more events than this in the current activity file, you can do this when you make the archive by changing the *To* date. For example, if you always wanted to keep at least the activity for the past week, when you make the archive, you could set the *To* date a week in the past.

Exporting Activity When Archiving

Export Transactions: If you check this, then whenever you make an archive, HandNet exports all the transactions being archived to an access database file called *expactvt.mdb* (you can also export transactions with *Export Activity* on the *File* menu; see page 115). While the main HandNet database files are password protected for security reasons, this file is not. This lets you create custom activity reports using the activity from HandNet using external report generating tools. If you are only going to generate reports with *Activity Reports* on the *File* menu, you do not need to check this box; doing so would only create a file that you do not need.

* * * * *

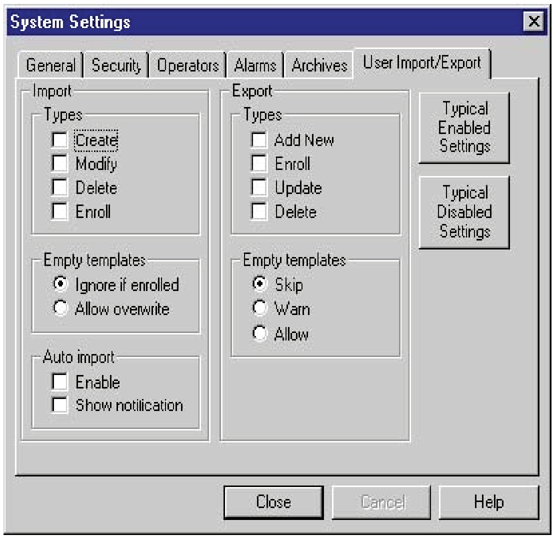
When Users Get Imported and Exported

User Import/ Export Tab

The *User Import/Export* tab is only available if you have purchased the upgrade to the full feature set of Version 2.0.

This tab controls what user information is imported and exported, and whether imports are automatic or manual. You only need this tab if you have readers connected to several different computers (each with its own copy of HandNet) and if users added to one system to be available on the others. If all of your readers are connected to a single copy of HandNet, you do not need this feature.

To get to this screen, pick *Settings* from the *View* menu, and then click the *User Import/Export* tab.



Import

Types

☐ Create
☐ Modify
☐ Delete
☐ Enroll

Empty templates

● Ignore if enrolled
○ Allow overwrite

Auto import

☐ Enable
☐ Show notification

Export

Types

☐ Add New
☐ Enroll
☐ Update
☐ Delete

Empty templates

● Skip
○ Warn
○ Allow

Setting Up for Common Situations

If all of your readers are connected to a single copy of HandNet: You do not need this feature. Click the *Typically Disabled Settings* button to make sure that the import and export features are both turned off.

If you have HandNet running on several computers and you want to be able to add, change or delete users from any of those computers: Click the *Typically Enabled Settings* button to turn both the import and export features on.

If you have multiple computers with HandNet but you only want users added, changed, deleted, or enrolled on this computer: Check the *Enroll, Update*, and *Delete* boxes in the *Export* column, and uncheck all of the boxes in the *Import* side of the screen. This causes HandNet to export users but prevents changes from elsewhere from being imported.

If you have multiple computers with HandNet but you only want users added, changed, deleted, or enrolled on another computer: Check the *Create, Modify, Delete* and *Enroll* boxes in the *Import* column, and uncheck all of the boxes in the *Export* side of the screen (you can also enable *Auto Import* if you wish). This keeps HandNet from creating an export file that you do not need, and enables it to import changes from another computer.

Import Settings

Types: This controls what user information HandNet will import. Make sure that you select the correct choices here before you try to import. When HandNet imports, it empties the *Import* file, discarding those user records that do not meet the conditions you have checked here.

Create: If this box is checked and HandNet finds a new user in the *Import* file, HandNet adds that user to your database. If this box is not checked, HandNet will not import any new users.

Modify: If this box is checked and HandNet finds a user in the *Import* file with the same ID number as a user that you already have, HandNet replaces the information for the user you have with the user in the *Import* file. If this box is not checked and HandNet finds a user in the *Import* file with the same ID number as a user that you already have, HandNet will not change the user that you have. If you do not have this checked, you could end up with different information for a user on different computers.

Delete: If this box is checked and HandNet finds a user marked for deletion in the *Import* file, HandNet deletes that user from your computer as well. If you do not have this checked, you could end up users that are still on your computer that are not in the copies of HandNet running on the other computers.

Enroll: If this box is checked and HandNet finds a newly enrolled user in the *Import* file, HandNet imports the user and the template (image of the user's hand). If you do not check this, you will have to enroll new users on each computer where they are imported.

Empty Templates: If HandNet finds a user that is not enrolled in the *Import* file, and it finds a user with the same ID number that is enrolled, this entry controls what HandNet will do. *Ignore if enrolled* keeps the enrolled Version of the user that you already have rather than replacing the user with the unenrolled user. *Allow overwrite* replaces the enrolled user with the unenrolled one; this means that the user will have to be enrolled again (to avoid this, on the computer that is exporting the users, do not check *Add New* on the *Export* side and make sure *Empty Templates* on the *Export* side is set to *Skip*. This way, users will not be exported until they are enrolled).

Auto Import:

Enable: If you check the *Enable* box, HandNet automatically import users whenever it finds an *import.mdb* file in the HandNet directory. If this box is not checked, then HandNet only import users when you pick *Import Users* from the *File* menu; see page 99.

Show Notification: If you check this box and the *Enable* box above is also checked, then when HandNet automatically imports users, it shows a message on the screen that lets you know that users are being imported. If you do not check this box, then HandNet just imports the users without popping a message up (either way, HandNet also records the activity in the *Activity* window). If the *Enable* box is not checked above, this entry does not apply.

Export Settings

Types: This controls what user information HandNet exports.

Add New: If this box is checked and you add a user, HandNet exports the user. Normally you do not want this box checked; you usually want HandNet to wait until the user is enrolled before exporting the user. If you have this checked, HandNet exports the unenrolled user.

Enroll: If this box is checked, then HandNet exports a new user after the user is enrolled.

Update: If this box is checked and change information for a user, HandNet exports the changed information. This can help keep user information the same on all of the computers.

Delete: If this box is checked and you delete a user, HandNet exports the fact that the user was deleted. If the other copies of HandNet are set up to import deletions, then the user will be removed from those computers as well.

Empty Templates: If you add or change a user that has not been enrolled yet, this controls whether or not HandNet will export it. Normally you only want HandNet to export users after they are enrolled, so you would leave this set to *Skip*.

"Typical" Settings

These buttons automatically check the appropriate options for two situations:

Typically Enabled Settings: This checks the appropriate boxes for a computer to be able to automatically import and export users.

Typically Disabled Settings: This unchecks all of the boxes; this is appropriate for any user who is not running HandNet on more than one computer.

See *Setting Up for Common Situations* on page 28 for more on common setups.

Getting Exported Users to Another Computer

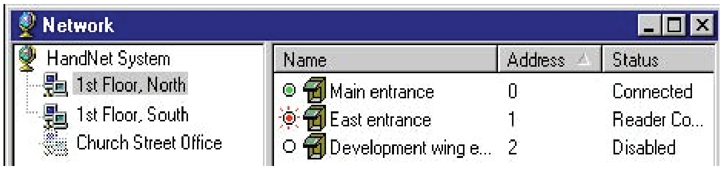
See *Importing Users from Another Copy of HandNet* on page 99 for more on how to get the exported user information to the other computer so you can import them there.

* * * * *

Setting Up Sites and Readers

Seeing Sites and Readers in the Network Window

The *Network* window lists every site and reader that you have added in HandNet. To open this window, pick *Network* from the *View* menu or press *CTRL-N*.



Network

HandNet System
- 1st Floor, North
- 1st Floor, South
- Church Street Office

	Name	Address	Status
🟢	Main entrance	0	Connected
🔴	East entrance	1	Reader Co...
○	Development wing e...	2	Disabled

The left pane lists all of your sites (that is groups of connected readers). The right pane lists all of the readers in the currently selected site (to list all readers for all sites, click *HandNet System* at the top of the left pane).

Understanding the Icons to the Left of the Name

You see one of these icons to the left of each reader's name:

🟢	The green light indicates that this reader is currently connected and communicating with HandNet.
◉	The black dot indicates that HandNet communicates with this reader by modem, and HandNet is not currently connected with the reader (when HandNet connects with the readers in that site depends on what you have on the *Schedule* tab in *Site Properties*).
○	The empty circle indicates that you have not enabled this reader. This is the case when you are setting a new reader up (you enable a reader on the *General* tab in *Reader Properties*. You must also enable the site on the *General* tab in the *Site Properties*).
🔴	The red light indicates that there is a communication problem between HandNet and the reader. The reader may not be configured correctly, or there may be a problem with the way the reader is connected.

Changing How the Readers are Sorted

You can sort the list of readers using the information in any column by clicking on the column heading. For example, to sort the list alphabetically by name, click on the name heading. If you click on the same heading again, it will sort the list in reverse order; for example, using the name, it would sort from Z to A. You can also sort by address (this might be useful if you wanted to find the next available number for a new reader), by status (this could be useful to group all of the readers that are not enabled or that are having communication problems), or by site if you clicked *HandNet System* at the top of the site list to list all readers from all sites at once.

Rearranging or Resizing the Columns

To move any column, click the column heading and hold the mouse down. With the mouse held down, drag the column heading to the left or right (see the *User's window* in the online help for an example of this).

You can also change the width of a column by pointing to the edge of the column heading, holding the mouse down, and then dragging the edge of the column to the desired position. This lets you fit more columns in the window.

F5 restores all columns to the width they had when you started HandNet. If you want HandNet to save the new column widths, exit the HandNet program and come back in. HandNet then uses your changed column widths as the new standard or default.

* * * * *

Setting Up Sites, Overview

What a Site Is

In HandNet, a site refers to a group of up to thirty-two connected readers. Put another way, one reader is physically connected to the computer (by network, serial cable, or modem), and up to thirty-one additional readers can be daisy chained to that first reader; that is, a cable runs from the first reader to the second, another cable runs from the second to the third, and so on. We call this chain of readers a site. A site does not have any connection to a particular building or location; these readers could be in one building or in more than one building (if the buildings are close enough to run a cable from one to the other), and one building could have one or many sites.

You control access to each reader separately, so having readers with unrelated purposes in one site is fine; the site designation merely indicates that the readers are physically connected to each other.

There are two parts to setting up a site and readers: you must physically set the readers up and connect them to each other and to the computer, and you must add the site and readers in HandNet. This help only explains adding the site in HandNet. For help setting up and connecting the readers, see the manual that came with the readers.

Before You Enable a Site

If you have been using readers without HandNet and you want to get the users from the reader(s), follow these steps BEFORE enabling the site and reader:

1. Pick *Settings* from the *View* menu.
2. Click the *Security* tab.
3. Check the box by *Do not delete unauthorized enrollments* (see page 23 for more about what this option does; after you have gotten your users from the reader, you may want to check this box again).

If you enable both the site and the reader without changing this setting, HandNet regards all of the users in the reader as unauthorized (because they are not in HandNet yet) and deletes them from the reader. Once it deletes them, there is no way to get them back without adding and enrolling the users again.

* * * * *

Adding or Changing a Site

QUICK STEPS

Adding a Site in HandNet

1. Click *Site* on the main menu bar at the top of the screen, and then pick *Add Site*. This starts the *New Site Wizard*.
2. Complete each screen and then click the *Next* button at the bottom of the screen. The screens that you see in this process vary depending on whether the site is connected to the computer by a serial cable, through a network, or by a modem.
3. On the final screen, indicate whether to enable site
   If the site is physically set up and connected: Enable the site now. Check the *Enable Site* box and then click *Finish*.
   If the site is not physically set up yet: Enable the site later. To do this, you will open the *Network* window, double-click the site in the left pane of the window to open up the site properties, check the *Enabled* box, and then click *OK*.

Adding a Site

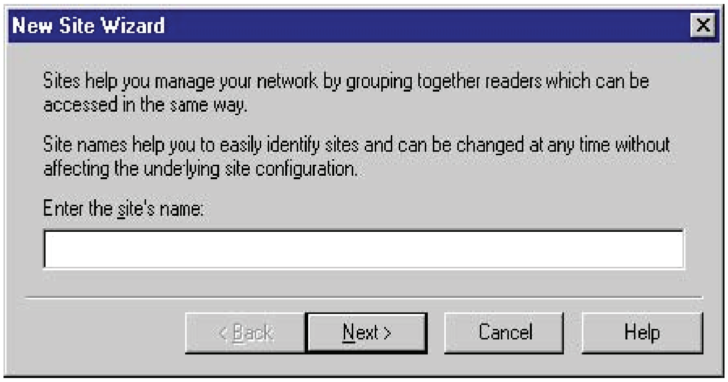
Click *Site* on the main menu bar at the top of the screen, and then pick *Add Site*. This starts the *New Site Wizard*.

Changing a Site

Click a site in the left pane of the *Network* window, pick *Properties* from the *Site* menu, and then click the tab with the information you need to change.

Name

This is the first screen in the process of adding a new site. Enter a name that identifies the site, and then click the *Next* button.



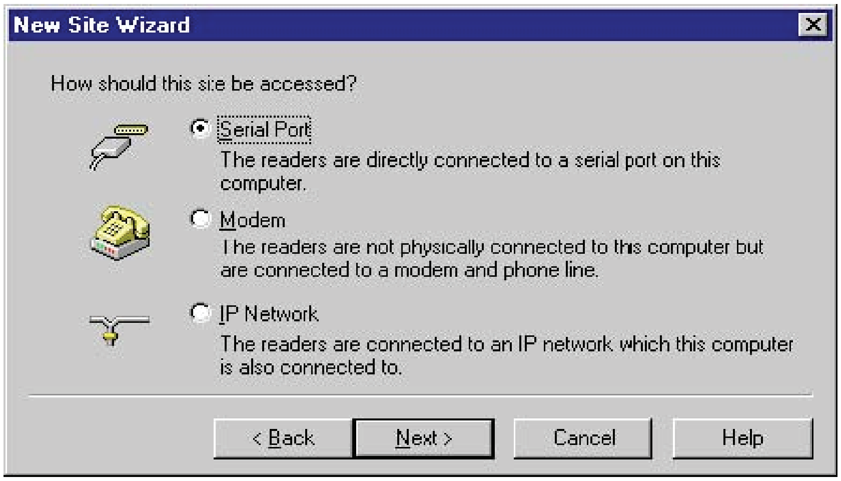
Sites help you manage your network by grouping together readers which can be accessed in the same way.

Site names help you to easily identify sites and can be changed at any time without affecting the underlying site configuration.

Enter the site's name:

Type of Connection

When adding a new site, this screen lets you indicate how HandNet will communicate with the site.



How should this si:e be accessed?

● Serial Port
The readers are directly connected to a serial port on this computer.

○ Modem
The readers are not physically connected to this computer but are connected to a modem and phone line.

○ IP Network
The readers are connected to an IP network which this computer is also connected to.

Serial Port: To connect to a site by running a cable from your computer to the reader, you must have a free serial port on your computer. See the HandKey manual for more on the requirements for the cable. This first reader must have an address of zero (and no other reader in the site can have an address of zero).

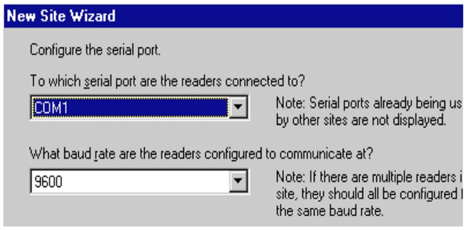
Modem: To connect to a site by modem, the first reader in the site must have a modem installed in it (contact your dealer for more information). This first reader must have an address of zero (and no other reader in the site can have an address of zero).

IP Network: To connect to a site through your network, you must have a TCP/IP network with static IP addresses. Your computer must have a network card and be connected to the network. If the network is faster than 10baseT, you must have a switching hub. The first reader in the site must have an ethernet card (contact your dealer for more information). This first reader will automatically have an address of zero (no other reader in the site can have an address of zero), and you must enter a unique IP address in the reader; see *Configuring the Physical Reader* on page 54 for more detail on this.

Serial Port Connection

To connect to a site by running a cable from your computer to the reader, you must have a free serial port on your computer; see the HandKey manual for more on the requirements for the cable. This first reader must have an address of zero (and no other reader in the site can have an address of zero).

when adding a new site



New Site Wizard

Configure the serial port.

To which serial port are the readers connected to?

COM1

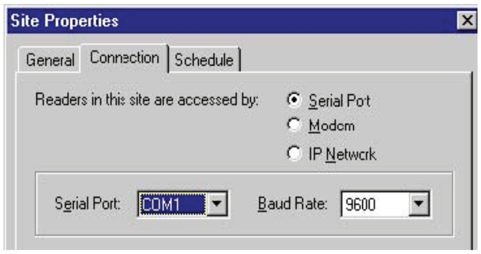
Note: Serial ports already being us by other sites are not displayed.

What baud rate are the readers configured to communicate at?

9600

Note: If there are multiple readers i site, they should all be configured t the same baud rate.

when changing a site



Site Properties

Readers in this site are accessed by: ● Serial Port ○ Modem ○ IP Network

Serial Port: COM1   Baud Rate: 9600

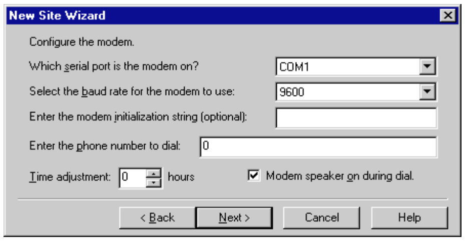
Serial Port: Click this and pick the serial port that the cable from the reader is connected to. If you pick the wrong port here, HandNet will not be able to communicate with the reader. If you have several sites, each must be connected to a different serial port. HandNet only lists ports set up on your computer that are not already used for communicating with another site. If you click this and get a blank list, all of the serial ports are already used. Contact the person who services your computer hardware if you need to add additional serial ports.

Baud Rate: Click this and pick the baud rate, we recommend 9600. While 19200 should theoretically be faster, because of the way the reader sends information, this does not result in any real gain. The speed here must match the speed set in the reader; see *Configuring the Physical Reader* on page 54 for more detail on how to change the baud rate in the reader.

Modem Connection

To connect to a site by modem, the first reader in the site must have a modem installed in it (contact your dealer for more information). This first reader must have an address of zero (and no other reader in the site can have an address of zero).

when adding a new site



New Site Wizard

Configure the modem.

Which serial port is the modem on? COM1

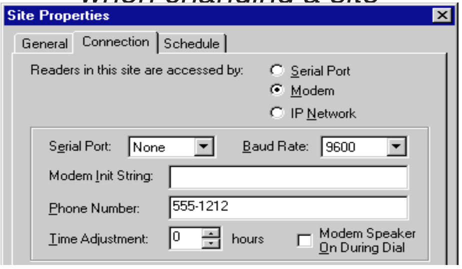
Select the baud rate for the modem to use: 9600

Enter the modem initialization string (optional):

Enter the phone number to dial: 0

Time adjustment: 0 hours ☑ Modem speaker on during dial.

when changing a site



Site Properties

Readers in this site are accessed by: ○ Serial Port ● Modem ○ IP Network

Serial Port: None

Baud Rate: 9600

Modem Init String:

Phone Number: 555-1212

Time Adjustment: 0 hours

□ Modem Speaker On During Dial

Serial Port: If you have an external modem, click this and pick the serial port your modem is connected to; this is usually (but not always) *COM1* or *COM2*. If you have an internal modem, it is usually connected to *COM3* or *COM4*. HandNet only lists ports that are set up on your computer and that are not already used for communicating with another site.

Baud Rate: Choose 9600 if you are connecting to a HandKey II or HandKey CR; choose 2400 if connecting to a HandKey.

Modem Init String: If you need HandNet to send any commands to the modem before dialing, enter the appropriate codes here. The modem must be set up for no data compression, no error correction, an appropriate baud rate, and auto answer. The manual that came with your modem explains the various commands that work with your modem. An inappropriate init string can prevent the modem from connecting. Try connecting without any init string to see if you can communicate; you modem may be automatically set up correctly. If you have problems getting your modem to connect and communicate with the site, here are init strings that have worked for some modems:

Typical Modem Strings		AT&F&C1&D2X1V1E0 AT&C1&D2X1V1E0 AT&C1X1VE0
Rockwell Chip Set Modems		AT&D2E0&Q0N0S37=5
US Robotics Sportster 14.4 F/M		AT&F0 AT&FX0&C1&D2&H0&N6&K0S0=0
Everex 2400E		AT&F
Hayes Accura 14,400	1200 Baud	AT&F&C1&D2&K0S0=0S37=5
	2400 Baud	AT&F&C1&D2&K0S0=0S37=6
Hayes Optima 14,400	1200 Baud	AT&F&C1&D2&K0S0=0S37=5
	2400 Baud	AT&F&C1&D2&K0S0=0S37=6
Practical Peripherals PM144MTII	1200 Baud	AT&F&C1&D2&K0S0=0S37=5
	2400 Baud	AT&F&C1&D2&K0S0=0S37=6
Practical Peripherals 14.4 FXSA	1200 Baud	AT&D2E0&Q0N0S37=5
	2400 Baud	AT&D2E0&Q0N0S37=6

Cardinal 33.6 V.34/V.FC	1200 Baud	ATE0S37=5&C1&D2&K0
	2400 Baud	ATE0S37=6&C1&D2&K0
Multitech Model MT1932ZPX		AT&F&C1&D2X1V1E0&E0&E3&E7&E8 &E10&E12&E14$MB1200$SB1200
Zoom Model cc4336	2400 Baud	AT&Q0&K0+MS=2

Phone Number: If you have to dial some digit to get an outside line, enter this digit followed by a comma before the phone number. If the number is a long distance number, enter the one and the area code as appropriate. For example, if you had to dial a nine for an outside line, and the number was long distance and required one and an area code, you would enter the number like this:

9, 1-802-555-1212

You do not have to enter the dashes; they do not make a difference. You could equally well enter the number above like this:

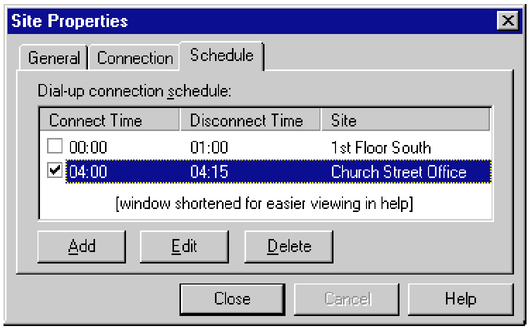
9,18025551212

Time Adjustment: If this site is in a different time zone, enter the number of hours the time difference is. For example, if you are in New York and were setting up a connection with a site in California, you would enter *-3* since in California it is three hours earlier than in New York. If you are in California and setting up a connection with a site in New York, you would enter *3* since it is three hours later in New York. Only do this if you want all times reflecting the time zone you are currently in.

Modem Speaker On During Dial: If you check this box, when HandNet connects to this site, it turns the modem speaker on so you can hear it dialing and connecting. If there is a problem connecting, turning the modem speaker on can help identify where the problem is. Unless you are having a problem connecting, we do not recommend checking this box.

Scheduling a Connection Time

If you are connecting to sites by modem, this screen shows when HandNet is scheduled to connect with each site. You can only change the connection time for the current site (this screen does not apply if you are not communicating by modem; if you connect by serial port or through a network, HandNet stays connected to the site continuously and does not need a scheduled connection time).



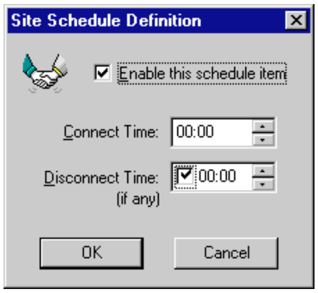
Dial-up connection schedule:

Connect Time	Disconnect Time	Site
□ 00:00	01:00	1st Floor South
☑ 04:00	04:15	Church Street Office

[window shortened for easier viewing in help]

Adding a New Scheduled Connection Time

When you choose to add a new schedule time, you see this screen:



☑ Enable this schedule item

Connect Time: 00:00

Disconnect Time: (if any) ☑ 00:00

Enable this schedule item: This box must be checked for HandNet to make the connection. Only uncheck this box if the modem is not set up yet at the site and you do not want HandNet to try to communicate with the site.

Connect Time: Enter the time that you want HandNet to try to connect. This must be at least one minute later than the disconnect time for the previous connection. For example, if another connection is scheduled to end at 5:00, the new connection can be scheduled for 5:01, but not for 5:00. If the phone lines are busy when HandNet tries to connect, it will keep trying until it makes a connection (or reaches the *Disconnect Time*).

Disconnect Time: If you uncheck this box, HandNet will stay connected to this site continuously. Since the modem will be continuously connected to that site, you will not be able to schedule a connection to any other site; if you need more than one connection, this must be checked. When you enter a disconnect time, it must be after the start time. For example, you cannot schedule a connection to both begin and end at 5:00; if the connection begins at 5:00, the disconnect time must be 5:01 or later.

When you enter the disconnect time, allow enough time for HandNet to download all of the potential activity in the reader. The reader can send about 100 events a minute. This means that if the reader were full (with 5000 events), it could take up to an hour to get all of the activity. The amount of activity you have each day and the number of times you connect to reader during the day determine how long your connection must be.

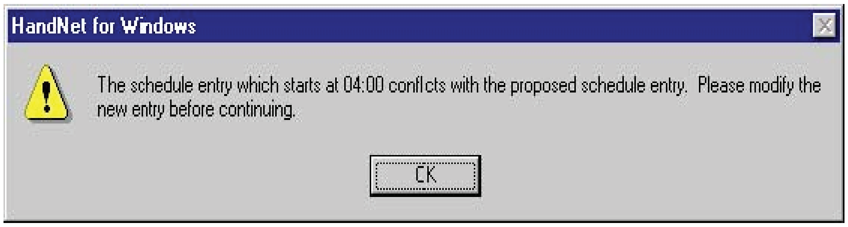
When HandNet reaches the disconnect time, it disconnects even if there is still activity that the reader needs to send. When HandNet disconnects, if the reader is not done sending activity, a few activities would be lost. If there is regularly more activity at the reader than the connection time allows for, the reader's memory would eventually fill up, at which point additional activity would also cause activity to be lost. To avoid this, make sure the time between the *Connect Time* and the *Disconnect Time* is long enough to get all of the activity.

Changing or Deleting a Scheduled Communication Time

Even though HandNet lets you see the scheduled connection times for all sites, HandNet only lets you change a scheduled time for the site with which you are currently working. To change a scheduled time for a different site, you must go to the properties for that site, select the scheduled time there, and then click the *Edit* button.

If You Get a Message that the Time Conflicts

If the time that you enter conflicts with the time that HandNet is already scheduled to communicate with a different site, you see a message like this:



The schedule entry which starts at 04:00 conflcts with the proposed schedule entry. Please modify the new entry before continuing.

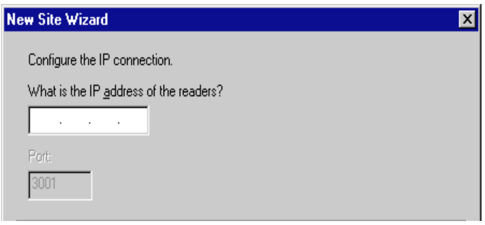
Make sure that each other scheduled connection has a disconnect time. If you schedule a connection with no end time, HandNet would never disconnect from that site, so it would not be possible to schedule another connection. If you want to have more than one scheduled connection, each connection must have a disconnect time.

Also make sure the connect time is at least one minute later than the disconnect time for the previous connection. For example, if another connection is scheduled to end at 5:00, the new connection can be scheduled for 5:01, but not for 5:00.

IP Address

You see this screen if you indicate that HandNet will communicate with this site through a network.

when adding a new site

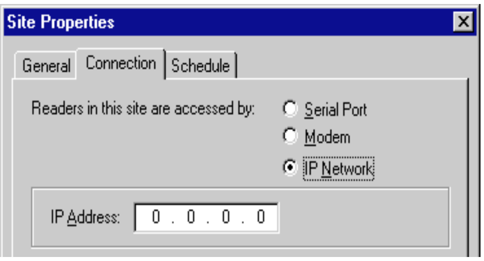


Configure the IP connection.

What is the IP address of the readers?

Port: 3001

when changing a site



Readers in this site are accessed by: ○ Serial Port ○ Modem ● IP Network

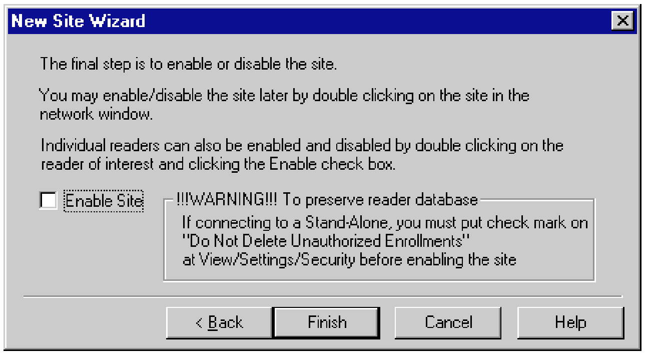
IP Address: 0 . 0 . 0 . 0

IP address: Each site must have a unique IP address. Ask your network administrator for an appropriate address. The address you enter here must match the address you enter in the reader; see *Configuring the Physical Reader* on page 54 for more on how to change the address in the reader.

Port: This entry no longer applies; it is always grayed out.

Enabling the Site

This is the final screen that you see in the *New Site Wizard* (when you go back to *Site Properties* to change this site, this is on the *General* tab).



New Site Wizard

The final step is to enable or disable the site.

You may enable/disable the site later by double clicking on the site in the network window.

Individual readers can also be enabled and disabled by double clicking on the reader of interest and clicking the Enable check box.

☐ Enable Site

!!!WARNING!!! To preserve reader database

If connecting to a Stand-Alone, you must put check mark on "Do Not Delete Unauthorized Enrollments" at View/Settings/Security before enabling the site

Enable Site: You must enable the site before HandNet can communicate with the readers in it, but you might not want to enable it yet. Please read the sections below if you are not sure.

If the site is not physically set up yet

If the site is not physically set up yet, do not enable it; you do not want HandNet to repeatedly try to communicate with something that is not there. This would slow the system down.

If you have been using readers independently of HandNet and you need to get users from the readers

If you have been using readers independently of HandNet and if you want to get the users from the readers into HandNet, **you also do NOT want to enable the site until you have set HandNet to accept users from the reader that are not in HandNet.** To do this:

1. Click *Finish* without checking the *Enable Site* box.
2. Pick *Settings* from the *View* menu.
3. Click the *Security* tab.
4. Check the box by *Do not delete unauthorized enrollments* (see page 23 for more about what this option does; after you have gotten users from the reader, you may want to check this box again).

If you enable both the site and the reader without changing this setting, HandNet will regard all of the users in the reader as unauthorized (because they are not in HandNet yet) and it will delete them from the reader. Once it deletes them, there is no way to get them back without adding and enrolling the users again.

If you are ready to connect

If the site is physically set up and you do not need to get users from the readers (or if you have already changed the setting above), then you can enable the site now. Check the *Enable Site* box and then click *Finish*.

To Enable the Site Later

After you leave this screen, you can enable the site by doing this:

1. Open the *Network* window.
2. Double-click the site in the left pane of the window to open up the site properties (or click once and pick *Properties* from the *Site* menu).
3. Check the *Enabled* box and then click *OK*.

* * * * *

Setting Up Readers, Overview

There are two parts to setting up readers: 1) physically setting the readers up and connecting them to each other and to the computer; and 2) adding the site and readers in HandNet. This manual only explains adding the site and readers in HandNet. For help setting up and wiring readers, see the manual that came with the readers.

Before You Enable the Reader

Before you add readers, you must set up the site they are connected to; see page 34.

If you have been using readers without HandNet and you want to get users from the reader(s), follow these steps BEFORE enabling the site and reader:

1. Pick *Settings* from the *View* menu.
2. Click the *Security* tab.
3. Check the box by *Do not delete unauthorized enrollments* (see page 23 for more about what this option does; after you have gotten your users from the reader, you may want to check this box again).

If you enable the site and the reader without changing this setting, HandNet regards all users in the reader as unauthorized (because they are not in HandNet yet) and deletes them. Once it deletes them, there is no way to get them back without adding and enrolling the users again.

Selecting Readers

Most options on the *Reader* menu are disabled until you select a reader.

To select a single reader: Click that reader in the list.

To select multiple readers that are together on the list: Click the first reader in the group, hold the *SHIFT* key down, and click the last reader that you want to select.

To select multiple readers that are not together on the list: Click the first reader to select, hold the *CTRL* key down, and click each other reader that you want to select.

Renaming a Reader

You might rename a reader if you discovered that the original name was not clear or if you changed the purpose of the areas the reader gave access to. Renaming the reader does not change any of its properties and does not require you to set anything up again; it only changes the name that appears in the lists on the screen and in reports that you generate.

To rename a reader:

1. If the *Network* window is not open, pick *Network* from the *View* menu (or press *CTRL-N*).
2. Click the reader in the right pane of the *Network* window.
3. Pick *Rename* from the *Reader* menu (you could also right click and pick *Rename*, or you could double-click the reader and change the name in the *Reader Properties*).

* * * * *

Setting Up a New Reader

QUICK STEPS

Adding a New Reader

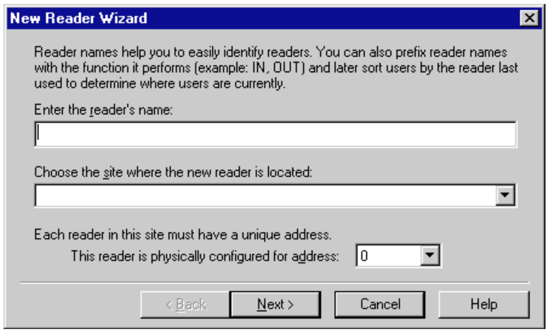
1. Click *Reader* in the main menu bar at the top of the screen, and then pick *Add New*. This starts the *New Reader Wizard*.
2. On the second screen of the *New Reader Wizard*, indicate whether you want to set the reader up by going through each configuration screen, or whether you want to copy the settings from another reader. Copy the settings from another if the settings are identical or even similar to the other reader (if you copy settings, you can use *Properties* on the *Reader* menu to make changes).
3. If you are setting up the reader by going through each configuration screen, see the different tabs in the *Reader Properties* for help with particular entries. Click the *Next* button at the bottom of the screen to continue with the next screen.
4. Make sure that the address in the reader matches the address you entered on the first reader properties screen; see *Configuring the Reader* for more details.
5. Once the reader is physically connected and set up correctly, enable the reader. To do this, open the *Network* window, double-click the site in the right pane of the window to open the *Reader Properties*, check the *Enabled* box, and then click *OK*.

Getting Started

When you pick *Add New...* from the Reader menu, HandNet starts the *New Reader Wizard*. This takes you through the process of adding the reader.

Name and Address Screen

This is the first screen that you see when adding a new reader:



New Reader Wizard

Reader names help you to easily identify readers. You can also prefix reader names with the function it performs (example: IN, OUT) and later sort users by the reader last used to determine where users are currently.

Enter the reader's name:

Choose the site where the new reader is located:

Each reader in this site must have a unique address.

This reader is physically configured for address: 0

Enter the reader's name: Enter any name that clearly describes the reader's function and location. This name is used in the *Activity* window and in activity reports to identify where activity took place.

Choose the site where the new reader is located: Click this to pick the site (group of readers) that this reader is connected to. You must set the site up before you can add the reader.

This reader is physically configured for address: HandNet automatically fills in the first available address that has not been used yet in this site. For example, if you already have readers 0, 1, and 2 in this site, HandNet automatically fills in an address of 3. You can change this if you wish. The first reader in each site my be reader 0; other readers in the site can use any number up to 254. Readers do not need to be numbered sequentially. For example, your readers could be numbered 0, 1, 2, 3... or they could be numbered 0, 100, 110, 137... Within a site, each reader must have a

unique number. For example, you cannot have two readers in the same site that both use the address of 1. However, you can reuse numbers in different sites. For example, if you have twenty sites, you could have a reader with an address of 1 in each of them.

Make sure the address matches the address in the reader

The number here must match the address entered in the reader; see *Configuring the Physical Reader* on page 54 for more on how to set the address up in the reader.

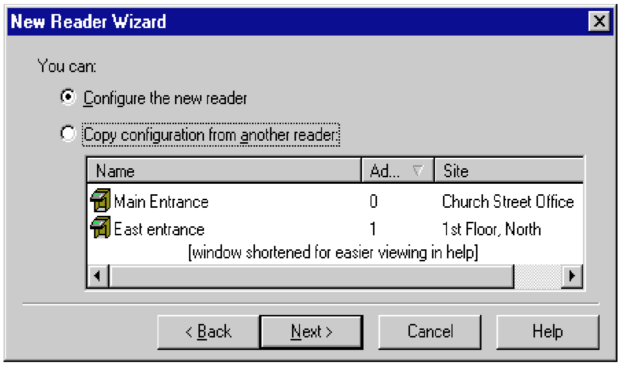
Never put more than 32 readers in a site

Even though HandNet allows numbers from 0 to 254, you should never have more than thirty-two readers in a site. While it is sometimes technically possible to connect more than thirty-two readers, not all readers support this, and even for readers that do, connecting more than this causes unacceptably slow response times from readers. The software was not designed to handle more than this, and we cannot guarantee results with more than thirty-two readers. If you feel that more than thirty-two readers in a single site is essential for you, please contact us to discuss your situation first; in nearly all cases, the preferable (and sometimes only) solution is to set up additional site(s).

Click *Next* to go on to the next screen. This button is disabled until you have filled in all of the entries on this screen.

Configuration

This is the second screen that you see in the process of adding a new reader. This screen lets you choose whether you want to set the reader up by going through each configuration screen in the reader properties, or whether you want to copy the settings from another reader. Copy the settings from another reader if the settings are identical or even similar to the other reader. If you copy the settings from another reader, and you want to make the settings slightly different, you can use *Properties* on the *Reader* menu to make changes; see page 45.



You can:

● Configure the new reader

○ Copy configuration from another reader:

Name	Ad...	Site
Main Entrance	0	Church Street Office
East entrance	1	1st Floor, North

[window shortened for easier viewing in help]

Configure the new reader: This lets you go through each of the *Reader Properties* screens so you can choose the appropriate settings on each. The *Reader Properties* screens are explained starting on page 45. You would choose this for the first reader you add. You would also choose this if you wanted very different settings from the other readers. For example, if other readers are set to trigger an auxiliary alarm after certain events and you do not want this reader to trigger an alarm, or if other readers have an automatic unlock time and you do not want that for this reader, then you might want to use this option.

Copy the configuration from another reader: If another reader has the same or nearly the same settings as you want for this reader, copying settings from the other reader is faster. It also protects you from accidentally

making the settings slightly different if you want readers configured exactly the same way.

If you choose this option, click the reader in the list to copy the settings from and then click the *Finish* button (the *Next* button changes to a *Finish* button when you choose this option).

When you copy the configuration from another reader, HandNet does NOT enable the reader. You must go to the *General* tab in the *Reader Properties* to enable the reader before HandNet will communicate with it; see page 45.

If you copy the settings from another reader, and you want to make the settings slightly different, you can use *Properties* on the *Reader* menu to make changes; see page 45.

* * * * *

Changing Reader Settings with Reader Properties

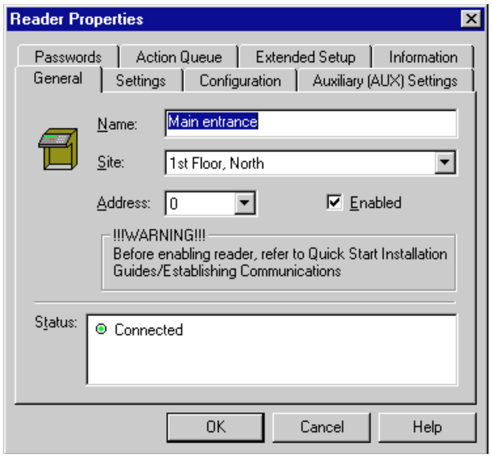
Getting to the Reader Settings

Click a reader in the right pane of the *Network* window, and pick *Properties* from the *Reader* menu (or just double-click the reader in the *Network* window). You are initially on the *General* tab; click any other tab to jump to the corresponding screen.

General

This screen contains the reader's name and address, the site the reader is a part of, and whether or not the reader is currently enabled and connected.

Name: The name is to help you identify the reader. Changing the name does not affect any of the reader's other settings or connection. If you change the name of the reader, the new name is used in activity reports for activity at that reader, even if the activity occurred before the name change.



Name: Main entrance

Site: 1st Floor, North

Address: 0

☑ Enabled

!!!WARNING!!!
Before enabling reader, refer to Quick Start Installation Guides/Establishing Communications

Status: ● Connected

Site: This is the site (that is, the group of up to thirty-two readers) that this reader is associated with.

Address: The number here can be from 0 to 254. If the site is connected by IP Network, the first reader in the site (the one with the ethernet card) must be reader 0. Other readers can use any number and do not need to be numbered sequentially. For example, your readers could be numbered 0, 1, 2, 3... or they could be numbered 0, 100, 110, 137.... You can use the same reader number in more than one site. For example, if you have twenty sites, you could have a *Reader One* in each of them.

The number here must match the address entered in the reader; see *Configuring the Physical Reader* on page 54 for more on how to set the address up in the reader.

Even though HandNet allows numbers from 0 to 254, you should never have more than thirty-two readers in a site. While it is sometimes technically possible to connect more than thirty-two readers, not all readers support this, and even for readers that do, connecting more than this causes unacceptably slow response times from readers. The software was not designed to handle more than this, and we cannot guarantee results with more than thirty-two readers. If you feel that more than thirty-two readers in a single site is essential for you, please contact us to discuss your situation first; in nearly all cases, the preferable (and sometimes only) solution is to set up additional site(s).

Enabled: This should be checked once reader setup is done and users should have access through the reader. Leave this unchecked if you do not want HandNet to try to communicate with the reader at this point.

If you have been using readers without HandNet and you want to get the users from the reader, follow these steps BEFORE enabling the site and reader:

1. Pick *Settings* from the *View* menu.

2. Click the *Security* tab.

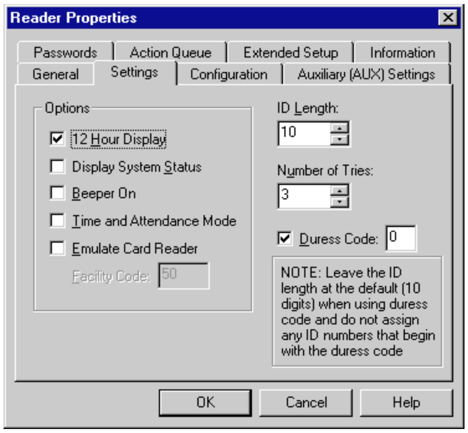
3. Check the box by *Do not delete unauthorized enrollments* (see page 23 for more about what this option does. After you have gotten your users from the reader, you may want to check this box again).

If you enable both the site and the reader without changing this setting, HandNet will regard all of the users in the reader as unauthorized (because they are not in HandNet yet) and it will delete them from the reader. Once it deletes them, there is no way to get them back without adding and enrolling the users again.

Status: This indicates whether the reader is connected.

Settings

This screen controls the reader's display and other factors that affect what happens when the user enter an ID number at the reader.



☑ 12 Hour Display
☐ Display System Status
☐ Beeper On
☐ Time and Attendance Mode
☐ Emulate Card Reader
Facility Code: 50

ID Length: 10
Number of Tries: 3
☑ Duress Code: 0

NOTE: Leave the ID length at the default (10 digits) when using duress code and do not assign any ID numbers that begin with the duress code

12 Hour Display: If you check this, the reader displays times after noon using the numbers one through twelve; if it is not checked, it uses twenty-four hour time. For example, if this is checked 5:00 PM displays on the reader as 5:00; if this is not checked, 5:00 PM displays as 17:00.

Display System Status: Do not check this option unless asked to by one of our support staff. This displays technical information on the reader display about the status of different aspects of the reader. It is not relevant to normal use of the reader.

Beeper On: If this is checked, the reader beeps each time you press a button on it; if this is not checked, the reader does not beep. In a high security setting, you might want the beeps off to make it harder for a casual observer to figure out how many digits are in the ID number. In other contexts, your choice here depends only on your preference; some people like the beeps since it lets them know that they have not missed the button; others prefer not to hear them.

Time and Attendance Mode: Do not check this option. If you check this, the reader asks users for additional information related to time and attendance tracking (whether one is coming in or out or leaving for a job, the job number you are working on, etc.). However, HandNet is currently NOT able to store or track this information.

Emulate Card Reader: If you want the readers to send output directly to a lock and unlock it, leave this unchecked. If you have an access control panel and want the reader to send information formatted like card output to that control panel, check this box.

Facility Code: This only applies if you are emulating a card reader.

ID Length: If all of your user IDs are the same length, you can enter the number of digits here so that users do not have to press *ENTER* or *YES* after typing the ID at the reader. For example, if all of your IDs are four digits long, then you could enter *4* here. Then, at the reader, once the user had entered four digits, the reader would ask the user to place the hand (assuming the ID was valid). Without this, the user would have to type the four digits and then press the *ENTER* or *YES* button on the reader. However, if you use a duress code (see below), do not enter a number here. This is because the duress code adds a digit; if your IDs are four digits, the user will have to be able to enter five digits if they ever need the duress code. If you are using a duress code, leave this set to ten.

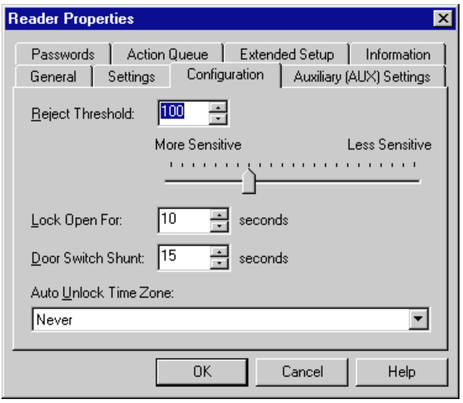
Number of Tries: If a user enters a valid ID number but the users hand does not match the image stored, the reader does not give access. This entry controls how many times the user can try to get access before the reader will block the user's ID and not allow further tries. This prevents someone from making repeated tries to gain access with someone else's ID number. Normally three is a good setting here; it allows for two retries if the user did not place the hand correctly, but limits the number of attempts someone can make.

If the user does not gain access after the number of tries here, the reader no longer accepts that user's ID until another user successfully gains access through that reader.

Duress Code: A duress code is single digit that users can enter before the ID number to indicate that they are in danger or that someone else is forcing them to open the door. For example, suppose that you set zero up as a duress code. If a user is being forced to let someone into the building, instead of entering the regular ID of *1234*, the user would enter *01234*. The system would still grant access as it would for the normal ID, but it would also trigger an alarm. This could be merely the alarm in the HandNet program, or, it could also trigger an external alarm through the *Auxiliary Settings*; see page 49.

Zero (0) is often a good digit for the duress code because you cannot begin a user ID with zero if you enroll users from the command menus on the reader (while HandNet distinguishes between *5* and *0005*, the process of adding a user from the reader command menu does not. This means that if you create a user with an ID of *0005* in HandNet and try to enroll that user with the command menus on the reader, when you type *0005*, the reader would think you were enrolling User Five. This would not correspond with *0005* in HandNet).

Configuration



Reject Threshold: 100

Lock Open For: 10 seconds

Door Switch Shunt: 15 seconds

Auto Unlock Time Zone: Never

This screen controls how closely the typical user's hand must match the image that is stored, how long the door can stay open, and when (if ever) the door should be automatically unlocked.

Reject threshold: The lower this number is, the more closely the user's hand must match the image or template of the hand stored in HandNet. Thirty

(the lowest possible number) requires the hand shape and position to match very closely; two hundred fifty (the highest possible number) will grant access if the hand match is close but not exactly the same. One hundred is good for most contexts; enter a lower number if you have an especially high security situation. You can either enter a number or drag the pointer.

If particular users have trouble placing their hands consistently because of arthritis or some other hand condition, you can override the reader's setting for an individual user on the *Security* tab in the *User Properties*; see page 93.

Lock Open For: This is the number of seconds the door stays unlocked once a user's hand is recognized.

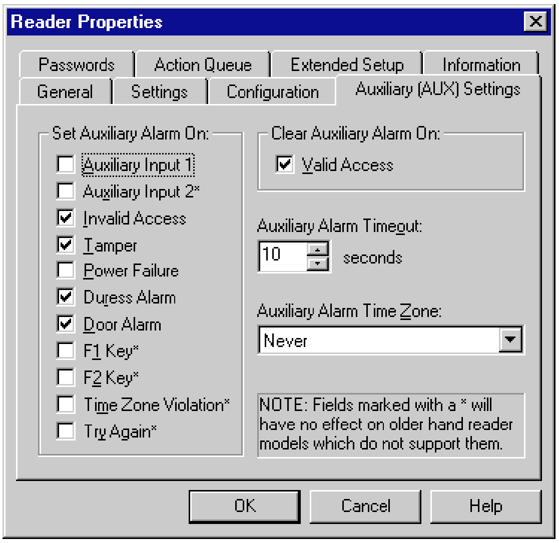
Door Switch Shunt: This is the number of seconds the door can be open before potentially triggering an alarm. The *Alarms* tab in *System Properties* (see page 25) and the *Door Alarm* on the *Auxiliary (AUX) Settings* (see below) and *Extended Settings* (see page 51) tabs control whether this causes an alarm.

Auto Unlock Time Zone: This controls when (if ever) the door is automatically unlocked. For example, you might want a door unlocked during normal business hours, and you might want the door to require hand recognition for access during other hours. You would set up a time zone that reflected the hours you wanted the door open and then pick that time zone here (see page 61 for more on setting up time zones). When you reached the start time, HandNet would unlock the door, and when you reached the end of the time zone, HandNet would lock it again. Leave this set to *Never* if you always want the door locked.

Auxiliary (AUX) Settings

Readers can communicate with auxiliary devices like alarms, lights, or security cameras. HandKey readers can communicate with one auxiliary device; this screen controls when and under what conditions output is sent to that device. HandKey II and HandKey CR readers can communicate with up to three auxiliary devices; this screen controls the output to the first; the *Extended Setup* tab (see page 51) controls output to the second and third.

To get to this screen, click a reader in the right pane of the *Network* window, pick *Properties* from the *Reader* menu, and then click the *Auxiliary (AUX) Settings* tab.



Set Auxiliary Alarm On:

- ☐ Auxiliary Input 1
- ☐ Auxiliary Input 2*
- ☑ Invalid Access
- ☑ Tamper
- ☐ Power Failure
- ☑ Duress Alarm
- ☑ Door Alarm
- ☐ F1 Key*
- ☐ F2 Key*
- ☐ Time Zone Violation*
- ☐ Try Again*

Clear Auxiliary Alarm On:

- ☑ Valid Access

Auxiliary Alarm Timeout: 10 seconds

Auxiliary Alarm Time Zone: Never

NOTE: Fields marked with a * will have no effect on older hand reader models which do not support them.

Set Auxiliary Alarm On: Even though this says *Set Auxiliary Alarm On*, the device does not have to be an alarm; this can trigger any type of auxiliary device. If a condition occurs and the corresponding box is checked, HandNet turns auxiliary output on if it is during the time zone selected at the bottom of the column on the right.

Auxiliary Input 1: This occurs if the reader receives input from an auxiliary input device. This is irrelevant if you do not have an auxiliary input device connected to the reader.

Auxiliary Input 2: This occurs if the reader receives input from the second auxiliary input device (HandKey II and HandKey CR support two auxiliary input devices; HandKey readers support just one). This is irrelevant if you do not have a second auxiliary input device connected to the reader.

Invalid Access: This occurs if someone repeatedly entered a valid ID at a reader, and each time the reader does NOT recognize the user's hand (at the reader, the user would see the message *ID Refused*, and the *Activity* window would show the message *Access Denied*). The number of times that a user can try before this occurs depends on the *Number of Tries* entry on the *Settings* tab in the *Reader Properties*; see page 47. If this occurs, someone might be trying to gain access with someone else's ID.

Tamper: This occurs if someone has shaken the reader roughly or opened the reader. Unless someone was servicing the reader, this message generally warrants further investigation.

Power Failure: This occurs if the reader loses power from an external source. While this could just be due to an ordinary power failure, sometimes someone trying to gain invalid access will cut power in an attempt to disable alarm systems.

Duress Alarm: This occurs if a user entered the duress code. This code indicates that the user is in trouble or that someone is forcing the user to give him/her access; see page 47 for more on setting up a duress code.

Door Alarm: This occurs if the door connected to the reader is forced open, or if the door is kept open for longer than allowed based on the *Door Switch Shunt Time* on the *Configuration* tab in the *Reader Properties*; see page 48.

F1 / F2 Key: This occurs if the corresponding key was pressed on the reader keypad (HandKey II and HandKey CR have F1 and F2 keys to the right of the number keys. The HandKey reader does not have these buttons, what you check here does not make any difference for that type of reader).

Time Zone Violation: This occurs if a user enters a valid ID at a reader, but the user is not authorized to have access during the hours or days of the week based on the time zone associated with the reader in the access profile.

Try Again: This occurs if a user enters a valid ID at a reader, but the reader does not recognize the user's hand (this situation causes the *Identity Unknown* message in the *Activity* window). This could be just the result of incorrect hand placement (if this happens repeatedly, HandNet generates the *Invalid Access* condition above.)

Clear Auxiliary Alarm On: If the auxiliary device is turned on, this controls whether it will be shut off when someone gains valid access (that is, enters a valid ID number and has his/her hand recognized). If this is checked, the alarm (or other auxiliary output) is turned off when a valid user gains access through that reader; if this is not checked, the output continues until the time entered in the following entry ends or until you go to the *Reader* menu, highlight *Auxiliary Output*, and pick *Off*; see page 129.

Auxiliary Alarm Timeout: This indicates the number of seconds that the auxiliary device should be on for.

Auxiliary Alarm Time Zone: This controls when HandNet should turn output to an auxiliary device on. For example, if the auxiliary device is a set of floodlights, it would only help to turn the lights on if the condition occurred at night. To do this, you would create a time zone for night hours, and then assign that time zone here (see page 61 for more on setting up time zones). If this says *Always*, HandNet turns output on for the auxiliary device whenever the checked condition(s) occur.

Passwords

This screen controls the passwords needed to access the menus available through entered command mode on the reader. Generally the passwords below are adequate since a user must be set up with the appropriate authority level on the *Security* tab in *User Properties* (see page 92), and the user must know how to get to these menus in the reader before the passwords below would do any good.

What is available on the different reader menus

1. **Service:** This lets you recalibrate the reader and change the reader's status display.

2. **Setup:** This lets you control reader setup issues including how the reader is connected to your computer network, what language the reader displays in, the date/time, etc.

3. **Management:** This lets you list users.

4. **Enrollment:** This lets you add or remove users.

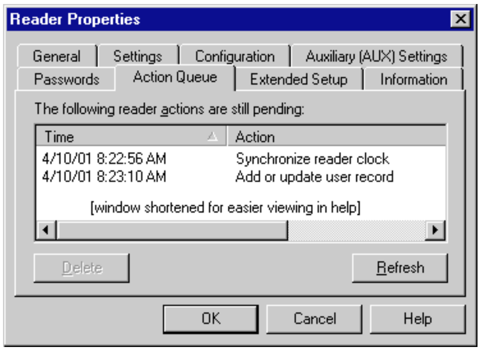
5. **Security:** This lets you control the passwords for the reader menus, change time zones, enroll users who do not need hand access, etc.

For more detail, see the reader manual.

Action Queue

If the reader is not connected to HandNet continuously (typically only the case if HandNet communicates with the reader by modem), this screen lists changes that have not been sent to the reader yet. These actions will be sent to the reader the next time the modem connects.

To get to this screen, click a reader in the right pane of the *Network* window, pick *Properties* from the *Reader* menu, and click the *Action Queue* tab.



The following reader actions are still pending:

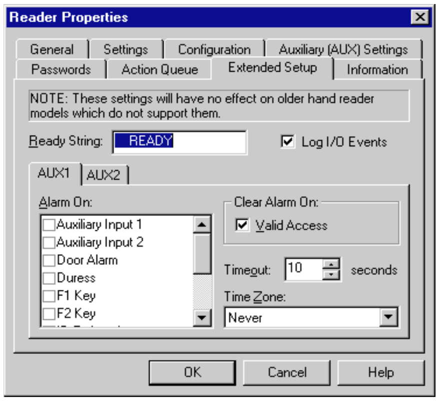
Time	Action
4/10/01 8:22:56 AM	Synchronize reader clock
4/10/01 8:23:10 AM	Add or update user record

[window shortened for easier viewing in help]

If there is been a change that requires that certain actions NOT be sent to the reader, you can select those actions in the list and click *Delete*.

Extended Setup

Readers can turn auxiliary devices like alarms, lights, or security cameras on or off. HandKey II and HandKey CR readers can communicate with up to three auxiliary devices; this screen controls the output to the second and third auxiliary devices; the *Auxiliary (AUX) Settings* tab controls output to the first; see page 48. If you have a HandKey (instead of a HandKey II or HandKey CR), this screen does not apply since the HandKey only supports one auxiliary device.



NOTE: These settings will have no effect on older hand reader models which do not support them.

Ready String: READY

☑ Log I/O Events

Alarm On:
□ Auxiliary Input 1
□ Auxiliary Input 2
□ Door Alarm
□ Duress
□ F1 Key
□ F2 Key

Clear Alarm On:
☑ Valid Access

Timeout: 10 seconds

Time Zone: Never

Ready String: This is the text that appears in the reader display when the reader is ready and waiting for the user to enter an ID. For example, if you want the readers to read *Enter ID* instead of *Ready* you could change the text here. You can enter up to fourteen characters. If you want this text centered in the reader's display, add spaces before the text if needed.

Log I/O Events: This entry only applies to the HandPunch. We do not recommend connecting a HandPunch to HandNet. The HandPunch is used for tracking time and attendance, which is not what HandNet is for. If you do connect a HandPunch and this box is checked, the reader records all activity (including invalid access attempts, door alarms, accessing command mode on the reader, etc.); if you do not have this checked, the HandPunch only records successful accesses. If you have an ID3D HandKey, HandKey II, or HandKey CR, the reader records all activity regardless of whether this is checked or not.

AUX1/AUX2

Aux1 contains the settings for the second auxiliary device that can be connected to a HandKey II or HandKey CR reader; *Aux2* contains the settings for the third (the settings for the first are on the *Auxiliary (AUX) Settings* tab; see page 48).

Alarm On: Even though this says *Alarm On*, the device does not have to be an alarm; this could trigger any type of auxiliary device. If a condition occurs and the corresponding box is checked, HandNet turns auxiliary output on if it is during the time zone selected at the bottom of the column on the right.

Auxiliary Input 1: This occurs if the reader receives input from an auxiliary input device. This is irrelevant if you do not have an auxiliary input device connected to the reader.

Auxiliary Input 2: This occurs if the reader receives input from the second auxiliary input device (HandKey II and HandKey CR support two auxiliary input devices; HandKey readers support just one). This is irrelevant if you do not have a second auxiliary input device connected to the reader.

Door Alarm: This occurs if the door connected to the reader is forced open, or if the door is kept open for longer than allowed based on the *Door Switch Shunt Time* on the *Configuration* tab in the *Reader Properties*; see page 48.

Duress Alarm: This occurs if a user entered the duress code. This code indicates that the user is in trouble or that someone is forcing the user to give him/her access; see page 47 for more on setting up a duress code.

F1 / F2 Key: This occurs if the corresponding key was pressed on the reader keypad (HandKey II and HandKey CR have F1 and F2 keys to the right of the number keys. The HandKey reader does not have these buttons, what you check here does not make any difference for that type of reader).

Invalid Access: This occurs if someone repeatedly entered a valid ID at a reader, and each time the reader does NOT recognize the user's hand (at the reader, the user would see the message *ID Refused*, and the *Activity* window would show the message *Access Denied*). The number of times that a user can try before this occurs depends on the *Number of Tries* entry on the *Settings* tab in the *Reader Properties*. If this occurs, someone might be trying to gain access with someone else's ID.

Power Failure: This occurs if the reader loses power from an external source. While this could just be due to an ordinary power failure, sometimes someone trying to gain invalid access will cut power in an attempt to disable alarm systems.

Tamper: This occurs if someone has shaken the reader roughly or opened the reader. Unless someone was servicing the reader, this message generally warrants further investigation.

Time Zone Violation: This occurs if a user enters a valid ID at a reader, but the user is not authorized to have access during the hours or days of the week based on the time zone associated with the reader in the access profile.

Try Again: This occurs if a user enters a valid ID at a reader, but the reader does not recognize the user's hand. This could be just the result of incorrect hand placement (if someone repeatedly entered a valid ID at a reader, and each time the reader does NOT recognize the user's hand, this would generate the *Invalid Access* condition above).

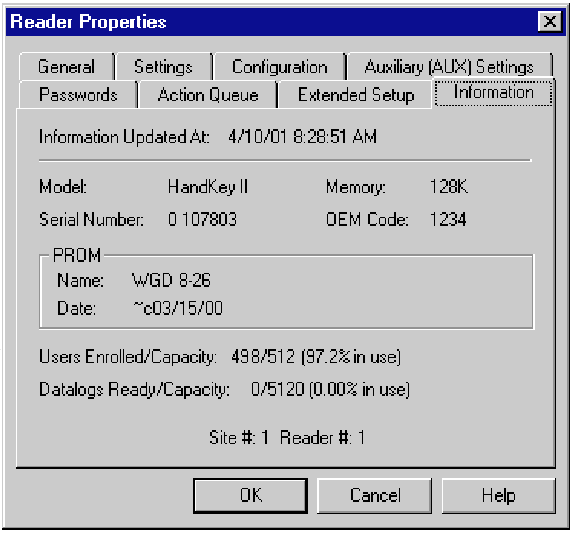
Clear Auxiliary Alarm On: If the auxiliary device is turned on, this controls whether it will be shut off when someone gains valid access (that is, enters a valid ID number and has his/her hand recognized). If this is checked, the alarm (or other auxiliary output) is turned off when a valid user gains access through that reader; if this is not checked, the output continues until the time entered in the following entry ends or until you go to the *Reader* menu, highlight *Auxiliary Output*, and pick *Off*; see page 129.

Timeout: This indicates the number of seconds that the auxiliary device should be on for.

Time Zone: This controls when HandNet should turn output to an auxiliary device on. For example, if the auxiliary device are a set of floodlights, it would only help to turn the lights on if the condition occurred at night. To do this, you would create a time zone for night hours, and then assign that time zone here (see page 61 for more on setting up time zones). If this says *Always*, HandNet turns output on for the auxiliary device whenever the checked condition(s) occur.

Information

This screen contains information about the reader. A key piece of information on this screen is the *Users Enrolled/Capacity:* this reflects the amount of available space in the reader. For example, the screen below reflects a reader with 498 users and space for up to 512 users. You could only add fourteen more users before this reader reached its limit. If you were approaching this limit, you would want to consider a memory upgrade for the reader so it would have space for additional users.



Information Updated At: 4/10/01 8:28:51 AM

Model: HandKey II
Memory: 128K
Serial Number: 0 107803
OEM Code: 1234

PROM
Name: WGD 8-26
Date: ~c03/15/00

Users Enrolled/Capacity: 498/512 (97.2% in use)
Datalogs Ready/Capacity: 0/5120 (0.00% in use)

Site #: 1 Reader #: 1

Most of the other information on this screen is helpful if your reader needs service, but not relevant to the ongoing use of the reader.

To get to this screen, click a reader in the right pane of the *Network* window, pick *Properties* from the *Reader* menu, and then click the *Information* tab.

* * * * *

Configuring the Physical Reader

While most of the information in the reader is controlled through HandNet, you must initially set up certain settings in the reader so it can communicate with HandNet. You do this through the command menus on the reader.

For readers with a network (ethernet) card: The IP address in this reader must match the *IP address on the Connection* tab in *Site Properties*; see page 39.

For a reader connected by serial port or connected as part of a chain of readers: The address in the reader must match the address on the *General* tab in *Reader Properties*; see page 45. The serial settings must also be correct, and the baud rate must match the baud rate on the *Connection* tab in *Site Properties*; see page 35.

We do not recommend changing any other settings through the reader command menus. All other settings can be controlled through *Reader Properties* in HandNet; see page 45 (if you were to make other changes directly in the reader, these would be overridden by the settings in HandNet when you enabled the reader).

Getting to the Setup Menu in the Reader

1. Enter command mode on the reader:

   If you have a HandKey II or HandKey CR reader: Press *CLEAR*, and then press *ENTER*.

   If you have an ID3D HandKey reader: Press *#* AND *** (you can press them at the same time, or one after the other).

If you have not used the reader with HandNet before, or if you have used it with HandNet and cleared its memory, the display looks like this.

```
ENTER PASSWORD
```

Type the password for the setup menu and press *ENTER* or *#.* If you have not changed it, the password is two (2).

If you have previously used the reader with HandNet and are reconfiguring it for another site or location, you may see:

```
READY:
*:
```

If the display looks like this, type your user ID and press *ENTER* or *#*. The reader will ask you to place your hand. Once you place it, you should then see the *Enter Password* display shown above. Type the password for the *Setup* menu and press *ENTER* or *#*. If you have not changed it, the password is two (2).

Changing the Reader Address

You must set the address in readers that are connected to the computer by a serial cable, and in readers that are connected to another reader (that is, readers that are not the first reader in the site). You cannot change the address in a reader that has an ethernet card; these readers automatically have an address of zero (0).

The following steps are specific to the HandKey II and CR; the menus are slightly different in other readers. Please see the manual that came with the reader if you are not sure how to find the correspond settings in your reader.

1. If you have not already done so, follow the steps on page 54 for getting to the reader setup menu.
2. Press the ** / NO* button until the display looks like this:

```
SET ADDRESS
*  NO     YES #
```

3. Press the *# / YES* button. The display will look like this:

```
RDR ADD ID 1
NEW?:
```

4. Type the new address. The address you enter must match the address on the *General* tab in *Reader Properties*; see page 45. Press *YES* or *ENTER*. The display returns to:

```
SET ADDRESS
*  NO     YES #
```

5. If you are done changing settings, press *CLEAR* to leave the *Reader Command* menu. If you need to change others settings, press *NO* until you get to the next setting you need to change.

Changing the Serial Settings and Baud Rate

You must have appropriate serial settings and baud rate in readers that are connected to the computer by a serial cable, and in readers that are connected to another reader (that is, readers that are not the first reader in the site). These settings do not apply to a reader with an ethernet card.

The following steps are specific to the HandKey II and CR; the menus are slightly different in other readers. Please see the manual that came with the reader if you are not sure how to find the correspond settings in your reader.

1. If you have not already done so, follow the steps on page 54 for getting to the reader setup menu.

2. Press the *NO* button until the display looks like this:

```
 SET SERIAL
* NO    YES #
```

3. Press the *YES* button. The display will look like this:

```
SET RS-485/422?
 * NO    YES #
```

4. Typically you will answer *YES* here. The display now asks for the baud rate. The baud rate here must match the rate on the *Connection* tab in *Site Properties*. Generally 9600 is appropriate.

   If you have a HandKey II or HandKey CR:

   The display will show the baud rate:

```
SET RS-485/422?
 * NO    YES #
```

   To accept the rate shown and continue, press *YES*. To change the rate, press *NO* to cycle through the choices until you find the one you want.

   If you have an ID3D HandKey: The baud rate is represented by a code:

baud rate	code	baud rate	code
38.4K	0	2400	4
19.2	1	1200	5
9600	2	600	6
4800	3	300	7

   For example, for 9600, you would enter the code of two (2).

5. The reader will display:

```
 SET RS-232?
* NO    YES #
```

Unless you have a printer connected directly to the reader, you would typically answer *NO* here. If you have a printer directly connected to this reader, answer *YES* (most users working with HandNet print from HandNet rather than connecting a printer directly to the reader). The only other time you might say *YES* here was if you had a single reader connected directly to HandNet with a serial port; there is a way to wire the connection to use RS-232 (if this were the case, you would say *YES*, pick the appropriate baud rate, and then indicate that RS-232 was connected to 1-Host (that is, HandNet)).

6. Once you are done, you see the *Set Serial* display again:

```
  SET SERIAL
*  NO     YES #
```

7. Press *CLEAR* to leave the command menu.

Changing the IP Address in a Reader with an Ethernet Card

You must set the IP address in a reader with an ethernet card. Before you do this, get the appropriate IP address and gateway (if needed) from your network administrator. If you have a WAN (wide area network), you also need the subnet mask; only certain subnet masks are supported; see the table below.

1. If you have not already done so, follow the steps on page 54 for getting to the reader setup menu.

2. Press the *NO* button until the display looks like this:

   SET SERIAL
   *** NO YES #**

3. Press the *YES* button. The display will look like this:

   IP ADDRESS
   000.000.000.000

   If the display says *Set RS-485/422?* at this point, the reader does NOT have a network card. Contact your dealer if you need to get one.

4. Quickly type the correct address; if you pause for more than about four seconds while entering the IP address, the reader advances to the next display without saving your change. The address will have four parts separated by periods. Enter each part as three digits; if one part has less that four digits, add zeros before that part of the number to make it three digits. You do not have to enter the periods. For example, if your administrator gave you the address 192.9.210.10, you would enter:

   192 009 210 010

   This address must match the IP address on the *Connection* tab in *Site Properties*; see page 39. Press *YES* or *ENTER*. The display will now look like this:

   GATEWAY
   000.000.000.000

5. If your network administrator has told you to enter a gateway, do so; otherwise press *YES* or *ENTER*. As with the IP address, if you change this, you must type fairly quickly; if you pause for more than about four seconds while entering the gateway, the reader advances to the next display without saving your change. Once press *ENTER*, you see:

   HOST BITS: 0
   NEW?

6. If you are communicating over a LAN (local area network), type zero (0) for the Host Bits and press *YES* or *ENTER*. If you have a WAN, enter the number from the table below that corresponds to your subnet mask (only the subnet masks listed are currently supported). If you are not sure, check with your network administrator.

For this subnet mask:	Enter this for the host bits:	For this subnet mask:	Enter this for the host bits:
255.255.255.255	0	255.255.224.0	13
255.255.255.254	1	255.255.192.0	14
255.255.255.252	2	255.255.128.0	15
255.255.255.248	3	255.255.0.0	16
255.255.255.240	4	255.254.0.0	17
255.255.255.224	5	255.252.0.0	18
255.255.255.192	6	255.248.0.0	19
255.255.255.128	7	255.240.0.0	20
255.255.255.0	8	255.224.0.0	21
255.255.254.0	9	255.192.0.0	22
255.255.252.0	10	255.128.0.0	23
255.255.248.0	11	255.0.0.0	24
255.255.240.0	12		

7. The reader will display:

```
  9600 BAUD
* NO     YES #
```

The speed you choose should match the baud rate you are setting in the rest of the readers in this site. Generally 9600 is appropriate. To accept the rate shown and continue, press *YES*. To change the rate, press *NO* to cycle through the choices until you find the one you want.

Once you press *YES*, the reader display returns to:

```
  SET SERIAL
*  NO     YES #
```

8. If you missed one of the settings because the reader display changed too quickly for you, press *YES* to go through the settings again. If you are done changing settings, press *CLEAR* to leave the command menus.

9. If you need the changes to take effect immediately, disconnect the power from the reader, wait a few seconds, and then connect the power again. This resets the reader. If you do not do this, it may take up to six minutes for the changes to take effect.

* * * * *

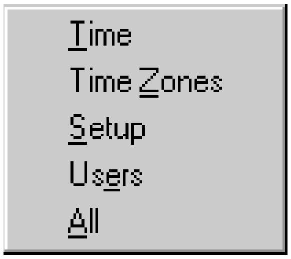
Resending Information to a Reader

Why You Might Need to Resend Information

While HandNet automatically sends the appropriate information to readers, occasionally you will need to use this when correcting a problem with a reader. You can do this with *Download* on the *Reader* menu.

Getting to the Download Option

To do this, select one or more readers, and go to the *Reader* menu, click *Download*, and then click the type of information to send.



Time: This sends the current time from the computer to the selected reader(s). You typically only need to use this option if the time changed (for example, for Daylight Savings Time). You can select all of your readers and send the time to all of them at once, or you can select specific readers.

Time Zones: This sends time zone and holiday information to the selected reader(s). You need to download this information if you change *Time Zones* (page 61) or *Holidays* (see page 65).

Setup: This sends configuration information to the selected readers. In most cases this is done automatically.

Users: After adding users, you need to download them to the hand readers so the readers will recognize the new users. This sends all current users to the selected readers.

All: This sends *Time, Time Zones, Setup*, and *User* information to the selected reader(s). You would use this when you set up a new reader so the reader had all the needed information.

Confirming That You Want to Send Information to the Reader

Whenever you choose to download information to readers, HandNet asks you to confirm that you want to download to the selected reader. Click *YES* to continue.

* * * * *

Settings That Control User Access

Setting Up Time Zones

What Time Zones Are

Time zones are periods of time on different days of the week when users can have access. There is no connection between what we call time zones in HandNet and the time zones we usually think of that have to do with different times around the world. This does not have anything to do with Eastern, Central, Mountain, or Pacific time; it only has to do with controlling which hours of the day access is available through readers.

When You Need to Set Up Time Zones

If you want some users to be able to use certain readers only during certain hours or on certain days of the week, time zones let you identify when access is available. For example, suppose some users should only be able to gain access through certain readers between 8:00 AM and 5:00 PM, Monday through Friday. You would create a time zone that identified these times and days, associate that time zone with appropriate readers using an access profile, and then assign that access profile to the users. After you did this, users with that access profile would only have access during the times you identified in the time zone.

You can also use time zones to determine when certain doors should be automatically unlocked; see *Automatically Unlocking a Door on a Scheduled Basis* on page 128.

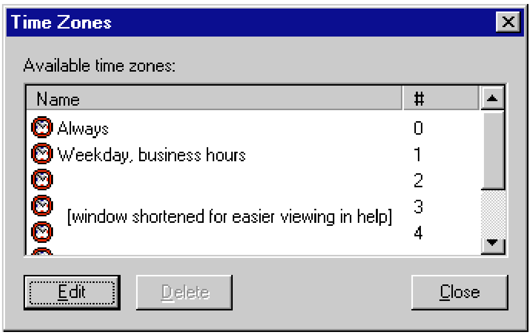
If users should have different access on holidays than on other days, you can set different hours for holidays in the time zone. You will have to also set up holidays; see page 65.

When You Do not Need to Set Up Time Zones

If you do not need to limit access by day or time (that is, if users could use the readers twenty-four hours a day, seven days a week if they wanted), and if you do not want doors to unlock automatically, you do not need to set up time zones.

Getting to the List of Time Zones

1. Click the *View* menu.
2. Click *Time Zones*. You see a screen like the one below (though the time zones listed will be different). From here you can add, change, or delete time zones.



Name	#
Always	0
Weekday, business hours	1
	2
[window shortened for easier viewing in help]	3
	4

Adding or Changing Time Zones

The first time zone is *Always* and the last (#61) is *Never*; you cannot change either of these.

To add a time zone, click one of the blank lines in the time zone list and click *Edit*. To change a time zone, click the time zone to change and click *Edit*. Change the *Time Zone Definition* screen (see below) as needed and then click OK to return to this list. You can then add or change another or click *Close* when done.

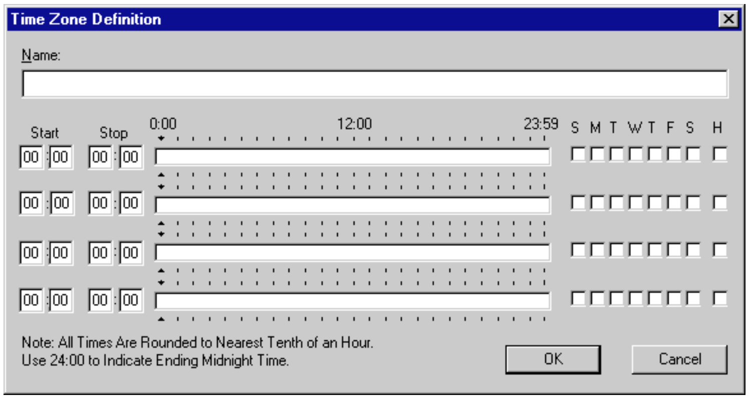
Deleting Time Zones

Click the time zone and click *Delete*. The program asks if you are sure you want to delete the time zone. Click *Yes*.

If you try to delete a time zone and get a message that the time zone is used in an access profile, you must close the time zone window, go to access profiles and select a different time zone for each reader that had this time zone selected if you still want to delete it.

Time Zone Definition Screen

This screen determines what hours access is available on different days of the week. A time zone is active if the time is equal to or after the start time and before the stop time, and if the day of the week matches one of those checked.



Start	Stop	S	M	T	W	T	F	S	H
00 : 00	00 : 00	□	□	□	□	□	□	□	□
00 : 00	00 : 00	□	□	□	□	□	□	□	□
00 : 00	00 : 00	□	□	□	□	□	□	□	□
00 : 00	00 : 00	□	□	□	□	□	□	□	□

Note: All Times Are Rounded to Nearest Tenth of an Hour.
Use 24:00 to Indicate Ending Midnight Time.

Name: Enter a name that will be clear to you so that when you associate the time zone with a reader in an access profile, you will be sure to pick the right one.

You can assign four different periods in each time zone if you need them; for example, if you want to give access during different hours on different days. Be sure to leave lines that you do not need blank.

Start/Stop Times: Enter hours after noon using military time. Use the chart below or see the examples if you need help. Times are divided into tenths of an hour, so HandNet rounds minutes to the nearest six minute interval. For example, if you enter 8:02, the program rounds this to 8:00; if you enter 8:03, the program rounds it to 8:06.

	Enter on the Time Zone screen		Enter on the Time Zone screen
noon	12:00	**7:00 PM**	19:00
1:00 PM	13:00	**8:00 PM**	20:00
2:00 PM	14:00	**9:00 PM**	21:00
3:00 PM	15:00	**10:00 PM**	22:00
4:00 PM	16:00	**11:00 PM**	23:00
5:00 PM	17:00	**midnight**	00:00 if a start time; 24:00 if a stop time
6:00 PM	18:00		

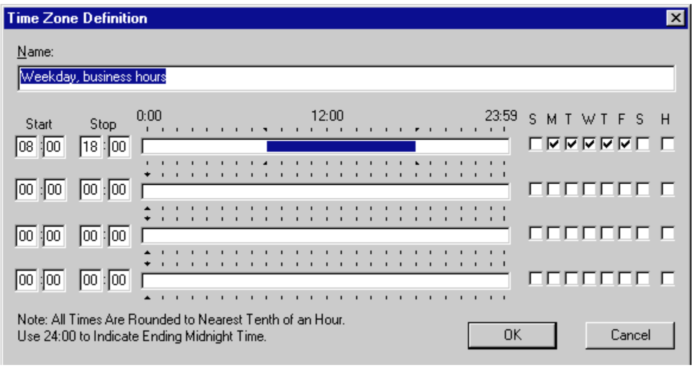
If a time zone must cross midnight (for example, if you want to give access between 8:00 PM and 4:00 AM), you must use two lines to create that access time. The first line would give access from 20:00 to 24:00 (that is, 8:00 PM to midnight), and the next line would give access on the same days of the week from 0:00 to 4:00 (that is, midnight to 4:00 AM). See the third example on the following page.

Days of the Week: Check the boxes for each of the day of the week that access should be available. The letters over the boxes correspond to the days of the week (Sunday through Saturday); H stands for holiday. If access is different on holidays than on other days, you must also set up holidays; see page 65. See the examples on the following page.

Click *OK* when done.

Examples of Time Zone Settings

These settings give access between 8:00 AM and 6:00 PM, Monday through Friday. They do not give any access on Saturday, Sunday, or Holidays. The blue bar in the center section of the screen shows when access is available.

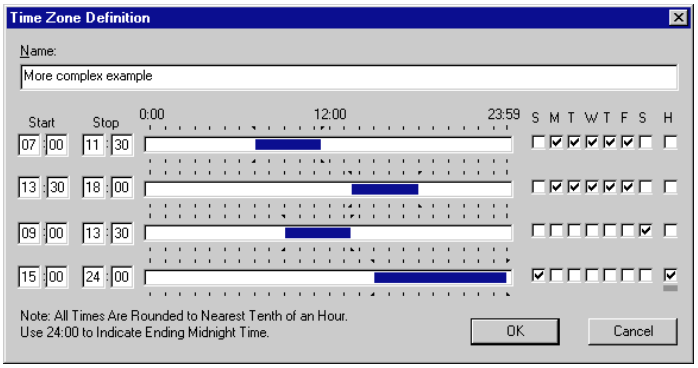


Name: Weekday, business hours

Start	Stop	S	M	T	W	T	F	S	H
08 : 00	18 : 00	□	☑	☑	☑	☑	☑	□	□
00 : 00	00 : 00	□	□	□	□	□	□	□	□
00 : 00	00 : 00	□	□	□	□	□	□	□	□
00 : 00	00 : 00	□	□	□	□	□	□	□	□

Note: All Times Are Rounded to Nearest Tenth of an Hour.
Use 24:00 to Indicate Ending Midnight Time.

The following settings give access from 7:00 to 11:30 in the morning on weekdays, from 1:30 in the afternoon to 6:00 PM also on weekdays, from 9:00 in the morning to 1:30 in the afternoon on Saturdays, and from 5:00 PM to midnight on Sundays and holidays.

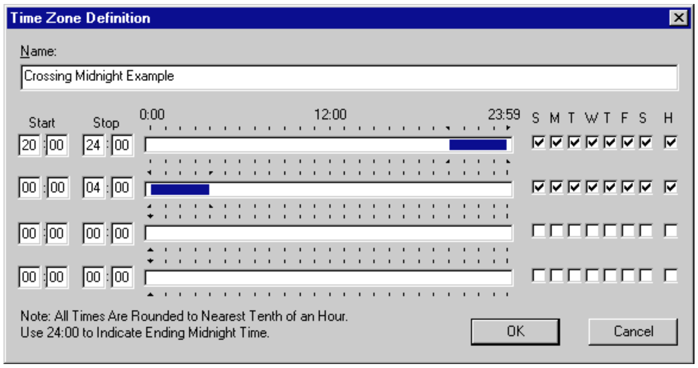


Name: More complex example

Start	Stop	S	M	T	W	T	F	S	H
07 : 00	11 : 30	□	☑	☑	☑	☑	☑	□	□
13 : 30	18 : 00	□	☑	☑	☑	☑	☑	□	□
09 : 00	13 : 30	□	□	□	□	□	□	☑	□
15 : 00	24 : 00	☑	□	□	□	□	□	□	☑

Note: All Times Are Rounded to Nearest Tenth of an Hour.
Use 24:00 to Indicate Ending Midnight Time.

The following settings show how to cross midnight. This gives access from 8:00 PM through 4:00 AM any day of the week. Notice that this requires two lines to set up: the first going from 8:00 PM to midnight, and the next going from midnight to 4:00 AM.



Name: Crossing Midnight Example

Start	Stop	S	M	T	W	T	F	S	H
20 : 00	24 : 00	☑	☑	☑	☑	☑	☑	☑	☑
00 : 00	04 : 00	☑	☑	☑	☑	☑	☑	☑	☑
00 : 00	00 : 00	□	□	□	□	□	□	□	□
00 : 00	00 : 00	□	□	□	□	□	□	□	□

Note: All Times Are Rounded to Nearest Tenth of an Hour.
Use 24:00 to Indicate Ending Midnight Time.

* * * * *

Setting Up Holidays

When You Need to Set Up Holidays

If you want to prevent access on holidays or to give different access on holidays than on other days, the holidays list identifies when those holidays are. When you reach a holiday in the list, HandNet applies the holiday access times instead of the regular access times (if you set holidays up, you will also have to set up time zones to indicate what access users should have on different days; see page 61 for more on setting up time zones).

When You Do not Need to Set Up Holidays

If you do not give different access on holidays than on other days, you do not need to set up any holidays.

Adjusting Holidays Each Year

If you set holidays up, remember to return to the holidays setup at the beginning of each year to adjust each holiday that is celebrated on a different date than the previous year. For example, Thanksgiving, Memorial Day, and Labor Day are on different dates each year. Also, while holidays like Christmas and New Year's are always on the same date, when these holidays fall on a weekend, the day they are taken off is sometimes on a different date.

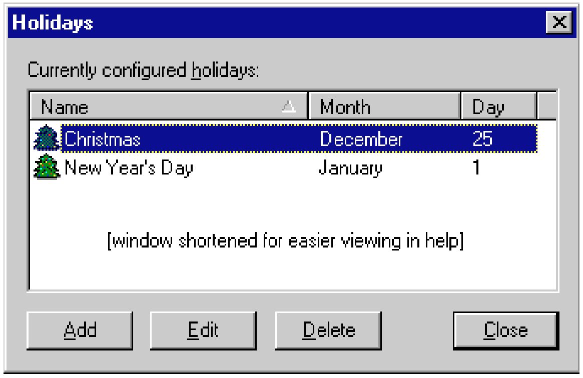
Getting to the Holidays List

1. Click *View* from the *Main Menu* bar.

2. Click *Holidays*. You see a list like this one below. From here you can add, change, or delete holidays.

Adding or Changing Holidays

To add a holiday, click *Add*; to change a holiday, click the holiday in the list and then click *Edit*. When you add or edit, you see this screen:



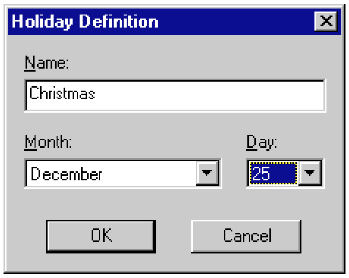
Currently configured holidays:

Name	Month	Day
Christmas	December	25
New Year's Day	January	1

[window shortened for easier viewing in help]

Name: Enter a name to help you identify the holiday.

Month: Click this entry and pick the month from the list (you could also press *TAB* from the *Name* entry and then type the first letter of the month. If more than one month begins with the same letter, typing that letter cycles through those months).



Name: Christmas

Month: December

Day: 25

Day: Click this entry and pick the day from the list (you could also press *TAB* from the *Month* entry and then type the first digit. For example, if you want to get to twenty-five, you would type two (2) several times. The first time you type two (2), the date would show *2*; when you type two (2) a second time, you would see *20*; typing two again would switch to *21*; you would repeat this until you got to the number you need).

Click *OK* when each entry is correct.

Deleting Holidays

To delete a holiday: Click the holiday in the list and click *Delete*.

* * * * *

Setting Up Access Profiles

When You Need to Set Up Access Profiles

If some users can only use certain hand readers and/or only use them at certain times or on certain days, access profiles define when each type of user can use each reader. For example, suppose your maintenance staff should have access to the maintenance rooms seven days a week, your office staff should have access to the office but only during business hours, and your supervisors should have access to everything at any time. You would create three access profiles: one for supervisors, one for office staff, and one for maintenance personnel. These profiles would identify which readers each group could use. In these profiles you would also identify which time periods each group could use each reader (you would set up these time periods first using *Time Zones*). After creating these different profiles, whenever you added a user, you would just identify which group the user was a part of, and the access profile for that group would automatically give the appropriate access.

To limit access to certain days or times, you must set up time zones before creating access profiles; see page 61 for more on setting up time zones.

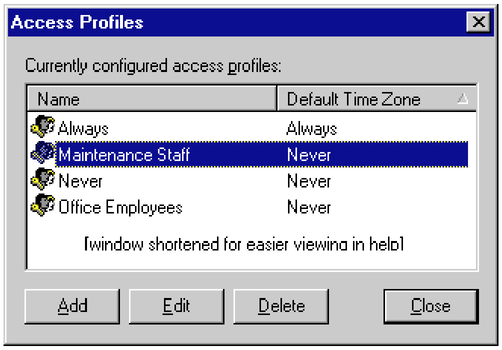
When You Do Not Need to Set Up Access Profiles

If you want all users to be able to use every reader any time, you do not need to set up access profiles. HandNet comes set up with an *Always* profile that lets users use any reader in the system twenty-four hours per day, seven days per week (it also has a *Never* profile that does not let the user verify at any reader at any time).

Getting to the List of Access Profiles

1. Click the *View* menu from the main menu bar.

2. Click *Access Profiles*. You see a screen like the one below (though the profiles listed will be different). From here you can add, change, or delete access profiles.



Currently configured access profiles:

Name	Default Time Zone
Always	Always
Maintenance Staff	Never
Never	Never
Office Employees	Never

[window shortened for easier viewing in help]

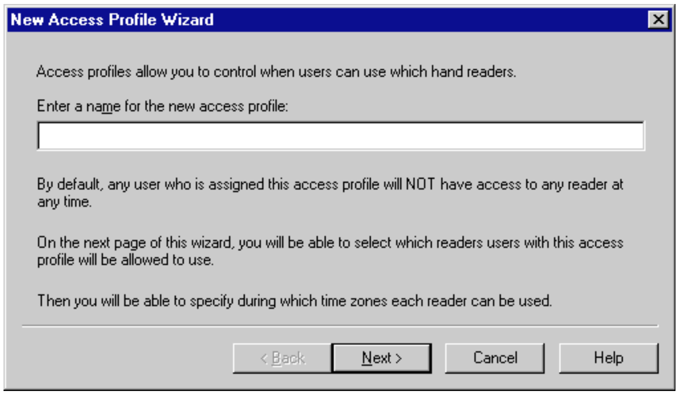
The *Default Time Zone* shown on this list does NOT reflect the time zones associated with the readers in this profile; it only reflects the time zone that HandNet initially picks if you associate another reader with this profile. Except for the *Always* profile, this column always says *Never*.

Adding an Access Profile

Click the *Add* button to add an access profile. This starts the *New Access Profile Wizard*.

New Access Profile Wizard, Screen 1

You see the *New Access Profile Wizard* when you add a new access profile to the list of access profiles.



Access profiles allow you to control when users can use which hand readers.

Enter a name for the new access profile:

By default, any user who is assigned this access profile will NOT have access to any reader at any time.

On the next page of this wizard, you will be able to select which readers users with this access profile will be allowed to use.

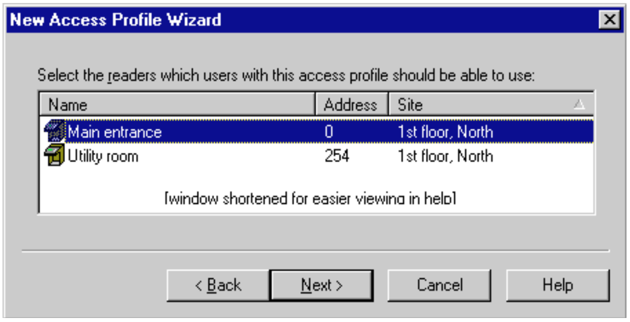
Then you will be able to specify during which time zones each reader can be used.

Name: Enter a name that describes the group of users that this access profile will be used for. For example, if this profile gives access that is appropriate for all of your maintenance staff, you could use that for the name. The important thing is for the name to be clear so that you do not give inappropriate access to users.

Click the *Next* button to go to the next screen.

New Access Profile Wizard, Screen 2

The second screen in the *New Access Profile Wizard* lists all of your readers (typically you will have many more than the two shown in the example below). Select each reader that you want to give access to with this profile, and then click *Next*.



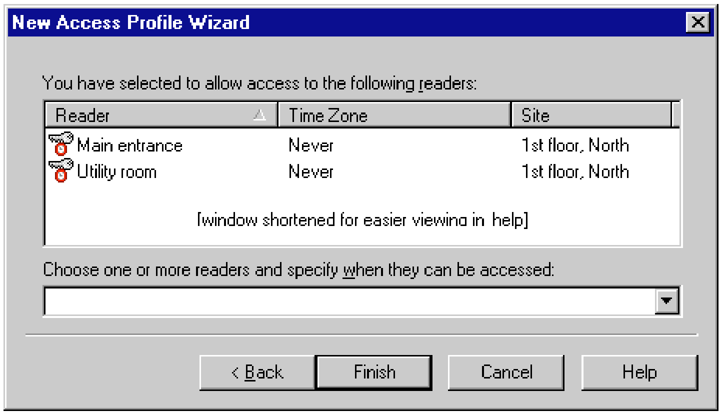
Select the readers which users with this access profile should be able to use:

Name	Address	Site
Main entrance	0	1st floor, North
Utility room	254	1st floor, North

[window shortened for easier viewing in help]

New Access Profile Wizard, Screen 3

The third and final *New Access Profile Wizard* screen shows all of the readers that you selected on the previous screen (if you discover that you missed a reader on the previous screen, click the *Back* button to return to the list of all readers and select it there).



You have selected to allow access to the following readers:

Reader	Time Zone	Site
Main entrance	Never	1st floor, North
Utility room	Never	1st floor, North

[window shortened for easier viewing in help]

Choose one or more readers and specify when they can be accessed:

When you come to this screen, each reader has a time zone of *Never*; you must change the time zone for each reader to give access to that reader through this profile.

To associate time zones with the readers:

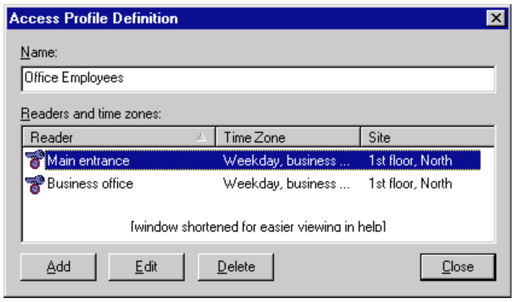
1. Select one or more readers on the list. If you forget to select readers, HandNet still lets you do the following step but it will not have any effect.

2. Click on the entry under *Choose one or more readers...* and select a time zone there. HandNet uses that time zone for each selected reader.

If you need to associate a different time zone with some readers, repeat these steps until you have specified a time zone for each reader. For example, suppose you were creating an access profile for maintenance workers, and suppose these workers had access to building entrances and maintenance facilities twenty-four hours a day, but they only had access to the business offices during normal business hours. You would select the entrance and maintenance readers and associate a time zone of *Always* with them. You would then select the business office readers and associate your normal business hours time zone with those readers.

Changing an Access Profile

To change an access profile, click it on the list and then click the *Edit* button. That brings up a list of readers that have been associated with the profile. The list looks like this:


Access Profile Definition

Name: Office Employees

Readers and time zones:

Reader	Time Zone	Site
Main entrance	Weekday, business ...	1st floor, North
Business office	Weekday, business ...	1st floor, North

[window shortened for easier viewing in help]

To add another reader to those associated with this profile: Click the *Add* button to bring up the *Access Profile Override* box (shown on the following page). Complete the entries there and click *OK*.

To change the time zone a reader is accessible with this profile: Click the reader in the list and click *Edit* to bring up the *Access Profile Override* box. Click the *Time Zone* entry, select the appropriate time zone, and then click *OK*.

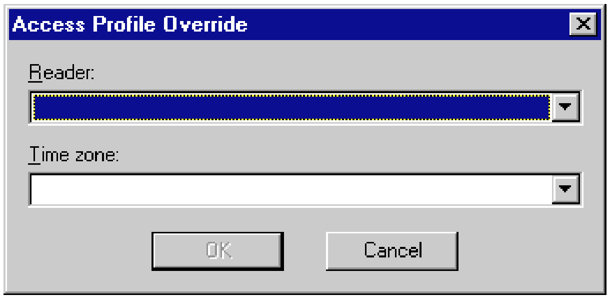
To change the time zone for several readers at once: Hold the *CTRL* key down and click each reader that you want to change the time zone. When all the appropriate readers are selected, click *Edit*. This brings up the *Access Profile Override* box but you can only change the *Time Zone* entry. Click the *Time Zone* entry, select the appropriate time zone, and then click *OK*.

To remove one or more readers from this access profile: Select the reader(s) in the list and click *Delete*.

Click *Close* to return to the list of profiles.

Access Profile Override Box

You see this same screen whether you are adding a reader to a profile or editing a reader that you have added previously (when adding the entries are initially blank; when editing, the entries are filled in with your previous choices).



Reader: Click this to choose a reader that should be associated with this profile. This only lists readers that have not already been added to this profile. If you click this and an empty pick box comes up, then you have already added all readers to this profile. This entry is disabled if you are changing several readers at once.

Time Zone: Click this and pick the time zone that the users with this profile should have access to the selected reader(s). If you have selected several readers, this changes all of them at once.

Click *OK* to return to the list of readers in this profile.

Deleting an Access Profile

To delete an access profile, click the profile on the list and click the *Delete* button. HandNet does not ask you to confirm the deletion, so make sure you pick the right one.

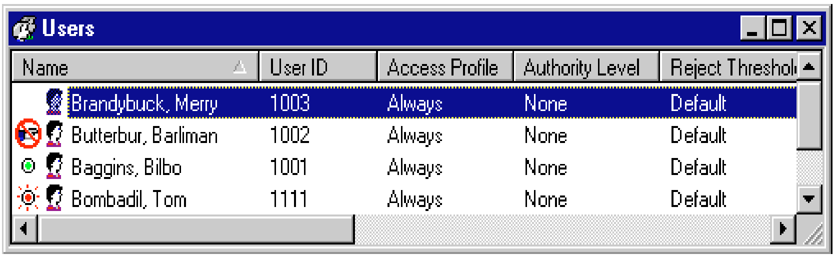
If you get a message that the access profile you are trying to delete is still assigned to a user, go to the list of users, double-click the user to go to the *User Properties*, click the *Security* tab, and select a different access profile for the user there. The message only lists the last user that the profile was assigned to, so there may be other users that also use the profile. Check the list of users to see if any other users use that profile (click the heading of the profile column in the user list to sort by profile; that will put all users with each profile together). If you find any other users using the profile you want to delete, select a different profile for each of them as well. Once no users are using the profile, you can return to this option and delete the profile.

* * * * *

Adding and Maintaining Users

Users Window

The users window lists every user that is in HandNet. To open this window, pick *Users* from the *View* menu or press *CTRL-U*.



Name	User ID	Access Profile	Authority Level	Reject Threshol
Brandybuck, Merry	1003	Always	None	Default
🚫 Butterbur, Barliman	1002	Always	None	Default
🟢 Baggins, Bilbo	1001	Always	None	Default
🔴 Bombadil, Tom	1111	Always	None	Default

Understanding the Icons to the Left of the Name

	No icon indicates that the user is enrolled able to use any readers permitted by the access profile.
🚫	The no access icon indicates that the user is not enrolled yet and hence will not have access to any readers. You must enroll the user to give access; see page 87.
🟢	The green light indicates that the user currently has access, and that the limited access feature was used to so this access will automatically expire at some point; see page 93 for more about limited access.
●	The black dot indicates that the limited access feature was used to set a begin and end date/time for this user’s access, and the user does NOT have access because the access period has not started yet; see page 93 for more about limited access.
🔴	The red light indicates that the limited access feature was used to set a begin and end date/time for this user’s access, and the user does NOT have access because the access period has ended; see page 93 for more about limited access.

Changing How the User List is Sorted

You can sort the list of users using the information in any column by clicking on the column heading. For example, to sort the user list alphabetically by name, click on the name heading. If you click on the same heading again, it will sort the list in reverse order (for example, using the name, it would sort from Z to A). Usually sorting by name or ID is most useful, but occasionally you might sort by another column to put all similar users together. For example, if you were preparing to change or delete a particular access profile, you might sort by the access profile column so that all users with that profile would be together on the list.

Rearranging Columns in the User Window

To move any column, click the column heading and hold the mouse down. With the mouse held down, drag the column heading to the left or right; see the online help for an example of this.

You might want to move columns to keep important information like user IDs out of view, or, if you have created custom user entries, you might want to move them to where you can see them, since they are initially out of view.

Changing Column Width

F5 restores all columns to the positions they had when you started HandNet. If you want HandNet to save the new column positions, exit the HandNet program and come back in. HandNet then uses your changed column positions as the new standard or default.

You can also change the width of a column by pointing to the edge of the column heading, holding the mouse down, and then dragging the edge of the column to the desired position. This lets you fit more columns in the window (or, if you wanted to hide information from the casual observer, you could make columns wider to push other columns out of view); see the online help for an example of this.

Columns of Information in the User Window

F5 restores all columns to the widths they had when you started HandNet. If you want HandNet to save the new column widths, exit the HandNet program and come back in. HandNet then uses your changed column widths as the new standard or default.

User ID: The ID number the user must enter at the reader to gain access.

Access Profile: The profile determines which readers the user can access and when. You set up access profiles using *Access Profiles* on the *View* menu. You can change a user's access profile on the *Security* tab in *User Properties*; see page 92.

Authority Level: This indicates whether the user is allowed to access the command menus on the readers. For most users, this should say *None*. You can change a user's authority level on the *Security* tab in *User Properties*; see page 92.

Reject Threshold: The reject threshold controls how closely a user's hand must match the stored hand profile for the user to gain access. If this says *Default*, then HandNet uses the *Reject Threshold* on the *Configuration* tab in the *Reader Properties* (see page 47). If this says *Default** (with an asterisk), this means the user does not need hand recognition to gain access because the user was set up with a special enrollment; see page 76. If this shows a number, someone chose to override the standard reject threshold on the *Security* tab in *User Properties*; see page 93. A lower number requires a very precise match to gain access; a high number requires the hand to match less exactly. Thirty is the lowest number possible; 250 is the highest. One might use a lower number for users with access to the highest security areas; one might need a higher number if a user had arthritis or other hand condition that made it impossible to consistently place the hand on the reader in exactly the same position.

Last Site: This lists the last site where the user gained access. This is blank for a new user who has not accessed a reader yet.

Last Reader: This lists the last reader the user gained access through. This is blank for a new user who has not accessed a reader yet.

Last Time Used: This shows the date and time of the user's last access.

Limited State: This says *Unlimited* for users who are not set up to only have access for a limited period of time, that is, for users whose access will continue indefinitely. For users who are set up to only have access for a limited period of time, this says *Waiting* if the access period has not started yet, *Limiting* if the user currently has access, and *Expired* if the user's access period has ended; see page 93 for more about limited access.

Limited Start Time: If this user has been set up to have access for a limited period of time, this shows the date and time that the user's access begins. HandNet will not give the user access before this date/time. This is blank for other users; see page 93 for more about limited access.

Limited End Time: If this user has been set up to have access for a limited period of time, this shows the date and time that the user's access ends. HandNet will not give the user access after this date/time. This is blank for other users; see page 93 for more about limited access.

Additional Custom Columns: If you created any custom user entries, those columns would be listed as well; see page 97 for more about adding custom entries.

* * * * *

Adding Users Overview

Before You Add Users

If you are going to limit access to specific time periods or specific readers, set up *Time Zones* (see page 61) and *Access Profiles* (see page 67) before you set your users up.

Choosing How to Add the Users

If you have already set up users in a stand alone reader: You do not need to add users; you can upload user information from the reader; see *Getting User Information from a Reader* on page 99.

If you have been using one of our MS-DOS HandNet products (HandNet or HandNet Plus): You do not need to add users; you can import them from HandNet(+); see page 98.

If you only have one user to add, if you do not assign ID numbers sequentially, if you are adding users with different access profiles, if you want to fill in custom entries when adding the users, or if users choose their own ID numbers: Add a single new user; see page 76.

If a user needs access without hand recognition: Add a single new user and choose the *Special Enrollment* option. Before you do this, read *Adding a User Who Has Access Without Hand Recognition* below.

If you have many new users with the same access profile and you want automatically assigned ID numbers: Add multiple new users; see page 81.

Adding a User Who Has Access Without Hand Recognition

If a user has severe arthritis, missing fingers, or other hand deformities that keep the user's hand from being recognized, you can give the user access without hand recognition (if you choose this, the reader still asks the user to place a hand on the reader so it will not be apparent to others that hand recognition is not required, but the reader does not check the image of the hand; it gives access regardless of whose hand is placed there). **Since bypassing hand recognition gives you reduced security, only use this as a last resort.** Try these options first:

If the user only has a problem with the right hand: Enroll the user using the left hand (the user will place the hand palm up on the reader).

If the user has all of his/her fingers and is just having trouble with placing the hand consistently: On the *Security* screen in *User Properties*, check *Override the reader's reject threshold*, and drag the pointer to the far right (the *Less Sensitive* side). This causes the reader to be more tolerant of what it considers a match for that user's hand.

If these options are not possible, or if you try them and they do not work, then you will have to set the user up so that hand recognition is not required. To do this, follow the steps below.

1. If you have already added this user, open the *User* window, click the user once, press the *DEL* key (or pick *Delete* from the *User* menu), and confirm that you want to delete the user.
2. Click the *User* menu and then click *Add New….* This takes you to the first screen of the *New User Wizard*.
3. Check the *Special Enrollment* box. Since this option does give lower

security, HandNet asks you to confirm that you want to do this; click *Yes*.

4. Click the *Next* button.

5. Complete the rest of the process just as you would for any other new user.

6. Since the reader does not have to recognize this user's hand, you do not need to enroll this user; once you click *Finish*, the process is done for this user.

Allowing Users to be Added at the Reader

HandNet is initially set up to only allow new users to be added in the program; you can enroll a user at a reader, but you cannot add a new user there. If you want to be able to add and enroll a new user at a reader without adding the user to HandNet first, do this:

1. Click the *View* menu.

2. Click *Settings*.

3. Click the *Security* tab.

4. Check the box by *Do not delete unauthorized enrollments*.

5. Underneath this, indicate what access profile should be given to a user who is added at a reader (if you do not want the user to be able to access any readers until you change them in HandNet, choose *Never*).

6. Click the *OK* button at the bottom of the box.

Preventing Users from Being Added at Readers

Follow the steps above to get to the *Security* tab and make sure that *Do not delete unauthorized enrollments* is NOT checked.

* * * * *

Adding a Single New User

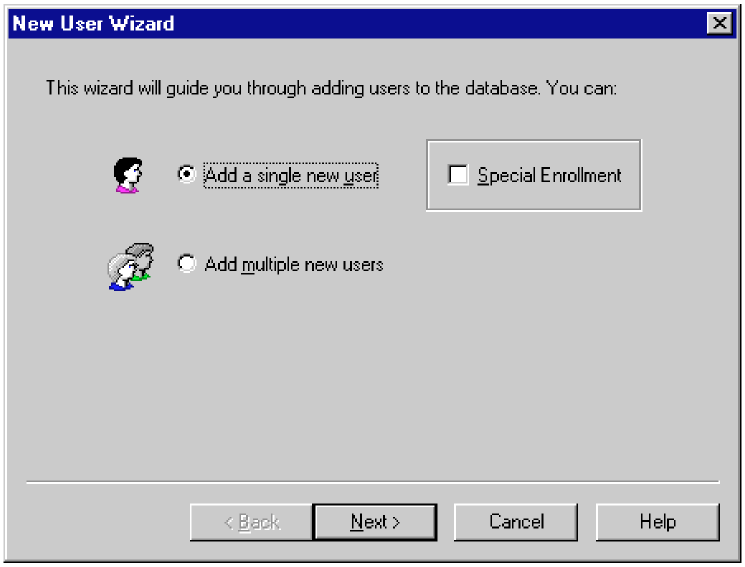
QUICK STEPS

Adding a Single User

1. Click the *User* menu and then click *Add New....* This takes you to the first screen of the *New User Wizard*.
2. *Add a single new user* is automatically selected, so click *Next* to continue.
3. On the *Name/ID* screen, enter the name and the ID number you are assigning to that user, and then click *Next* to continue.
4. On the *Security* screen, choose the access profile, authority level, and other security options. If you have set up custom user entries, click *Next*; otherwise click *Finish*.
5. If you see the *Custom* entries screen, fill in the column on the right and then click *Finish*.
6. Once you are done adding the user, you must enroll the user before the user will have access; see page 87.

Beginning the Process

To begin adding a new user, pick *Add New...* from the *User* menu.



This wizard will guide you through adding users to the database. You can:

● Add a single new user

□ Special Enrollment

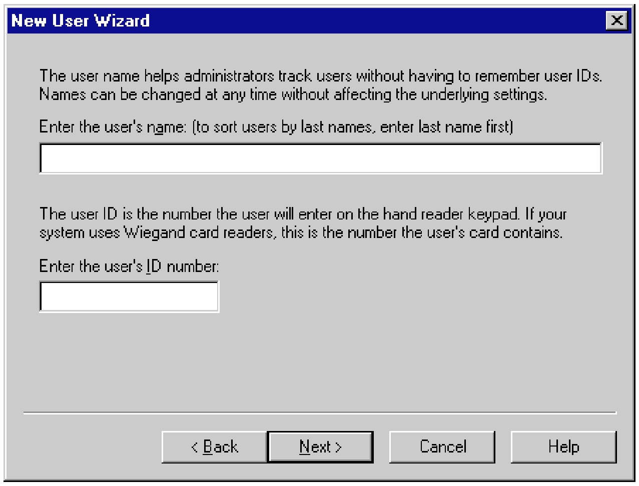
○ Add multiple new users

Special Enrollment: Check this box only if the user has severe hand deformities that require you to give the user access without hand recognition. This box is disabled if you are adding multiple users; if you are enrolling a user without hand access, you must add a single user.

Click *Next* to continue.

Name/ID Screen

This is the second screen in the process of adding a single new user:



The user name helps administrators track users without having to remember user IDs. Names can be changed at any time without affecting the underlying settings.

Enter the user's name: (to sort users by last names, enter last name first)

The user ID is the number the user will enter on the hand reader keypad. If your system uses Wiegand card readers, this is the number the user's card contains.

Enter the user's ID number:

Name: Enter the user's name.

If you want to sort the list of users by last name: Enter the last name first. For example, if the user's name is Sam Gamgee, you would enter *Gamgee, Sam*.

If you have two users with the same name: You must enter a unique name for each user. If two users have the same name, you might add a middle initial, or you might add a job description after each. For example, if you have two users named John Jones, you might enter something like *Jones, John (engineer)* and *Jones, John (maintenance).*

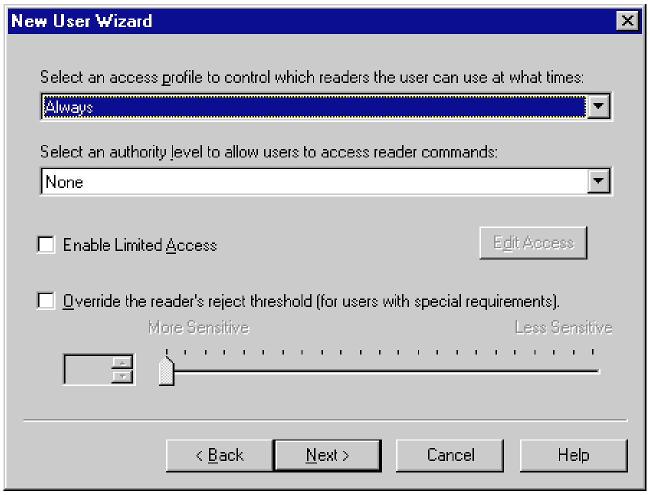
ID Number: Each number must be unique (if you could give the same number to two users, the reader would not know which was trying to gain access). Longer numbers are slightly more secure, but four or five digits are generally adequate in context where user's must enter the number. You may enter up to ten digits if you do not use a duress code, or up to nine digits if you do use a duress code. If you use a duress code, make sure that you do not create an ID that begins with that digit (see page 47 for more about duress codes). If you have set up an ID length on the *Settings* tab in the *Reader Properties* (see page 46), make sure that you do not create an ID that is longer than this.

If you use Wiegand card readers: Enter the ID number that is stored on the card.

Do not begin an ID with 0 (zero) if you are going to enroll the user with the command menus on the reader: HandNet lets you enroll a user by either picking *Enroll* from the *Reader* menu, or by using the *Command* menus on the reader (see page 88 for more about these options). If you are going to use the command menus on the reader, the *ID Number* should not begin with zero (0). While HandNet distinguishes between *5* and *0005*, the process of adding a user from the reader command menu does not. This means that if you create a user with an ID of 0005 in HandNet and try to enroll that user with the command menus on the reader, when you type 0005, the reader thinks you are enrolling user 5. This will not correspond with 0005 in HandNet. If you are going to use *Enroll* on the *Reader* menu, you can begin an ID with zero (0) (if you are never going to begin an ID with zero, this might be a good choice for a duress code if you use one).

Security Screen

This screen controls what this user has access to and when.



New User Wizard

Select an access profile to control which readers the user can use at what times: Always

Select an authority level to allow users to access reader commands: None

☐ Enable Limited Access

☐ Override the reader's reject threshold (for users with special requirements).

Select an access profile to control which readers the user can use at what times: Click this entry for a list of available access profiles. If this user can use all readers at all times, choose *Always*. If you do not want the user to be able to use any readers, choose *Never*. For other access, select the appropriate profile. You must set access profiles up before they are available here; see page 67 for more on setting up access profiles.

Select an authority level to allow users to access reader commands: This determines what the user can do at the reader. Each higher level gives access to the lower levels as well. For example, a user with an authority level of four can also use the *Level 1, 2* and *3* menus. Except for recalibrating the reader (part of *Level 1*), and enrolling a user if you have not purchased the upgrade to the full feature set, HandNet can control every setting in the reader, so there is generally no need to control settings through the reader menus.

None: This lets the reader gain access through the reader, but not use the command menus in the reader to change the reader's settings. This choice is appropriate for most users.

(1) Service: This lets you recalibrate the reader and change the reader's status display.

(2) Setup: This lets you control reader setup issues including how the reader is connected to your computer network, what language the reader displays in, the date/time, etc.

(3) Management: This lets you list users.

(4) Enrollment: This lets you add or remove users.

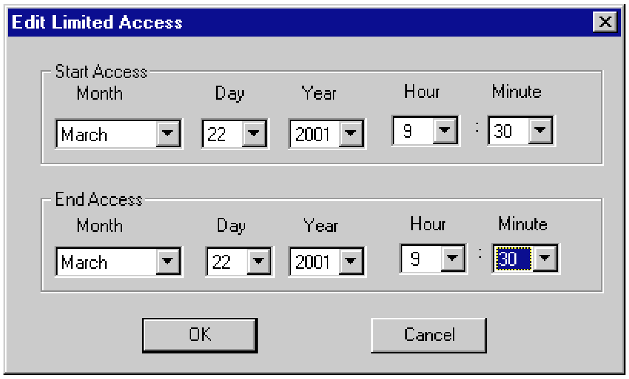
(5) Security: This lets you control the passwords for the reader menus, change time zones, enroll users who do not need hand access, etc.

See the HandKey manual for more on directly changing settings through the reader.

Limited Access

Enable limited access: This gives a user access for a specific date range. For example, suppose a contractor or temporary employee was going to be working in your building for a month. Or suppose an employee gave notice that s/he was leaving for a new job in two weeks. Once this period was over, you would not want these users to have access. Rather than having to remember to disable the user on the appropriate date, this option lets you set a start and end date/time so the user is automatically enabled and disabled at the appropriate points.

To set up start and end date/times, check the box by this button and then click the *Edit Access* button (this button only works if you have checked the box). This takes you to the *Edit Limited Access* screen:



Edit Limited Access

Start Access

Month	Day	Year	Hour	Minute
March	22	2001	9	30

End Access

Month	Day	Year	Hour	Minute
March	22	2001	9	30

To change either start or end date or time, click the corresponding entry and pick from the list that comes up.

This option is disabled if you have not purchased the license upgrade to the full feature set of Version 2.0.

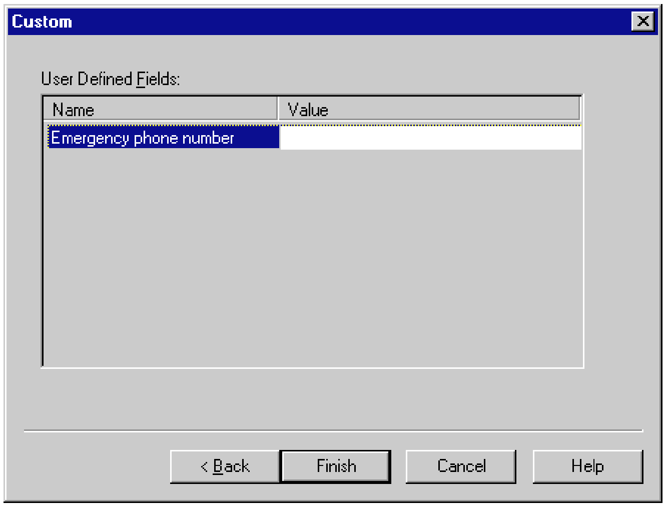
This option is NOT for limiting access to specific readers or for specific times of the day; to control that, use the *Access Profiles* entry.

Override the reader's reject threshold (for users with special requirements): For users with a physical condition like arthritis that prevents them from placing their hands on the reader in exactly the same way each time, this option lets you control how exact the hand match must be for the reader to grant access.

Normally you would not change this when adding the user. Instead, add and enroll the user, and then see if the user is having trouble gaining access. If a user is having trouble getting access consistently, go to the *Security* tab in the *User Properties* and change this entry there. You would check this box and then slide the pointer further to the right (the *Less Sensitive* side). If a user has a really severe hand condition, it is possible to give access without hand recognition, but because this offers reduced security, that should only be a last resort.

Custom Entries Screen

You only see this screen if you have set up any custom user entries (see page 97). The entries on this screen vary depending on what you have set up. For each entry on this screen, type the information in the *Value* column.



Name	Value
Emergency phone number	

Click *Finish* when done.

What to Do Next

The next step is to enroll the user; see page 87.

* * * * *

Adding a Group of Users at Once

You would add a group of users at once if you have to add many new users with the same access profile and other security access options, and if you want HandNet to automatically assign sequential ID numbers (if each user needs a different access profile, if you need to assign non-sequential ID numbers, or if you want to fill in custom user entries while adding the users, add single users instead; see *Adding a Single New User* on page 76).

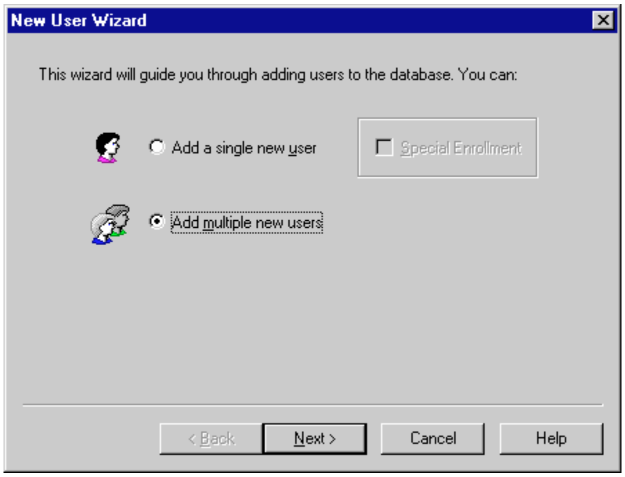
QUICK STEPS

Adding Multiple Users

1. Click the *User* menu and then click *Add New....* This takes you to the first screen of the *New User Wizard*.
2. Click *Add multiple new users*, and then click *Next*.
3. On the screen that asks for the number of users and starting ID, enter the number of users to create, and the ID number for the first new user. Click *Next* to continue.
4. On the *Security* screen, choose the access profile to assign to each of the new users. If needed, you can change the authority level and limited access. Do NOT change the user reject threshold. If you need to, you can later change this individually for a user who is having access problems. Click *Next* to continue.
5. The next screen shows the progress in adding the users. Once the process is done, click *Finish*.
6. You need to enroll the users before they have access. Typically, you will also rename the users since adding multiple users at once uses the ID number for the name.
7. If you have set up custom user entries, you will also want to edit the *Properties* for each user, click the *Custom* tab, and fill the appropriate information in there.

Beginning the Process

To begin adding a new user, pick *Add New...* from the *User* menu.



New User Wizard

This wizard will guide you through adding users to the database. You can:

○ Add a single new user

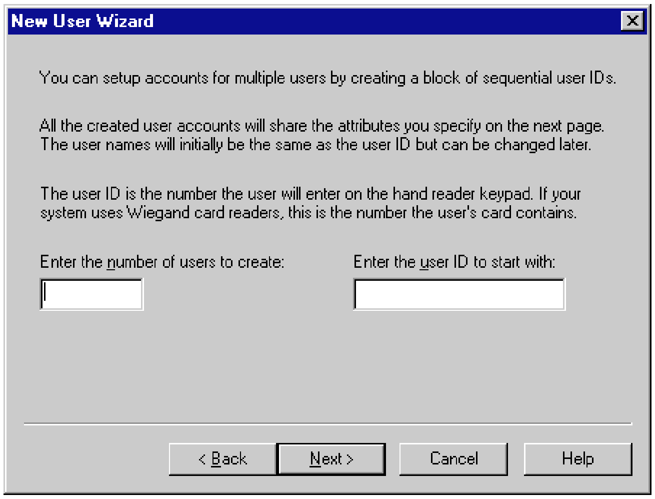
□ Special Enrollment

● Add multiple new users

Click the *Radio* button by *Add Multiple Users*, and then click the *Next* button.

Number of Users to Add and Starting ID

After you choose to add multiple users at once on the first screen of the *New User Wizard*, you see this screen.



New User Wizard

You can setup accounts for multiple users by creating a block of sequential user IDs.

All the created user accounts will share the attributes you specify on the next page. The user names will initially be the same as the user ID but can be changed later.

The user ID is the number the user will enter on the hand reader keypad. If your system uses Wiegand card readers, this is the number the user's card contains.

Enter the number of users to create:

Enter the user ID to start with:

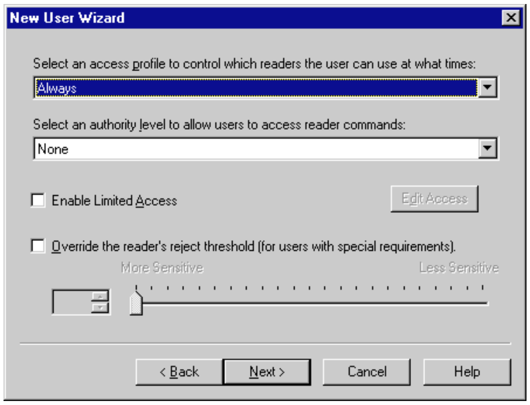
Number of users to create: Enter the number of users you want to add.

User ID to start with: Enter the starting user ID number. Use the number of digits that you would like for the final ID. For example, if you always want a five-digit ID number and you want to start with *1*, enter 00001 rather than just *1*. If you enter *00001*, HandNet will use *00002* next, then *00003*, and so on. If HandNet finds that a number is already used, if will skip that number and use the next available number. For example, if you enter *1000* as the starting number and *1000* through *1020* are all used, HandNet will automatically skip these numbers and start at *1021*. When the program adds the numbers at the end of the process, it lets you know if it had to skip any existing ID numbers.

However, do not begin an ID with zero (0) if you are going to enroll the user with the command menus on the reader. HandNet lets you enroll a user by either picking *Enroll* from the *Reader* menu, or by using the *Command* menus on the reader. If you are going to use the *Command* menus on the reader, the ID number should not begin with zero (0). While HandNet distinguishes between *5* and *0005*, the process of adding a user from the reader command menu does not. This means that if you create a user with an ID of *0005* in HandNet and try to enroll that user with the command menus on the reader, when you type *0005*, the reader thinks you are enrolling User Five, and this will not correspond with *0005* in HandNet. If you are going to use *Enroll* on the *Reader* menu, you can begin an ID with zero (if you are never going to begin an ID with zero, this might be a good choice for a duress code if you use one; see page 47 for more about duress codes).

Security Options

This screen controls what this user has access to and when.



New User Wizard

Select an access profile to control which readers the user can use at what times: Always

Select an authority level to allow users to access reader commands: None

☐ Enable Limited Access

☐ Override the reader's reject threshold (for users with special requirements).

After you click *Next* on this screen, HandNet adds the new users.

Select an access profile to control which readers the user can use at what times: Click this entry for a list of available access profiles. If these users can use all readers at all times, choose *Always*. If you do not want these users to be able to use any readers at this point, choose *Never*. For other access, select the appropriate profile. You must set access profiles up before they are available here; see page 67 for more about setting up access profiles.

Select an authority level to allow users to access reader commands: This determines what the users can do at the reader. For most users, *None* is the appropriate choice.

Each higher level gives access to the lower levels as well. For example, users with an authority level of four can also use the *Level 1, 2* and *3* menus. Except for recalibrating the reader (part of *Level 1*), and enrolling a user if you have not purchased the upgrade to the full feature set, HandNet can control every setting in the reader, so there is generally no need to control settings through the control menus in the reader.

None: This lets the reader gain access through the reader, but not use the command menus in the reader to change the reader's settings. This choice is appropriate for most users.

(1) Service: This lets you recalibrate the reader and change the reader's status display.

(2) Setup: This lets you control reader setup issues including how the reader is connected to your computer network, what language the reader displays in, the date/time, etc.

(3) Management: This lets you list users.

(4) Enrollment: This lets you add or remove users.

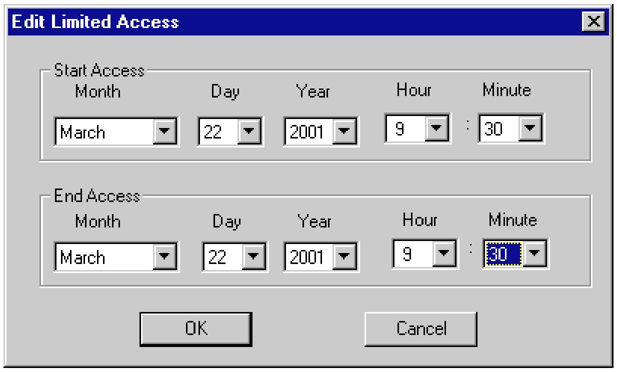
(5) Security: This lets you control the passwords for the reader menus, change time zones, enroll users who do not need hand access, etc.

See the HandKey manual for more on directly changing settings through the reader.

Limited Access

Enable limited access: This gives a user access for a specific date range. For example, suppose a contractor or temporary employee was going to be working in your building for a month. Or suppose an employee gave notice that s/he was leaving for a new job in two weeks. Once this period was over, you would not want these users to have access. Rather than having to remember to disable the user on the appropriate date, this option lets you set a start and end date/time so the user is automatically enabled and disabled at the appropriate points.

To set up start and end date/times, check the box by this button and then click the *Edit Access* button (this button only works if you have checked the box). This takes you to the *Edit Limited Access* screen:



Edit Limited Access

Start Access

Month	Day	Year	Hour	Minute
March	22	2001	9 :	30

End Access

Month	Day	Year	Hour	Minute
March	22	2001	9 :	30

To change either start or end date or time, click the corresponding entry and pick from the list that comes up.

This option is disabled if you have not purchased the license upgrade to the full feature set of Version 2.0.

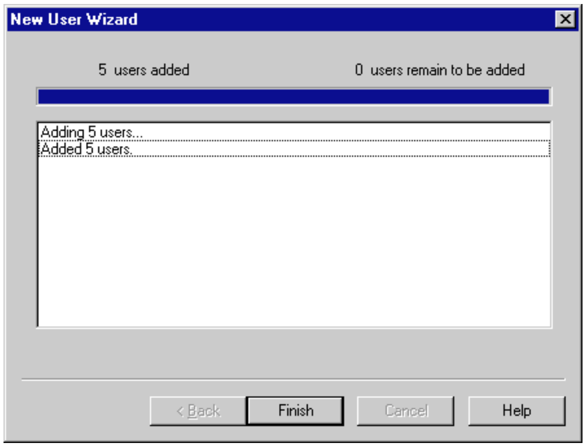
This option is NOT for limiting access to specific readers or for specific times of the day; to control that, use the *Access Profiles* entry.

Override the reader's reject threshold (for users with special requirements): Never change this option when adding multiple users at once. For users with a physical condition like arthritis that prevents them from placing their hands on the reader in exactly the same way each time, this option lets you control how exact the hand match must be for the reader to grant access. Only change this for individual users who are having trouble gaining access, never for a whole group of users at once.

If you later discover that a user is having trouble getting access consistently, go to the *Security* tab in the *User Properties* and change this entry there; see page 92. You would check this box and then slide the pointer further to the right (the *Less Sensitive* side). If a user has a really severe hand condition, it is possible to give access without hand recognition, but because this offers reduced security, that should only be a last resort; see *Adding a User Who Has Access Without Hand Recognition* on page 74 for more on this.

Progress Bar

This is the final screen in the process of adding new users. If you are adding a large number of users, it gives you an idea of how much longer the process will take.



Adding 5 users...
Added 5 users.

If HandNet tries to add ID numbers that are already used, you see messages about those numbers being skipped (this will not changed the number of new users that are added).

What to Do Next

After you click *Finish* to leave the screen above, you need to enroll the users before they have access; see page 87. You will typically also want to rename the users since this process uses the ID number for the name; page 90. And if you created custom user entries, you will want to go to the *Custom* tab in *User Properties* to fill these entries in for each user; see page 94.

* * * * *

Teaching Users How to Place Their Hands on Readers

Correct Hand Placement

Because the reader is looking at the shape of the hand, it is important that you place your hand on the reader the same way every time. When you put your hand on the reader, do this:

- If you are wearing a ring, make sure the stone is up in its normal position.
- Slide your hand forward onto the platen (moving forward like a plane would land at the airport; not straight down like a helicopter would land). Place your hand gently and comfortably; there is no need to apply pressure.
- Keep your hand flat. You should feel the platen with your palm and with the bottom of your fingers.
- Once you hand is flat on the platen, gently close your fingers so they touch against the finger pins. Again, there is no need to apply pressure or press hard. Watch the lights on the hand diagram on the top of the reader; if a light stays on, that finger is not making proper contact with the pin.

Left Hand Placement

If you have been enrolled with your left hand, follow the instructions above, but put your left hand palm up on the reader. The back of your hand should be as flat as possible against the platen.

* * * * *

Enrolling Users

Before a user can have access, you must take the user to a reader and have the reader create an image or template of the user's hand. If you have purchased the upgrade to the full feature set, you can start this process using *Enroll* on the *Reader* menu. If you have not purchased this upgrade, you must use the reader command menus to start the enrollment process.

Using the Enroll Option on the Reader Menu

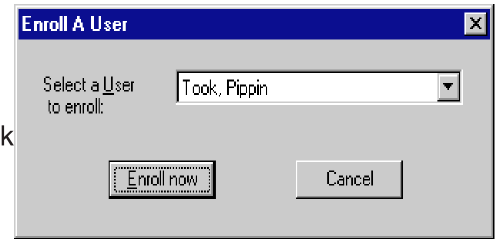
Before you enroll a user, add the user in HandNet; see page 76. You should also teach the user about correct hand placement; see page 86.

1. If the *Network* window is not open, press *CTRL-N* to open it.

2. In the *Network* window, click the reader to enroll the user at.

3. Click the *Reader* menu, and click *Enroll*. You see a screen like this:

4. If the user to enroll is not shown, click the entry and pick the user's name. Then click *Enroll now*.



Took, Pippin

5. The reader asks the user to place and remove his/her hand three times (if it asks for the hand more than three times, the user is not placing his/her hand consistently; go over the instructions for correct hand placement).

Unless you get a message indicating that there was a problem, the user is now enrolled.

Manually Enrolling Users Using the Reader Command Menus

Before you enroll a user, add the user in HandNet; see page 76. You should also teach the user about correct hand placement on page 86.

1. Check the list of users to make sure you have an authority level of four or higher. If you have an authority level of none, one, two, or three, you cannot do this (to change your authority level, double-click your name on the list of users, click the *Security* tab, click the *Authority Level* entry, and select the appropriate level).

2. Go to the reader to be recalibrated, and enter command mode on the reader:

   If you have a HandKey II or HandKey CR reader: Press *CLEAR*, and then press *ENTER*.

   If you have an ID3D HandKey reader: Press # AND * (you can press them at the same time, or one after the other).

   The display on the reader should look like this:

```
        READY
      * :
```

3. Type your user ID number (the same one you enter to get access through the reader), and press *ENTER* or *#.* The reader asks you to place your hand. Once it recognizes your hand, this display looks like this:

```
ENTER PASSWORD
```

4. Type *4* and press *ENTER* or *#* (this is the standard password for the *Enrollment* menu in the reader; if you have changed this on the *Passwords* screen in the *Reader Properties*, enter the password you have set up).

   If you have a HandKey II or HandKey CR reader: The display should now look like this:

```
    ADD USER
 *  NO     YES #
```

   If you have an ID3D HandKey reader: The display should now look like this:

```
  ENROLL USER
 *  NO     YES #
```

   If the reader shows the *READY* screen again instead of this screen, then either you placed your hand improperly or you do not have the rights to do this; carefully check step one again.

5. Press the *YES / #* button. This display should now look like this:

```
ID?
:
```

6. Type the ID number of the user to enroll and press *ENTER* or *YES / #*. The display should now look like this:

```
** PLACE HAND **
    1/3
```

7. Have the user place his/her hand on the reader. The reader will ask the user to remove the hand and place it again. The reader should ask the user to place his/her hand three times; if it asks for the hand more than three times, the user is not placing his/her hand consistently; go over the instructions for correct hand placement.

   Once the user has correctly placed the hand three times, the reader asks for the time zone:

```
ENTER TIME ZONE
    (0)?:
```

8. When the user has access to this and other readers is controlled by the access profile you have assigned in the user's properties, so just press *ENTER* or *YES / #.*

9. The reader briefly flashes the message *User Enrolled* and then returns you to the *Add User* or *Enroll User* display. Enroll another user if needed, or press the *CLEAR* button to leave the *Enrollment* menu and return to the reader to its normal display.

* * * * *

Changing Users

Overview

QUICK STEPS

Changing Users

1. If the user window is not shown, press *CTRL-U* or pick *Users* from the *View* menu.
2. Double-click the user to change information. This takes you to the *General* tab in the *User Properties* (you can also click the user once and then pick *Properties* from the *User* menu).
3. Click the tab that has the information you want to change:
   To change the user's name or ID: this is on the *General* tab.
   To change the users access level, authority, limited access, or the reader's sensitivity: Click the *Security* tab.
   To change Custom entries: Click the *Custom* tab.
4. Change information as needed ant then click *OK*.

Renaming Users

1. If the user window is not shown, press *CTRL-U* or pick *Users* from the *View* menu.

2. Double-click the user to rename. This takes you to *User Properties*.

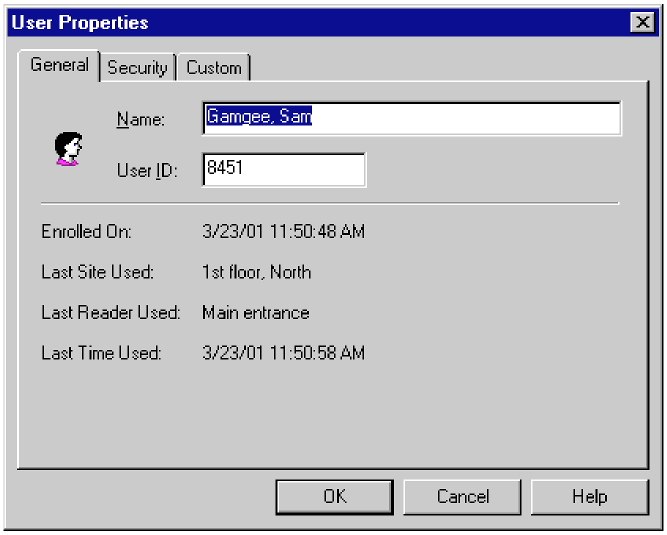
3. Type the new name, and then press *ENTER* or click *OK*.

Alternate Methods

Right-click the user's name and pick *Rename* from the menu that pops up; click the user once and pick *Rename* from the *View* menu; or click the user once, pause for long enough so the computer will not think you are double-clicking, and then click directly on the user's name.

User Properties, General

The *General* tab in *User Properties* lets you change the user's name or ID. It also shows when the user last accessed a reader.



User Properties

Name: Gamgee, Sam

User ID: 8451

Enrolled On: 3/23/01 11:50:48 AM

Last Site Used: 1st floor, North

Last Reader Used: Main entrance

Last Time Used: 3/23/01 11:50:58 AM

Name: Enter the user's name.

If you want to sort the list of users by last name: Enter the last name first. For example, if the user's name is Sam Gamgee, you would enter *Gamgee, Sam*.

If you have two users with the same name: You must enter a unique name for each user. If two users have the same name, you might add a middle initial, or you might add a job description after each. For example, if you have two users named John Jones, you might enter something like *Jones, John (engineer)* and *Jones, John (maintenance)*.

ID Number: If you change a user's ID, be sure to let the user know. The user will not be able to gain access through any reader without knowing the correct ID.

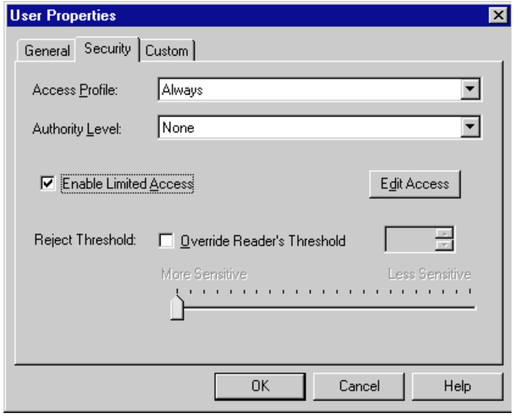
Each number must be unique (if you could give the same number to two users, the reader would not know which was trying to gain access). Longer numbers are slightly more secure, but four or five digits are generally adequate in context where user's must enter the number. You may enter up to ten digits if you do not use a duress code, or up to nine digits if you do use a duress code. If you use a duress code, make sure that you do not create an ID that begins with that digit; see page 47 for more about duress codes. If you have set up an *ID length* on the *Settings* tab in the *Reader Properties*, make sure that you do not create an ID that is longer than this; see page 47 for more about ID length.

If you use Wiegand card readers: Enter the ID number stored on the card.

Do not begin an ID with zero (0) if you are going to enroll the user with the command menus on the reader: HandNet lets you enroll a user by either picking *Enroll* from the *Reader* menu, or by using the command menus on the reader. If you are going to use the command menus on the reader, the ID number should not begin with zero (0). While HandNet distinguishes between 5 and 0005, the process of adding a user from the reader does not. This means that if you create a user with an ID of 0005 in HandNet and try to enroll that user with the command menus on the reader, when you type 0005, the reader thinks you are enrolling user 5; this will not correspond with 0005 in HandNet. If you are going to use *Enroll* on the *Reader* menu, you can begin an ID with zero (if you are never going to begin an ID with zero, this might be a good choice for a duress code if you use one).

User Properties, Security

The *Security* tab controls what this user has access to and when.



Access Profile: Always

Authority Level: None

☑ Enable Limited Access

Reject Threshold: □ Override Reader's Threshold

Select an access profile to control which readers the user can use at what times: Click this entry for a list of available access profiles. If this user can use all readers at all times, choose *Always*. If you do not want the user to be able to use any readers at this point, choose *Never*. For other access, select the appropriate profile. You must set access profiles up before they are available here.

Select an authority level to allow users to access reader commands: This determines what the user can do at the reader. For most users, *None* is the appropriate choice.

Each higher level gives access to the lower levels as well. For example, a user with an authority level of four can also use the *Level one, two* and *three* menus. Except for recalibrating the reader (part of level 1), and enrolling a user if you have not purchased the upgrade to the full feature set, HandNet can control every setting in the reader, so there is generally no need to control settings through the reader menus.

None: This lets the reader gain access through the reader, but not use the command menus in the reader to change the reader's settings. This choice is appropriate for most users.

(1) Service: This lets you recalibrate the reader and change the reader's status display.

(2) Setup: This lets you control reader setup issues including how the reader is connected to your computer network, what language the reader displays in, the date/time, etc.

(3) Management: This lets you list users.

(4) Enrollment: This lets you add or remove users.

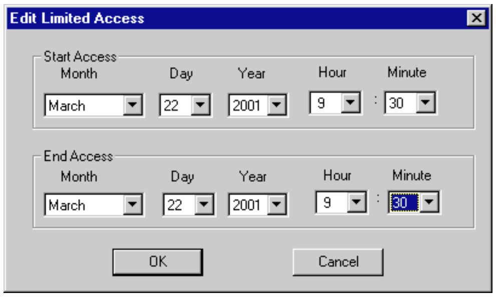
(5) Security: This lets you control the passwords for the reader menus, change time zones, enroll users who do not need hand access, etc.

See the HandKey manual for more on directly changing settings through the reader.

Limited Access

Enable limited access: This gives a user access for a specific date range. For example, suppose a contractor or temporary employee is going to be working in your building for a month. Or suppose an employee gives notice that s/he is leaving for a new job in two weeks. Once this period is over, you would not want these users to have access. Rather than having to remember to disable the user on the appropriate date, this option lets you set a start and end date/time so the user is automatically enabled and disabled at the appropriate points.

To set up start and end date/times, check the box by this button and then click the *Edit Access* button (this button only works if you have checked the box). This takes you to the *Edit Limited Access* screen:



Edit Limited Access

Start Access

Month	Day	Year	Hour	Minute
March	22	2001	9	30

End Access

Month	Day	Year	Hour	Minute
March	22	2001	9	30

To change either start or end date or time, click the corresponding entry and pick from the list that comes up.

This option is disabled if you have not purchased the license upgrade to the full feature set of Version 2.0.

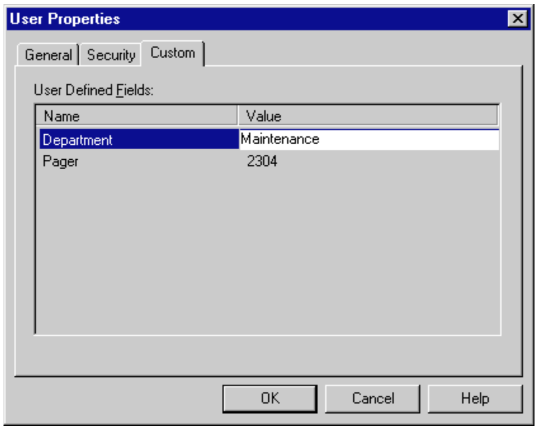
This option is NOT for limiting access to specific readers or for specific times of the day. To control that, use the *Access Profiles* entry.

Override the reader's reject threshold (for users with special requirements): For users with a physical condition like arthritis that prevents them from placing their hands on the reader in exactly the same way each time, this option lets you control how exact the hand match must be for the reader to grant access.

If a user is having trouble getting access consistently, check this box and then slide the pointer further to the right (the *Less Sensitive* side). If a user has a really severe hand condition, it is possible to give access without hand recognition, but because this offers reduced security, that should only be a last resort.

User Properties, Custom

You only see entries on the *Custom* tab if you have set up custom user entries (see page 97 for more on creating custom user entries). The entries on this screen vary depending on what you have set up; the entries on your screen will probably be completely different from the examples show below.



User Defined Fields:

Name	Value
Department	Maintenance
Pager	2304

To change a value, click the item in the *Value* column and then enter the correct value.

When You Are Done

When you are done changing *User Properties*, click the *OK* button at the bottom of the screen.

* * * * *

Changing Access for Many Users at Once

Import TZ Option

Import TZ on the *File* menu lets you change the access profile to *Always* or *Never* for many users based on information in a text file (this file would be created with some other program).

Caution

If you use this option, be aware that there are security risks involved: if you mistype a number in the file, you could easily give full access to a different user than you intended. And unlike most other changes in HandNet, the fact that this option is used and the fact that a user's access is changed is NOT reflected in the activity log, so you will not have any record of the change. In most contexts, it is more appropriate to change user access through the *Security* tab in *User Properties*; see page 92.

File Format

Each line of the file would list a user ID number followed by a comma, and then either 0 (zero) to set that user's access profile to *Always*, or sixty-one, to set that user's profile to *Never* (currently, you cannot use the file to switch to any other profile). For example, suppose your text file looked like this:

```
1001, 0
1002, 0
1003, 61
21345, 0
43567, 61
```

If you import this file, HandNet would set the access profile to *Always* for users with the IDs of 1001, 1002, and 21345, and it would set the profile to *Never* for users with IDs 1003 and 43567. It would not change the access profiles for any other users. If HandNet could not find a user with the corresponding ID number, or if you have something other than zero or sixty-one after the comma, HandNet would skip that line. It would not give you any message or tell you the line was skipped. If you have any lines that did not match the format above (for example, if you do not have the comma between the ID and the zero or sixty-one), HandNet would give a message at the end of the process that tells you how many bad records are ignored. If other lines are in the correct format, HandNet would still process them successfully.

You do not see any message or progress bar during the import process. If you are importing many records, you could have some delay where it looks like nothing is happening. For example, on a 166MHz processor, importing 1,000 records takes slightly over thirty seconds; you would not see any activity while this is happening.

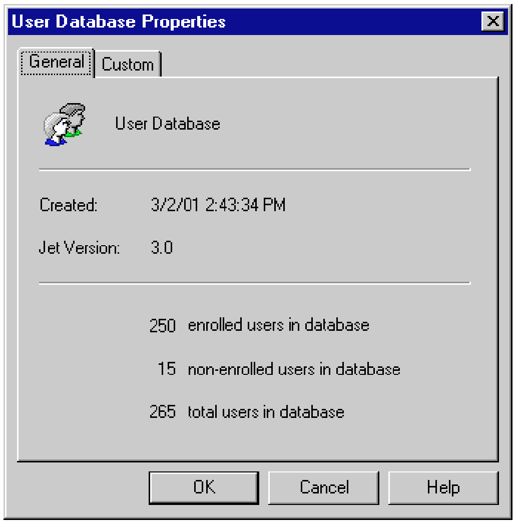
* * * * *

User Database Properties

What Information Is Shown

This screen shows general information about the whole user database, including the date it is created, the Version number, the number of enrolled users and number of non-enrolled users, and the total number of users in the database. You do not typically need this information during normal use of the program. However, if you want to add or change custom user entries, you would come to this screen and then click the *Custom* tab.

You get to this screen by picking *DB Properties* from the *User* menu.



User Database

Created: 3/2/01 2:43:34 PM

Jet Version: 3.0

250 enrolled users in database

15 non-enrolled users in database

265 total users in database

* * * * *

Adding Custom User Entries

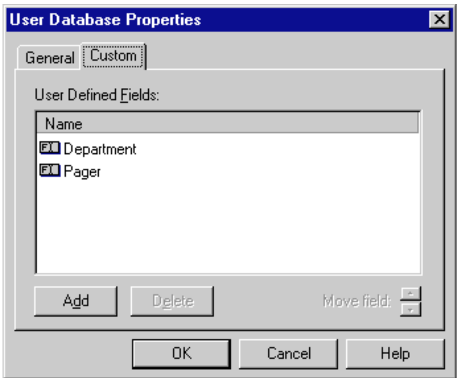
To collect additional information about users in HandNet, you can add additional custom entries. HandNet then asks for this information on the *Custom* screen of *New User Wizard* (see page 80) and the *Custom* tab in the *User Properties* (page 94).

What you might want to collect could vary widely depending on how you are using HandNet: emergency phone numbers, employment start dates, department, pager number. You can add as many entries as you need.

The information that you add in custom entries is only available on the screen, either in *User Properties* or on the list of users (available by picking *Users* from the *View* menu). Currently, HandNet does not include custom user information on any reports.

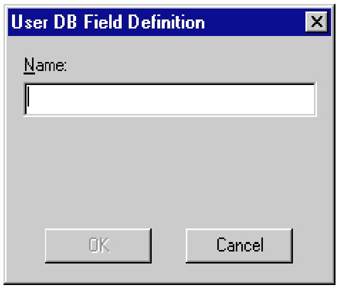
Getting to the List of Custom Entries

1. Click the *User* menu and then click *DB Properties*.
2. Click the *Custom* tab. You will see a screen like this, but with different entries.



Adding a New Entry

To add a new custom entry, click the *Add* button. You see this screen:



Type the name of the field or entry to add and press *ENTER* or click *OK*. Make sure that you enter the name of the entry correctly; once you continue, you cannot change the name.

Deleting a Custom Entry

Click the entry in the list and click *Delete*. Be sure that you are deleting the correct item; the program will not ask you to confirm the deletion, and once you delete a custom entry, all information that you have entered for users in that entry is gone. For example, suppose you create an *Emergency Phone Number* entry and entered phone numbers for all of your users. If you delete emergency phone numbers here, all of the phone numbers that you enter would be gone and there would be no way to get them back unless you make a backup of your HandNet information.

Changing the Order of the Entries

On the *Custom* screen in the *User Properties*, the entries in the same order as they are listed here. To change the order of the entries, click the entry to move and then click the up or down arrows next to the words *Move field*.

* * * * *

Converting Users from MS-DOS HandNet or HandNet+

If you have been using one of our MS-DOS programs (either HandNet or HandNet+), *Convert HandNet+...* on the *File* menu lets you import your users so you do not have to enter and enroll them again. This option brings in each user's name, ID number, authority level, and reject threshold.

If you have been using an older Version of HandNet for Windows, you do not need to do anything to convert that information.

To Convert HandNet Plus Users

1. If you have been using HandNet rather than HandNet Plus, follow the steps below to convert your user information from HandNet to HandNet Plus format.
2. Pick *Convert HandNet+* from the *File* menu.
3. If you have installed HandNet+ somewhere other than in C:\HNET, click the *Browse* button and go to the directory where HandNet+ is installed. Then click the *Open* button.
4. Click the *Convert* button. The HandNet+ database is converted to HandNet for Windows™ format.
5. This con Version does not bring in the access profiles for the users, so when this is done you must assign an access profile to each user on the *Security* tab in *User Properties*.

To Convert MS-DOS HandNet Users

If your DOS Version of HandNet is in the standard /HNETdirectory: Press *F1* while in HandNet to pop up the help. In the index, type *convert* and open the topic on converting HandNet+ information. In this topic there is a button that automatically does this process for you.

If your DOS Version of HandNet is NOT in the standard /HNET directory:

1. Copy the *convert.exe* file from the HandNet for Windows directory to the directory the MS-DOS Version of HandNet is located. The standard location for HandNet for Windows is *C:\Program Files\Schlage Biometrics, Inc.\HandNet for Windows.* For example, to copy the convert file from this directory to *c:\hnet*, you would type:

   ```
   copy c:\progra~1\recogn~1\handne~1\convert.exe c:\hnet\
   ```

2. Switch to the directory the MS-DOS Version of HandNet is in. For example, to switch to the *\hnet* directory, you would type *cd\hnet* and press *ENTER*.
3. Make a backup copy of the file that contains your user information. This file is called *id_dbase.dat*. For example, you might type:

   ```
   copy id_dbase.dat id_dabase.bak
   ```

4. Type *convert* and press *ENTER*. This should convert the information to HandNet Plus format. Once you have done this, you are ready to import the information into HandNet for Windows using the steps described above.

* * * * *

Importing and Exporting Users

Getting User Information from a Reader

If you have already set up users in a reader that you are connecting to HandNet, you do not need to recreate those users. You can get user information from the reader by doing this:

1. Pick *Network* from the *View* menu (or type *CTRL-N*).
2. On the list of readers in the right pane of the *Network* window, select the reader(s) to get user information from.
3. Click the *Reader* menu, click *Upload*, and click *Users*.
4. The program asks you to confirm that you want to upload users from the reader; click *Yes* to continue.

Importing Users from Another Copy of HandNet

You only need to import users if you have readers connected to several different computers (each with its own copy of HandNet) and if users added to one system need to be available on the others. If all of your readers are connected to a single copy of HandNet, you do not need this feature.

The export feature is only available if you have purchased the upgrade to the full feature set of Version 2.0.

Setting Up Import Settings First

Make sure that you select the correct choices for what to import on the *User Import/Export* tab in *System Settings* before you try to import; see page 28. When HandNet imports, it empties the *Import* file, discarding those user records that do not meet the conditions you have checked there.

Importing Users From Another Computer

1. On the computer where you exported users, go to the HandNet directory and copy the file *export.mdb* to a floppy disk (you could also copy this file to a network drive, attach it to an e-mail, etc.).
2. Rename the file on the disk (or in the new location) to *import.mdb*.
3. Put this *import.mdb* file into the HandNet directory on the computer where you want to import users.
4. If you do not have that copy of HandNet set up to import automatically, pick *Import Users* from the *File* menu (if you have the *Enable* box under *Auto Import* checked on the *User Import/Export* tab in *System Settings*, HandNet starts importing as soon as it finds the *import.mdb* file in the directory; see page 28).

The activity window lists each user that is added, deleted or changed.

Exporting Users to Another Copy of HandNet

You only need to export users if you have readers connected to several different computers (each with its own copy of HandNet) and if users added to one system need to be available on the others. If all of your readers are connected to a single copy of HandNet, you do not need this feature.

The export feature is only available if you have purchased the upgrade to the full feature set of Version 2.0.

Automatically Exporting Users

HandNet can automatically export users when you create, enroll, change or delete users. When HandNet exports users is controlled by the items in the *Export* column on the *User Import/Export* tab in *System Settings*; see page 28.

Manually Exporting Users

1. Go to the *Users* window.
2. Select the users to export. To select multiple users that are together on the list, click the first user, hold the *SHIFT* key down, and click the last user that you want to select. To select multiple users that are not together on the list, click the first user to select, hold the *CTRL* key down, and click each other user that you want to select.
3. Right-click (this brings up a menu).
4. On the menu, point to *Export*, and then pick *Selected* (or pick *All* to export every user in the list whether selected or not).

You will see a message with a progress bar that indicates that the users are being exported (if you only selected a few users, this may vanish almost instantly). Once this box disappears, the export process is done.

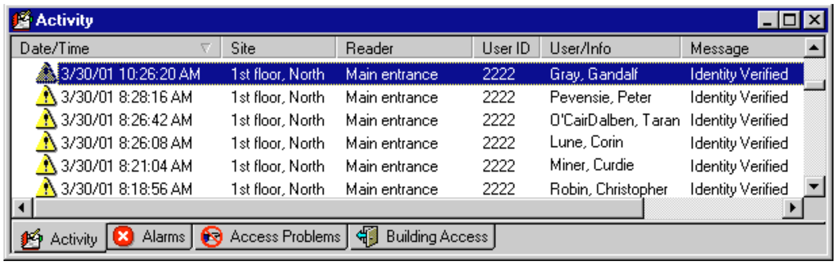
To import these users on the other computer, see the instructions for *Importing Users from Another Copy of HandNet* on page 99.

* * * * *

Monitoring Ongoing Activity

Activity Window

The *Activity* window lists everything that happens at any reader connected to HandNet, and any change made in the HandNet program. To open this window, pick *Activity* from the *View* menu, or press *CTRL-A*.



Activity

Date/Time	Site	Reader	User ID	User/Info	Message
3/30/01 10:26:20 AM	1st floor, North	Main entrance	2222	Gray, Gandalf	Identity Verified
3/30/01 8:28:16 AM	1st floor, North	Main entrance	2222	Pevensie, Peter	Identity Verified
3/30/01 8:26:42 AM	1st floor, North	Main entrance	2222	O'CairDalben, Taran	Identity Verified
3/30/01 8:26:08 AM	1st floor, North	Main entrance	2222	Lune, Corin	Identity Verified
3/30/01 8:21:04 AM	1st floor, North	Main entrance	2222	Miner, Curdie	Identity Verified
3/30/01 8:18:56 AM	1st floor, North	Main entrance	2222	Robin, Christopher	Identity Verified

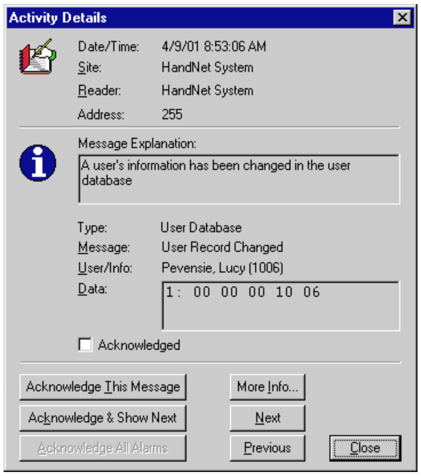
Only the first two tabs at the bottom of this screen (*Activity* and *Alarms*) are always there. The others are merely examples of custom activity views that you can create as needed; see *Creating Custom Activity Views* on page 104.

Rearranging or Resizing Columns in the Activity Window

To move any column, click on the column heading and hold the mouse down. With the mouse held down, drag the column heading to the left or right.

Getting More Detail about an Activity in the Activity Window

When you double-click on an activity in the *Activity* window, you get a screen like this that tells more about that activity.



Activity Details

Date/Time: 4/9/01 8:53:06 AM
Site: HandNet System
Reader: HandNet System
Address: 255

Message Explanation:
A user's information has been changed in the user database

Type: User Database
Message: User Record Changed
User/Info: Pevensie, Lucy (1006)
Data: 1: 00 00 00 10 06

□ Acknowledged

Date/Time: This shows the date and time when the activity occurred. The date is listed in month/day/ year order, and the time lists hours/minutes/seconds.

Site: If this activity happened at a reader, this shows the name of the site the reader is associated with.

Reader: If this activity happened at a reader, this shows the reader's name.

Address: If this activity happened at a reader, this shows the reader's address; this address should correspond with the name of the reader listed above. If this activity occurred in the HandNet program, this says *255*.

Message Explanation: This shows some additional explanation of the message. For more explanation, see the complete list of activity messages starting on *Activity Messages* on page 116.

Type: Each message falls into one of ten categories. When you are creating an activity filter or custom activity report, you can limit your report or activity view to specific types of messages; see *Message Types* on page 111 for more detail.

Message: This shows the same message that you saw on the list in the *Activity* window.

User/Info: If this message is associated with a particular user, this shows the user's name and ID number.

Data: This shows technical detail about the message that is not relevant to your use of the program. This is occasionally useful to support in debugging a problem.

Acknowledged [checkbox]: This shows whether this message has been acknowledged yet. You cannot uncheck this box once it is marked. You also can check the box directly; you must use one of the three *Acknowledge...* buttons below.

Buttons on the Activity Details Screen

Acknowledge This Message: This marks the message as acknowledged. After the message on the activity or alarm list, you will see *:ACK* followed by the name of the operator who acknowledged the message and the date/time when it was acknowledged. If this is an alarm, this also shuts the alarm off.

Acknowledge & Show Next: This acknowledges the current message and shows the next message. By next, we mean more recent in time; that is, the message above the current message on the activity list.

Acknowledge All Alarms: This button is disabled unless there is an alarm that has not been acknowledged yet. You might use this button if you see several related alarms on the list and you want to acknowledge them all at once.

More Info: This brings up the online help.

Next: This shows the message that occurred more recently in time, that is, the message directly before this on the activity list.

Previous: This shows the message that occurred before this message in time, that is, the message directly after it on the activity list.

* * * * *

Getting to and Acknowledging Alarms

Getting to the Alarms List

Alarms are listed with the rest of the activity in the *Activity* window, but we have also provided a separate view with just the alarms. To see this view, click the *Alarms* tab at the bottom of the *Activity* window.

Acknowledging an Alarm

If an alarm is triggered in HandNet, do this to acknowledge it and turn it off.

1. If the *Activity* window is not shown, press *CTRL-A* or pick *Activity* from the *View* menu.

2. Double-click the alarm message with the bell icon next to it (you can see it both in the regular activity view or by clicking the *Alarm* tab at the bottom of the window).

3. Click one of the *Acknowledge...* buttons at the bottom left of the window (you cannot just click the checkbox by the word acknowledged; you must click one of the buttons). After the message on the *Activity* or *Alarm* list, you will now see *:ACK* followed by the name of the operator who acknowledged the message and the date/time it was acknowledged.

4. Take whatever action is appropriate in response to the alarm.

What Situations Cause Alarms

Which situations trigger alarms depends on which items are checked on the *Alarms* tab in the *System Settings*; see page 25.

* * * * *

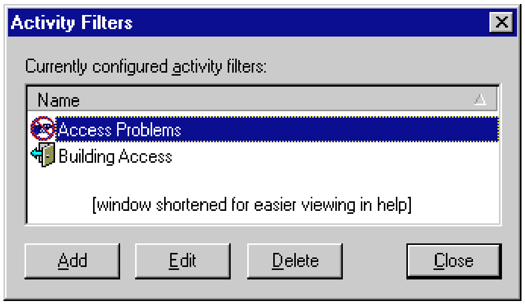
Creating and Printing Custom Activity Views

Creating a Custom Activity View

The main *Activity* window lists all activity that occurs: every access from every reader, every failed access, every user addition and enrollment, every alarm, and so on. Sometimes its useful to see less than this. For example, if you wanted to identify users who were having access problems, you might want to see only the *Identity Unknown* and *Access Denied* messages (the messages that can occur when someone enters a valid ID but then does not get a match on the hand). Or if you want to identify who has come in the building, you might want to see only *Identity Verified* messages and only for the readers that controlled entrances to the building.

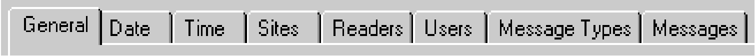
You can create (and print reports on) custom views for these or any other subsets of activity, limiting the view to specific messages, dates, times, users, and/or readers. To create a custom activity view:

1. Click the *View* menu, and click *Activity Filter*. You see a list of any custom activity views if you have created any yet. This list looks like this, but the *filters* listed will be different.


Activity Filters
Currently configured activity filters:
Name
Access Problems
Building Access
[window shortened for easier viewing in help]
Add
Edit
Delete
Close

2. Click the *Add* button to create a new filter (that is, a set of conditions that will filter out only the information you want to see). This takes you to the first *Activity Filter* screen (to change a filter you have already created, click the filter and then click *Edit*).

3. Give the filter a name, associate an icon if you wish, and then go to each tab where you want to include something less than all of the activity.



   Each tab is initially set up to include all information; go to those where you want to limit or filter out particular information. For example, if you only want activity at certain readers, you would go to the *Readers* tab. If you only want certain messages, go to the *Messages* tab. The options on these tabs are explained, starting on page 107.

4. When you have entered all of the conditions needed, click the *OK* button at the bottom of the window.

To start this process, you could also right click on the bar at the bottom of the *Activity* window, and then pick *Add New Filter....*

Removing a Custom Activity View

This does not remove any activity from HandNet; it only removes the custom view of the activity.

1. Click the *View* menu, and click *Activity Filter*. You will see a list of any custom activity views you have created.

2. Click the view or filter to remove and click *Delete*.

Printing an Activity Report Based on an Activity Window

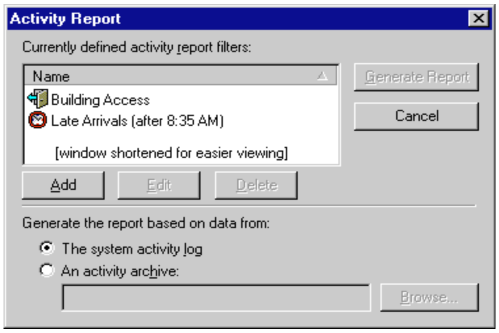
1. Right-click on the bottom bar of the *Activity* window (where the *Activity* and *Alarms* tabs are).

2. Pick *Generate Report*.

3. In the report window that comes up, click the printer icon in the header; see *Printing or Viewing Reports* on page 127 for more detail.

Creating a Custom Activity Report from the Reports Menu

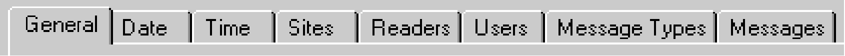
If you have not already created a custom activity view, or if you need to run the report on archived activity, then follow these steps to design the report.


Activity Report
Currently defined activity report filters:
Name
Building Access
Late Arrivals (after 8:35 AM)
[window shortened for easier viewing]
Generate Report
Cancel
Add
Edit
Delete
Generate the report based on data from:
● The system activity log
○ An activity archive:
Browse...

1. From the *Main Menu* bar, click *File*, click *Reports*, and click *Activity...*. You see a screen like this (if you created any custom reports they would be listed; your reports may be very different from the samples listed here).

2. Click the *Add* button to create a report (that is, a set of conditions that will filter out only the information you want to see). This takes you to the first *Activity Report* screen (to change a report you have already created, click the filter and then click *Edit*). The screens that you see are identical to those that you see when creating a custom activity view.

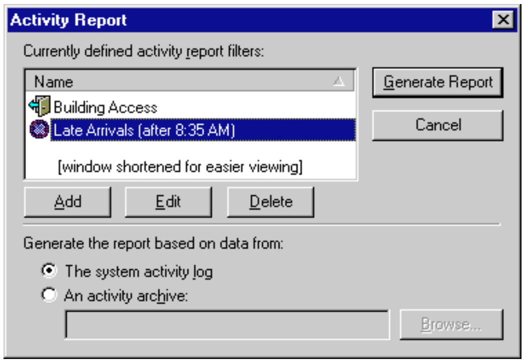
3. Give the report a name, associate an icon if you wish, and then go to each tab where you want to include something less than all of the activity.



Each tab is initially set up to include all information; go to those where you want to limit or filter out particular information. For example, if you only wanted activity at certain readers, you would go to the *Readers* tab. If you only want certain messages, go to the *Messages* tab. The options on these tabs are explained starting on page 107.

4. When you have entered all of the conditions needed, click the *OK* button at the bottom of the window. This returns you to the list of reports.

Printing an Activity Report from the Reports Menu


Activity Report
Currently defined activity report filters:
Name
Building Access
Late Arrivals (after 8:35 AM)
[window shortened for easier viewing]
Generate Report
Cancel
Add
Edit
Delete
Generate the report based on data from:
● The system activity log
○ An activity archive:
Browse...

1. From the main menu, click *File*, click *Reports*, and then click *Activity Reports*. You see a screen like this (if you have created any custom reports they would be listed; your reports may be very different from the samples listed here).

2. If you have not already designed the report, see *Creating a Custom Activity Report* from the *Reports* Menu above for help designing it.

3. Click the report in the list of reports at the top of the window.

4. At the bottom of the window, indicate which activity to generate the report from:

   The system activity log: This includes all the activity that has occurred since the last time you archived activity (and that meets your report conditions).

   An activity archive: This includes all activity that meets your report conditions that is in the archive file that you pick. Click the *Radio* button by this choice, click the *Browse* button, and pick the file. HandNet lists files that have an *.hna* extension. Pick the *Archive* file and click *OK*.

   If the activity that you want is in several archive files, you will have to run the report several times, once for each archive file. If you need the information in a single report, you can export each report to a file and then use another program to combine the reports into a single file.

5. Click the *Generate Report* button. HandNet generates the report and shows it in a new window on the screen.

6. Click the *Printer* icon near the middle of the header to print the report, or click the icon with the envelope to export the content of the report to a file. You can export to a variety of formats including Word, Excel, Lotus 1-2-3, .rtf, text, and others; see *Printing or Viewing Reports* on page 127 for more detail.

   If the printer icon is disabled and grayed-out, you do not have a printer set up yet on this computer (to set up a printer, go to the Windows *Start* menu, highlight *Settings*, pick *Printers*, and click *Add Printer*).

7. To close the *Report* window when done, click the *X* in the upper-right corner of the window.

* * * * *

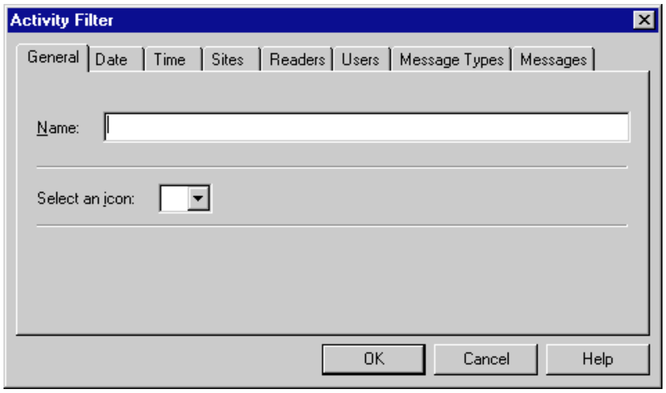
Condition Screens for Creating Custom Activity Views/Reports

When you create an activity filter (that is, a custom view of your activity; see page 104), or when you design a custom activity report (see page 105), you see the screen shown below.

Each tab is initially set up to include all information; you only need to go to those tabs where you want to limit or filter out particular information. For example, if you only want activity at certain readers, you would go to the *Readers* tab. If you only want certain messages, you would go to the *Messages* tab.

General

This screen contains the name and icon associated with activity filter or report.



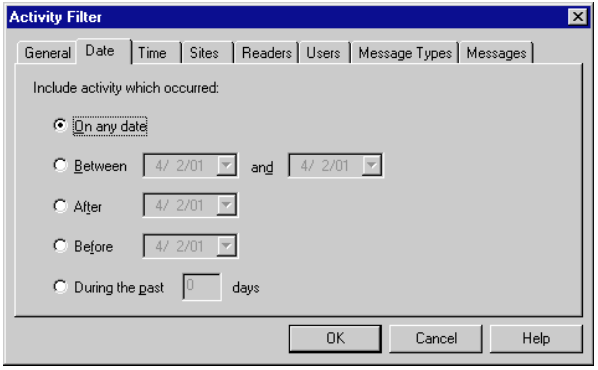
Name: Enter a name that describes the conditions that determine what activity will be included.

Icon: If you want an icon associated with the this activity view/report, click the this entry. You do not have to choose an icon if you do not want to. If you do not want an icon, do not pick an icon; once you pick one, you cannot go back to having no icon.

Do not click *OK* until you have gone to the other tabs and set up those conditions that limit the activity.

Date

This screen lets you limit the activity you see to certain dates.



Include activity which occurred:

● On any date

○ Between 4/ 2/01 and 4/ 2/01

○ After 4/ 2/01

○ Before 4/ 2/01

○ During the past 0 days

On any date: This includes activity from any date that is in the activity file. This is always the initial choice when you create a new report or activity filter.

Between: This includes any activity between the dates entered or on those dates. For example, if you chose *Between 05/01/01 and 05/31/01*, activity from both 05/01 and 05/31 would be included along with the activity in between.

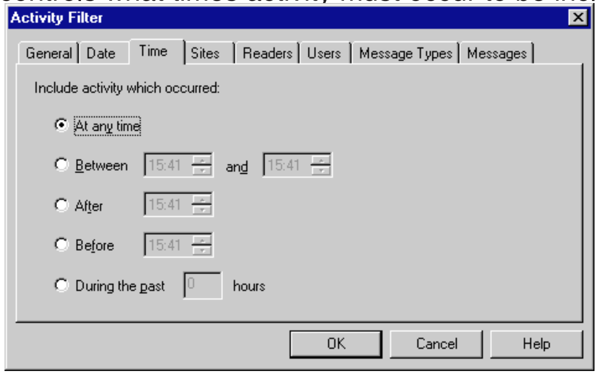
After: This includes activity that is after the date that you enter, but not activity that is on or before that date. For example, if you enter *05/01/01*, you would see activity from 05/02 on, but activity on 05/01 would not be included (if you want the activity from 05/01, you would have to enter *After 04/30*).

Before: This includes activity that is before the date that you enter, but not activity that is on or after that date. For example, if you enter *04/30/01*, you would see activity from 04/29 and before, but activity from 04/30 would not be included (if you want the activity from 04/30, you would have to enter *Before 05/01*).

During the past: This is useful for creating a view that lists only the most recent activity. For example, you might create a view that only listed activity during the past week. If you want to be more precise, this same option is on the *Time* screen so that you could, for example, limit a view to the last twenty-four hours.

Time

This screen controls what times activity must occur to be included.



Include activity which occurred:

● At any time

○ Between 15:41 and 15:41

○ After 15:41

○ Before 15:41

○ During the past 0 hours

On any time: This includes activity from any time. This is always the initial choice when you create a new report or activity filter.

Between: This includes any activity between the times entered or exactly at those times. For example, if you chose *Between 12:00 and 13:00*, activity that happened at exactly 12:00 or 1:00, PM along with the activity in between would be included. This goes from the earliest time to the latest time, regardless of which you enter first. For example, if you enter *Between 17:00 and 8:00* (hoping to get activity that was not during normal business hours), you would get the same activity as if you had entered *Between 8:00 and 17:00* (that is, activity that occurred during normal business hours). If you really want activity that is after 5:00 PM and before 8:00 AM, you would have to create two filters: one looking for activity after 17:00 and the other looking for activity before 8:00.

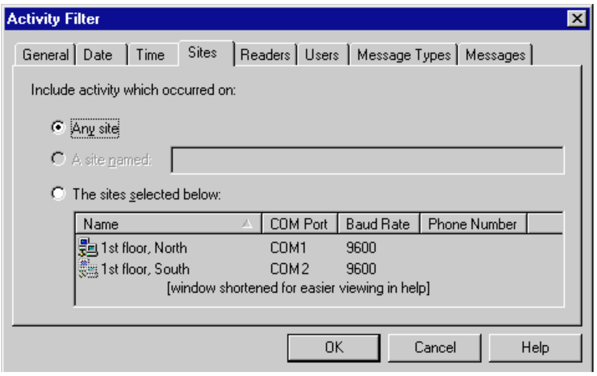
After: This includes activity that is after the time that you enter, but not activity that is exactly at that time. For example, if you enter 12:00, you would see activity from 12:00:01 (that is one second after 12) on, but activity at 12:00:00 or before would not be included.

Before: This includes activity that is before the time that you enter, but not activity that is exactly at that time. For example, if you enter 12:00, you would see activity from 11:59:59 (that is one second before 12:00) on, but activity at 12:00:00 or after would not be included.

During the past: This is useful for creating a view that lists only the most recent activity. For example, you might create a view that only listed activity during the past twenty-four or forty-eight hours (for longer periods, this same option is on the *Date* screen so that you could, for example, limit a view to the past thirty days).

Sites

This screen lets you limit the activity to certain sites.



Include activity which occurred on:

● Any site

○ A site named:

○ The sites selected below:

Name	COM Port	Baud Rate	Phone Number
1st floor, North	COM1	9600	
1st floor, South	COM2	9600	

[window shortened for easier viewing in help]

Any site: Leave this selected to not limit the activity based on site.

A site named: This option is permanently disabled. To get activity for a single site, use the following option and only click one site in the list.

The sites selected below: To limit the report/view to specific sites, click this and then select the sites to include activity from.

To select a single site: Click that site in the list.

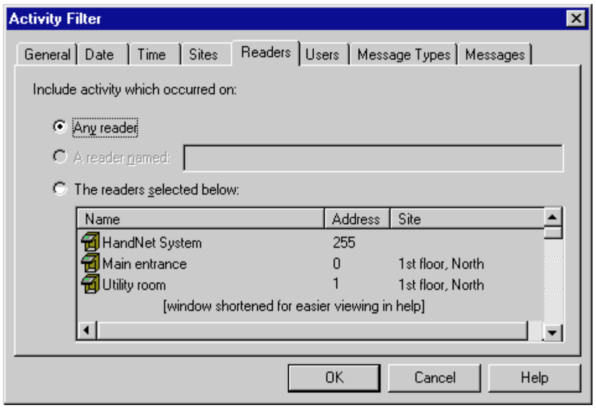
To select multiple sites that are together on the list: Click the first site in the group, hold the *SHIFT* key down, and with the *SHIFT* key down, click the last site that you want to select.

To select multiple sites that are not together on the list: Click the first site to select, hold the *CTRL* key down, and click each other site that you want to select.

If you select specific sites here, make sure you do not select readers from different sites on the *Reader* tab; if you select sites here and select readers from different sites, you will not see any activity with this filter. If you want to select specific readers, select *Any site* on this screen.

Readers

This tab lets you limit to activity that occurred at certain readers. For example, you might want to limit activity only to the readers controlling the entrances to the building so you could see who has come in. Or you might want to limit activity to the readers controlling the most secure areas so you could monitor them more closely.



Include activity which occurred on:

● Any reader

○ A reader named:

○ The readers selected below:

Name	Address	Site
HandNet System	255	
Main entrance	0	1st floor, North
Utility room	1	1st floor, North

[window shortened for easier viewing in help]

Any reader: Leave this selected to not limit the activity based on site.

A reader named: This option is permanently disabled. To get activity for a single reader, use the following option and select only that one reader in the list.

The readers selected below: To limit the report/view to specific readers, click this and then select the readers to include activity from.

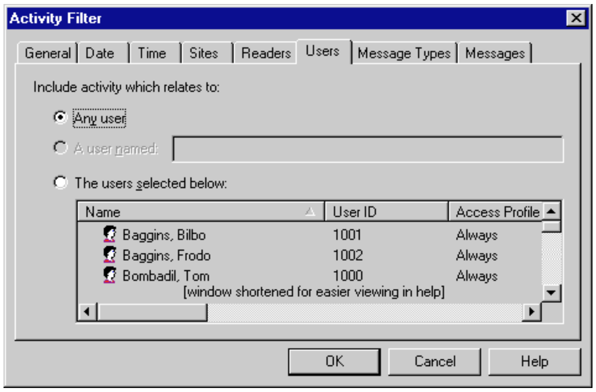
To select a single reader: Click that reader in the list.

To select multiple readers that are together on the list: Click the first reader in the group, hold the *SHIFT* key down, and click the last reader that you want to select.

To select multiple readers that are not together on the list: Click the first reader to select, hold the *CTRL* key down, and click each other reader that you want to select.

Users

This screen lets you limit to activity that occurred for certain users.



Include activity which relates to:

● Any user

○ A user named:

○ The users selected below:

Name	User ID	Access Profile
Baggins, Bilbo	1001	Always
Baggins, Frodo	1002	Always
Bombadil, Tom	1000	Always

[window shortened for easier viewing in help]

Any user: Leave this selected to not limit the activity to particular users.

A user named: This option is permanently disabled. For a single user, use the following option and select only that one user in the list.

The readers selected below: To limit the report/view to specific users, click this and then select the users to include activity for.

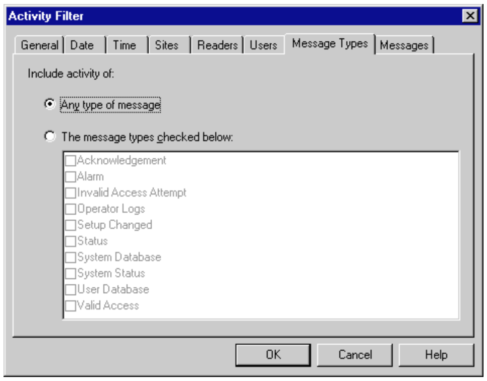
To select a single user: Click that user in the list.

To select multiple users that are together on the list: Click the first user in the group, hold the *SHIFT* key down, and click the last user that you want to select.

To select multiple users that are not together on the list: Click the first user to select, hold the *CTRL* key down, and click each other user that you want to select.

Message Types

This screen lets you limit the activity included to particular kinds of messages. If you need only specific messages within a category, use the *Messages* tab instead.



Include activity of:

● Any type of message

○ The message types checked below:

□ Acknowledgement
□ Alarm
□ Invalid Access Attempt
□ Operator Logs
□ Setup Changed
□ Status
□ System Database
□ System Status
□ User Database
□ Valid Access

Any message: This includes activity regardless of what type of message it generates.

The messages types checked below: Click this and then check any message type to include. You can check more than one box to include multiple types of messages.

Acknowledgement: This does not list anything.

Alarm: This lists any message that generates an alarm. Which messages generate alarms is controlled by your choices on the *Alarms* tab in *System Settings*. If you change which messages generate alarms, messages that did not generate an alarm when they occurred will not be listed, even if they would generate an alarm now.

Invalid Access Attempt: This lists any message where someone tries to get access and cannot. This includes the messages *Identity Unknown, Access Denied, and Access Refused, Time Zone*.

Operator Logs: This lists when operators log in or log out of HandNet, and it lists invalid login attempts. It does not list the addition of new operators or changes to the operator settings; only when each operator uses the system.

Setup Changed: This lists any setup changes made directly using command mode at the reader. For setup changes made through HandNet, use *System Database*.

Status: This lists any messages that tell whether auxiliary input and output is on or off.

System Database: This lists all setting changes made through HandNet. This includes adding or changing sites and readers, changing system settings, changing time zones, holidays and access profiles.

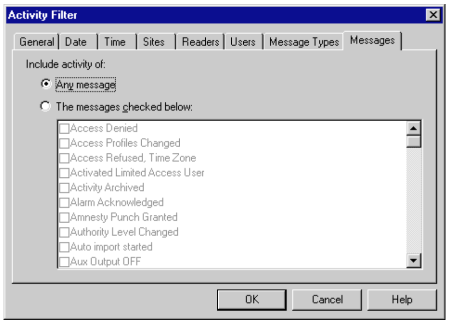
System Status: This lists messages related to when HandNet was started and exited, messages related to enrolling users, messages related to communication problems with readers, and messages related to information being downloaded/uploaded to/from readers.

User Database: This lists messages related to users being added, deleted, or changed. It does not include messages related to users being enrolled or attempted unauthorized enrollments.

Valid Access: This lists *Identity Verified* messages.

Messages

This screen lets you limit the report or activity view to specific messages. For example, if you were trying to track who came into the building, you might select the building entrances on the *Readers* tab, and then choose only the message *Identity Verified* here. Or if you were trying to track access problems, you might limit the output to the messages *Access Denied* or *Identity Unknown*. If you want all of the messages in a particular category, you may find it easier to use the *Message Types* tab instead.



Include activity of:

● Any message

○ The messages checked below:

□ Access Denied
□ Access Profiles Changed
□ Access Refused, Time Zone
□ Activated Limited Access User
□ Activity Archived
□ Alarm Acknowledged
□ Amnesty Punch Granted
□ Authority Level Changed
□ Auto import started
□ Aux Output OFF

Any message: This includes activity regardless of what message it generated.

The messages checked below: Check any message to include. See the list of activity messages starting on page 116 for an explanation of what causes each message. Not all of the messages include what you would expect. For example, the message *Authority Level Changed* does not include users whose authority level was changed on the *Security* screen in *User Properties*; it only includes users whose authority level was changed using the command menus on a reader, which is not how you would typically change a user if you use HandNet. Many of the messages are like this. If you want all of the messages in a particular category, you may find it easier to use the *Message Types* tab instead.

* * * * *

Archiving Past Activity

What Archiving Is

Archiving is moving past activity from the *Current Activity* file to a separate file. This keeps the *Activity* file smaller (and faster) while still keeping the information available for reports if needed. You can set HandNet to remind you to make archives using the *Archives* tab in the *System Settings*; see page 26.

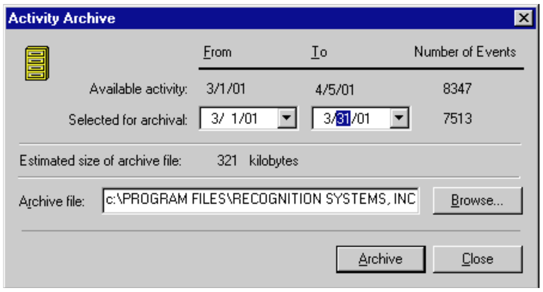
To generate an activity report on activity that is archived, you must indicate that you want to generate the report based on an activity archive (and then pick the appropriate archive).

Effect of Archiving on Reports

When you archive, HandNet removes activity from the current activity file and stores it in a different file. When you generate an activity report, you can use the current activity file OR one of your archive files, but you cannot include activity from more than one file in a single report. This means, for example, that if you make an archive once a month, you cannot generate a single report that looks at the previous year's activity; you would have to generate twelve reports, one for each monthly archive file. If you want an entire year's information in a single report, do not archive until the year is done, so all activity for the year will be in a single file.

Making the Archive

To make an archive of past activity, click the *File* menu and then click *Archive*. You see a screen like this:



Activity Archive

	From	To	Number of Events
Available activity:	3/1/01	4/5/01	8347
Selected for archival:	3/ 1/01	3/31/01	7513

Estimated size of archive file: 321 kilobytes

Archive file: c:\PROGRAM FILES\RECOGNITION SYSTEMS, INC

Available activity: This shows the date of the earliest activity in the activity file and the date of the most recent activity (usually today's date). One the right you will see the total number of events or activities currently in the file.

Selected for archival: This lets you choose the date range to include in the archive. The *From* date is initially set to the date of the earliest activity in the file; you do not normally want to change this date. The *To* date is initially set to today's date; you might sometimes want to make this earlier to keep more activity in the file. For example, suppose you make an archive on the fifth of each month for the previous month. You could change the *To* date to the last day of the previous month so that activity from the beginning of the current month would not be archived yet. Even if you leave the *To* date set to the current date, HandNet may not actually go up to that date: on the *Archives* tab in the *System Settings* there is an entry *Do not archive the latest ___ events*. The archive process keeps at least that many events in the current activity file, even if some of those events are before the date you enter here.

Estimated size of archive file: This is the approximate size that the archive file will be.

Archive file: This lists the name and location of the file that will be created. HandNet uses the location that you have entered for the *Default Archive Directory* on the *Archives* tab in the *System Settings*; see page 27. HandNet names the file using year/month/day hour/minute/seconds. For example *HN Activity Archive 20010406 094542.hna* is the default name for a file made on April 6, 2001 at 9:45 (and 42 seconds) AM. If you sometimes need to generate reports on past activity, and you do not find this naming method very clear, you can change this name. For example, if the archive contained information from the previous month, you might name it something like *Archive March, 2001.hna*. You must keep the .hna extension for HandNet to be able to find the file when you want to generate a report on it.

Once all entries are correct, click the *Archive* button to make the archive.

* * * * *

Exporting Activity

Why Export Activity

If you want to create custom activity reports using some external report tool, *Export Activity* on the *File* menu sends all of your current activity to an Access database file called *expactvt.mdb*. While the main HandNet database files are password protected for security reasons, this file is not, so you can open it (if you have Microsoft Access) and use any information in it. If you are only going to generate reports with *Activity Reports* on the *File* menu, you do not need this option; using it would only create a file that you do not need.

This option only exports current activity, not activity that you have archived, so if you plan to use this option you probably should check the *Export Transactions* box on the *Archive* tab in *System Settings*; see page 27. This causes activity to be automatically exported whenever you archive activity.

You only have access to this option if you have purchased the upgrade to full feature set of Version 2.0.

When you choose *Export Activity*, HandNet pops up a box that tells you how many activity records are going to be exported. Click *OK* to continue.

Avoiding Exporting the Same Information Twice

If you export activity and then export activity again without having archived the activity you exported last time, you will end up with duplicate records in that export file. That is, you will find the same activities listed more than once.

To avoid duplicate activity in the export file you can do one of two things:

- You can export activity and then immediately archive ALL activity. That way, the next time you export activity, the activity that was exported last time will not be in the current activity file, so it will not be exported again.
- If you do not want to archive activity after exporting (you might want to keep more activity in the current activity file so that you could see it in *custom activity* views or create reports that included a longer range of activity), delete or rename the last activity export file (*expactvt.mdb*) before exporting again. If you delete or rename this file, HandNet creates a new *expactvt.mdb* file when you export, and this new file will only contain the information from this export and not what you exported last time.

* * * * *

Activity Messages

You see activity messages in the *Activity* window. You can limit the activity in a custom activity view or in an activity report by checking the corresponding messages on the *Messages* tab in the filter/report design (see page 112). And you can control which messages cause alarms using the *Alarms* tab in the system settings (see page 25).

We have explained the messages in more detail here.

Command Menus in the Reader

Readers have built-in menus that let you change the settings in the reader. Some of the messages below can only occur if you make changes through these menus on the actual readers; you should not typically see these messages. Except for initially setting up the reader to communicate with HandNet, for recalibrating the reader, and for enrolling a user from the reader, you should NOT make changes to the reader through the reader command menus; you should control all other reader settings from within HandNet. See the HandKey manual for more about the reader menus.

Activity Messages

Access Denied: Someone repeatedly entered a valid ID at a reader, and each time the reader did NOT recognize the user's hand (at the reader, the user will see the message *ID Refused*). The number of times that a user can try before getting this message depends on the *Number of Tries* entry on the *Settings* tab in the *Reader Properties*; see page 47. If access is denied for a user, the reader will not accept that ID again until another user has successfully gained access at that reader.

Access Profiles Changed: Someone has changed one or more access profiles. During initial setup, this is a normal message. If you were not expecting access profiles to change, this could be an indication that someone was trying to give inappropriate access.

Access Refused, Time Zone: A valid ID was entered at a reader, but the user is not authorized to have access during the hours or days of the week based on the time zone associated with the reader in the access profile.

Activated Limited Access User: A user was set up with access for a limited date/time range. The computer's date and time matched the date/time the user was scheduled to start having access, so HandNet made the user active and sent the user's information to each appropriate reader so the user could can access; see page 93 for more about limited access.

Activity Archived: The operator used the *Archive* option on the *File* menu; (see page 113 for more on archiving past activity).

Alarm Acknowledged: An alarm occurred, and an operator went to the *Alarm Properties* screen and clicked one of the acknowledge buttons (following the message on the activity or alarm list, you will see *:ACK* followed by the name of the operator who acknowledged the alarm and when it was acknowledged); see page 103 for more on acknowledging alarms.

Amnesty Punch Granted: You should not see this message.

Authority Level Changed: A user's authority level was changed from the reader's command menu (typically you would change a user's authority

level from the *Security* tab in the *User Properties*; if you change the authority level there, you just see the message *User Record Changed*).

Auto Import Started: An *import.mdb* file (which contains users to import) was found, and HandNet was set up to automatically import users, so HandNet started importing them. Whether HandNet automatically imports users is controlled by the *Enable* box under *Auto Import* on the *User Import/Export* tab in *System Settings*; see page 28.

Aux Output OFF: The auxiliary output has been turned off.

Aux Unlock Via Wiegand Keypad: The auxiliary output has been turned on by a valid ID number at a remote keypad.

Auxiliary Input ON: The auxiliary input on the reader has been activated.

Auxiliary Output ON: The reader has turned on an auxiliary device (like an alarm) that is connected to the reader.

Auxiliary Output Setup Changed: The timing and clearing of an auxiliary output activation has been changed.

Baud Rate Changed: The communications baud rate has been changed using the command menus at the reader.

Command Mode Entered: Someone entered the command mode at a reader. Readers have built in menus that let you change the reader settings. These command menus are mainly needed when someone is using the readers without the HandNet program; HandNet controls most settings in the reader for you. The only tasks you should need to do through the reader command menus are setting up the reader's address and communication settings during initial setup, recalibrating the reader, and enrolling users at the reader if you are not using the *Enroll* option on the *Reader* menu.

Data Base Restored: You should not see this message.

Data Base Saved: You should not see this message.

Data Downloaded to Reader: Someone used one of the *Download* options on the *Reader* menu to send information to the reader; see page 60. Unless there was some problem with the reader that is being corrected, this is not usually necessary; HandNet usually automatically sends all information to the reader that the reader needs.

Data Log Buffer Empty: You should not see this message.

Deactivating Limited Access User: A user was set up with access for a limited date/time range. The computer's date and time matched the date/time the user's access was supposed to end, so HandNet made the user inactive and sent the appropriate information to readers so the user could no longer gain access, see page 93 for more about limited access.

Door Forced Open: A door was forced open without a valid ID and hand recognition at a reader.

Door Open Too Long: A door was kept open for longer than was allowed

based on the time entered in the *Door Switch Shunt Time* on the *Configuration* tab in the *Reader Properties*; see page 48.

Duress Alarm: A user entered the duress code, a code that indicates that the user is in trouble or that someone is forcing the user to give him/her access; see page 47 for more about duress codes.

Exit Granted: The user is permitted to exit.

Extended Datalog: Someone entered command mode on the reader and changed settings that do not have specific messages associated with them (for example, you get this message if you change the language of the reader's display or the format of the date on the reader).

HandNet Exited: Someone picked *Exit* from the *File* menu to shut HandNet down. Under normal circumstances, HandNet is left running continually so it can monitor activity and immediately process any alarm messages. If someone exited HandNet to install a new Version of the program or to perform maintenance on the computer it is on, there is probably no problem; if someone exited the program at some other point, this could be an indication of an attempt to get around security.

HandNet Started: Someone started the HandNet program. Under normal circumstances, HandNet is usually left running continually so it can monitor activity and immediately process any alarm messages. If someone exited HandNet to install a new Version of the program or to perform maintenance on the computer it is on and then restarted, then there is probably no problem. If you see the message *HandNet Started* but you do not see the message *HandNet Exited* earlier in the list, then someone exited the program and restored an older Version of the activity files; this could be an indication that someone is trying to hide activity.

HandNet+ File Converted: Someone used *Convert HandNet+* on the *File* menu to convert users from HandNet+ into HandNet for Windows (HandNet+ was an MS-DOS predecessor to HandNet for Windows); see page 98 for more on converting users from MS-DOS Versions of HandNet.

Holiday Table Changed: Someone has added, changed, or deleted a holiday with the *Holidays* option; see page 65 for more about setting up holidays.

Identity Unknown: Someone entered a valid ID at a reader, but the reader did not recognize the user's hand.

Identity Verified: At a reader, a user entered a valid ID and the reader recognized the user's hand and gave access.

Invalid Operator Login Attempt: Someone tried to log into HandNet but entered an invalid user name or password. This could occur if someone just typed the name or password incorrectly, or it could mean that an unauthorized person was trying to get into the program.

Leave Command Mode: Someone exited or left command mode at a reader. Readers have built-in menus that let you change the reader settings. These command menus are mainly needed when someone is using the readers without the HandNet program; HandNet controls most settings in the reader for you. The only tasks you should need to do through the reader command

menus are setting up the reader's address and communication settings during initial setup, recalibrating the reader, and enrolling users at the reader if you are not using the *Enroll* option on the *Reader* menu.

Lock Output OFF: Someone chose *Relock* from the *Reader* menu to relock an unlocked door; see page 128 for more about locking and unlocking doors.

Lock Output ON: Someone chose to unlock a door using one of the *Unlock* options on the *Reader* menu; see page 128 for more about locking and unlocking doors.

Lock Setup Changed: Using the command menus in the reader, someone changed the number of seconds the lock should be unlocked for or the number of seconds the door is allowed to be open (normally this is changed in HandNet on the *Configuration* tab in *Reader Properties*; if it is changed there, you just see the message *Reader Properties Changed*).

Manual Import Started: The operator selected *Import Users* to import users from the *import.mdb* file; see page 99 for more about importing users (when you must import users manually or whether HandNet imports them automatically is controlled by the *Enable* box under *Auto Import* on the *User Import/Export* tab in *System Settings*; see page 28).

Maximum ID Length Changed: Someone changed the maximum length for a user ID using the command menus in the reader (if you changed the ID length on the *Settings* tab in the *Reader Properties*, you would just see the message *Reader Properties Changed*).

Memory Cleared: Someone used the *Clear Memory* option from the *Command* menus in the reader. This erases all the users from the reader (typically you would do this if you were changing the use of the reader and wanted to make sure that those who previously had access through this reader no longer had access through it).

Messages Read: You should not see this message.

No Hand Read For Card: You should not see this message.

Operating Mode Changed: The operating mode of the reader has been changed using the command menus in the reader.

Operator Added: A new operator (someone authorized to use HandNet) was added on the *Operators* tab in *System Settings*; see page 24 for more about adding operators.

Operator Deleted: An operator (someone authorized to use HandNet) was removed from the *Operators* tab in *System Settings*; see page 24 for more about deleting operators.

Operator Login: An operator logged into HandNet.

Operator Logout: An operator logged out of HandNet.

Operator Properties Changed: Someone changed the tasks that an operator is allowed to do on the *Operators* tab in *System Settings*; see page 24 for more about controlling which options an operator can use.

Output Mode Changed: The output mode of lock output or card reader emulation has been changed using the *Command* menus in the reader.

Passwords Changed: Someone changed the passwords for the reader *Command* menus, using the command menus in the reader. Generally this setting is controlled from HandNet on the *Passwords* tab in *Reader Properties* rather than from the reader (if you change this or other settings for the reader in HandNet, you just see the message *Reader Properties Changed*).

Printer Setup Changed: If a serial printer is attached to the reader, the printer settings have been changed using the command menus in the reader.

Reader Action Failed: HandNet was unable to complete a communication attempt with the reader. This could be an indication that the connection to the reader is not set up correctly; see the *Troubleshooting* resolving this error.

Reader Added: A reader was added to HandNet.

Reader Connection Failed: HandNet was not able to establish communications with the reader. This could be an indication that the connection to the reader is not set up correctly; see *Troubleshooting* resolving this error.

Reader Connection Timeout: HandNet lost its connection with the reader. This could be an indication that the connection to the reader is not set up correctly; see the troubleshooting for help resolving this error.

Reader Data Uploaded to HandNet: Someone used *Upload Users* on the *Reader* menu to get user information from the reader; see *Getting User Information from a Reader* on page 99.

Reader Deleted: A reader was deleted from HandNet.

Reader Properties Changed: Someone went to the *Reader Properties* and changed the settings on one of the tabs there. HandNet does not keep track of which settings were changed. For more about *Reader Properties*, see page 45.

Record Imported for Creation: An new user was added to HandNet by the import process.

Record Imported for Deletion: A user that was already in HandNet was deleted based on information in the *Import* file.

Record Imported for Modification: A user that was already in HandNet was changed to match a user with the same ID in the *Import* file.

Record Imported, Empty Template Overwrote Local Enrollment: A user that was not enrolled was imported. This replaced an enrolled user, so the user is not longer enrolled in HandNet. You can prevent enrolled users by being replace by either preventing the exporting computer from exporting users that are not enrolled yet, or by changing the import settings so non-enrolled users cannot replace enrolled ones; see the explanation for the *Import/ Export* settings on page 28.

Reject Override Changed: Someone changed the reject threshold for an individual user using the command menus in the reader. Generally this setting is controlled in HandNet with the *Override* setting on the *Security* screen in *User Properties*; HandNet users would not typically change this at the reader (if you change this or other user settings in HandNet, you just see the message *User Properties Changed*).

Reject Threshold Set: Someone changed the reject threshold using the command menus in the reader. Generally this setting is controlled from HandNet using *Reject Threshold* on the *Configuration* tab in *Reader Properties* rather than from the reader (if you change this or other settings for the reader in HandNet, you just see the message *Reader Properties Changed*).

Remote Enrollment Started: A user was enrolled with the *Enroll* option on the *Reader* menu (for users enrolled from the *Command* menu on the reader, you see the message *User Enrolled*); see page 87 for more about enrolling users.

Report Engine Unavailable: You should never see this message.

Request to Exit Activated: A user has pressed the *Request to Exit* button in order to get out of the secure area.

Score Is: You should never see this message.

Site Added: A site was added to HandNet.

Site Code Changed: The site code was changed using the *Command* menus in the reader.

Site Connected: HandNet is set up to connect with the site by modem, and HandNet connected to the site.

Site Deleted: A site was deleted in HandNet.

Site Disconnected: HandNet is set up to connect with the site by modem, and HandNet disconnected from the site when it was done communicating with the site.

Site Properties Changed: In HandNet, one or more changes were made to the *Site Properties*; for more about *Site Properties*, see page 34.

Special Enrollment: The *Command* menus in the reader was used to enroll a user who does not require hand recognition to gain access.

Supervisor Override: You should not see this message.

System Re-calibrated: Someone recalibrated the reader; see page 124.

System Settings Changed: Someone changed one or more entries on one of the *System Settings* tabs that you get to with settings on the *View* menu; for more about system settings, see page 22.

Tamper Activated: Someone has shaken the reader roughly or has opened the reader. Unless someone was servicing the reader, this message generally

warrants further investigation.

Time and Date Set: Someone changed the time and date in the reader using the command menus in the reader (generally, rather than changing date and time in the reader, you would just make sure that the date and time were correct in the computer and then send the date and time to the reader using *Download Time* on the *Reader* menu).

Time Restrictions Turned On/Off For All Users: You should not see this message.

Time Zone Data Changed: Someone changed a time zone using the *Command* menus in the reader. Generally this setting is controlled with the *Time Zone* settings in HandNet and not changed at the reader (if you change time zones in HandNet, you see the message *Time Zones Changed*).

Time Zones Changed: In HandNet, someone changed *Time Zones*; see page 61 for more on setting up *Time Zones*.

Two Man Timeout: Two people were required to verify at the reader, and they have not done so within the permitted time period.

Unable to Close Communications Port: HandNet was unable to close the *Serial Communications* port.

Unable to Install Communications Port or Unable to Open Communications Port: You get this message if HandNet tries to establish communication with a reader through a serial port and it cannot. Generally this only happens if you are running another program that is already controlling that serial port. You cannot have two different devices connected to the same port, so if a reader really is connected to that port, nothing else should be. Either you have selected the wrong port on the *Connection* tab in the *Site Properties*, or the other program that you are running has the wrong port selected. If you were previously running another program (especially one trying to connect to a modem, fax, or printer), it is possible that the other program tried to use the port and did not close it properly. Make sure that other programs that might try to control the port are closed. If the problem still exists, trying shutting everything down and restarting the computer.

Unable to Retrieve Datalog: An attempt to get information from the reader failed.

Unauthorized Enrollment Attempted: Someone tried to enroll a user at a reader and the user had not been added to HandNet yet. Your settings do not allow this (to change your settings so this is allowed, check the box by *Do not delete unauthorized enrollments* on the *Security* tab in *System Settings*; see page 23).

Unit Address Changed: Someone changed the address of the reader using the command menus in the reader.

User Added From Card: You should not see this message.

User Database Field Added: Someone went to the *Custom* tab in the *User*

Database properties and added a new custom entry; see page 97.

User Database Field Deleted: Someone went to the *Custom* tab in the *User Database* properties and removed a custom entry.

User Database Import Finished: The process of importing users (from the *import.mdb* file) is done.

User Enrolled: A user was enrolled using the command menu on the reader (for users enrolled with the *Enroll* option on the *Reader* menu, you see the message *Remote Enrollment Started*); see page 87 for more about enrolling users.

User Record Added: A user was added in HandNet.

User Record Changed: *User Properties* were changed for a user in HandNet. The change could be on any of the three tabs of user information; see page 90 for more on user properties.

User Record Deleted: A user was deleted in HandNet.

User Removed: A user was removed using the command menus in the reader. A user who was removed in this way is only removed from that one reader; the user is not removed from HandNet or from any other reader. If you ever download users to a reader, the user will be added to the reader again if the user is still in HandNet (to remove a user from HandNet, click the user on the list of users and press the *DEL* key. Removing a user from HandNet generates the message *User Record Deleted*).

Users Listed: Someone listed users using the command menus in the reader (if you want a list of users, its generally much easier to just look at the list of users in HandNet or to print the *Users* report; see page 13).

Users Time Zone Changed: When a user can access the reader was changed from the command menus in the reader (typically, this is not changed at the reader; you would instead change the user's access profile on the *Security* tab in *User Properties* to change when the user has access to particular readers. If you did this, you would see the message *User Properties Changed*).

* * * * *

Other Ongoing Activities

Reader Maintenance

Cleaning Readers

You should periodically clean hand readers; if you do not, users may get rejected more often.

Spray any ordinary, non-abrasive cleaner on a clean cloth, and then use the cloth to wipe the platen, the mirror and reflector on the sides of reader, and the window above the platen. When wiping the platen, start from the back corners and wipe forward.

Never spray cleaning fluid directly onto the reader! Always spray a cloth and then wipe the reader with the cloth.

Never use an abrasive or gritty cleaner! An abrasive cleaner could scratch the reader; this would damage it.

Recalibrating Readers

If users are often being rejected at a particular reader, try recalibrating it. To do this:

1. Check the list of users to make sure you have an authority level of one or higher. If you have an authority level of *None*, you cannot do this (to change your authority level, double-click your name on the list of users, click the *Security* tab, click the *Authority Level* entry, and select the appropriate level).

2. Go to the reader to be recalibrated, and enter command mode on the reader:

   If you have a HandKey II or HandKey CR reader: Press *CLEAR*, and then press *ENTER*.

   If you have an ID3D HandKey reader: Press *#* AND *** (you can press them at the same time, or one after the other).

   The display on the reader should look like this:

```
      READY
   * :
```

3. Type your *User ID* number (the same one you enter to get access through the reader), and press *ENTER* or *#.* The reader asks you to place your

```
ENTER PASSWORD
```

hand. Once it recognizes your hand, this display looks like this:

4. Type *1* and press *ENTER* or *#* (this is the standard password for the *Service* menu in the reader; if you have changed this on the *Passwords* screen in the *Reader Properties*, enter the password you have set up). The display should now look like this:

```
  CALIBRATE
* NO     YES #
```

If the reader shows the *READY* screen again instead of this screen, either you placed your hand improperly or you do not have the rights to do this; carefully check step one again.

5. Press the *YES/#* button. This display should now look something like this:

```
  r0  c0  e100  s
RECAL  (Y#/N*)?:
```

(The actual numbers on the first line may be different).

6. Press the *YES/#* button again. After telling you to please wait, you will see the *Calibrate No/Yes* display again. At this point, the reader should be recalibrated.

7. Press the *CLEAR* button to leave the *Service* menu and return to the reader to its normal display.

* * * * *

Making Backups

Why Make Backups

Occasionally computer hard drives fail, losing the information on them. Occasionally computer files get damaged, making the information in them unusable. And occasionally computer users make mistakes and delete information they should not. A backup is an extra copy of the information on your computer, so that if the information gets damaged or lost, you have another copy to protect you.

The information in HandNet—information about readers, access profiles, and users—represents many hours of work. The record of activity (including archived historical activity) is often an important security record. So you should protect your many hours of work by periodically making a backup copy of this information.

Making Backups a Scheduled Event

In practice, many computer users understand that backups are important, but they still go months or even years without actually making one. Then, when a problem occurs, the backup they have is so old that it does not save them all that much work. The way to avoid this is to make backing up your information a scheduled part of your routine. How often you need to make them depends on how many changes to the information you make. If you are continually adding and removing users, a weekly backup might be appropriate. If you make fewer changes and losing a month's changes would not be that hard to redo, a monthly backup might be enough. Regardless, decide how often to make a backup, and then put it on your calendar; do it every Friday morning, or every month before you print your activity reports. If you do not schedule backups, they probably will not happen. And if you do not make them, sooner or later most computer users regret it.

How to Make a Backup of Your HandNet Information

You should periodically be making backups of all the information on your computer. How to best do that is beyond the scope of these instructions. Here, we will just tell you how to make a backup of your HandNet information.

1. Use *Windows Explorer* to go to the folder HandNet is in (if you installed HandNet in the standard location, it is in *C:\Program Files\Schlage Biometrics, Inc\HandNet for Windows*).

2. Make a copy of all of the Microsoft Access Database files (**.MDB*) and all of the HandNet Activity Archive files (**.HNA*) in this directory. You can copy these files to a floppy disk or to a network drive. If the files are large, WinZip is a helpful and inexpensive utility that lets you both compress a number of files into a single archive and spread the archive over a number of disks if needed (to get WinZip, go to *www.winzip.com*. For help making an archive span several floppy disks, look up "spanning" in the index of WinZip's help).

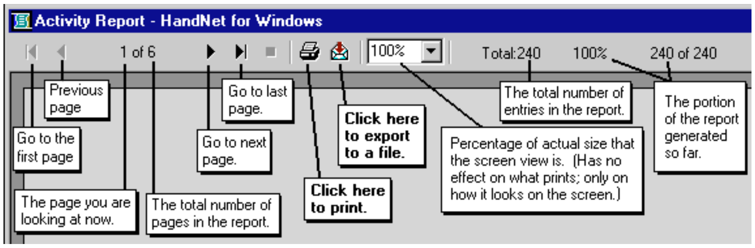
The best protection is to store the backup disks in a different place than the computer. That way, if the computer is damaged by fire or water, or if the computer equipment is stolen, there is no chance of the backup disks being damaged or taken.

* * * * *

Reporting and Exporting Information

Printing or Viewing Reports

Whenever you generate a report, HandNet shows the report in a new window. The header of that window lets you move from page to page, print the report, or export the report to a file. The header looks like this:


Activity Report - HandNet for Windows
1 of 6
100%
Total:240
100%
240 of 240
Previous page
Go to the first page
The page you are looking at now.
The total number of pages in the report.
Go to last page.
Go to next page.
Click here to export to a file.
Click here to print.
The total number of entries in the report.
Percentage of actual size that the screen view is. (Has no effect on what prints; only on how it looks on the screen.)
The portion of the report generated so far.

To print the report: Click the printer icon near the middle of the header to print the report.

If the printer icon is disabled and grayed out, you do not have a printer set up yet on this computer (to set up a printer, go to the Windows *Start* menu, highlight *Settings*, pick *Printers*, and click *Add Printer*).

To export the report to a file: Click the icon with the envelope. You can export to a variety of formats including Word, Excel, Lotus 1-2-3, ...rtf, text, and others.

To close the report window when done: Click the *X* in the upper-right corner of the window.

Getting Information from HandNet Database Files

HandNet for Windows stores information in access database files (*actions.mdb, activity.mdb,* and *HandNet.mdb*). These files are password-protected for security; we do NOT ever give these passwords out for any reason. If we did, it would put the integrity of your security at risk.

Exporting activity to an access database file

However, HandNet can export activity to an access database file that is not password protected so you can open it and access any information in it at will. If you want to create custom activity reports using some external report tool, *Export Activity* on the *File* menu sends all of your current activity to an access database file called *expactvt.mdb*.

Exporting the content of any report to various formats

To save HandNet information to a file, you can also generate any *Activity Report* or other report on the *Reports* menu and, when you see the report on the screen, click the *Export* button.

You will then be able to save the content of the report in a number of different formats so you can import it into other programs. These formats include: character-separated values, comma-separated values, Crystal Reports, Data Interchange Format (DIF), Excel (Versions 5.0, 7.0, or 8.0; either extended or not), Lotus 1-2-3 (WK1, WK3, or WKS), Access 97 database, paginated text, record style (columns of values(report definition, Rich Text Format (RTF), tab-separated, text, or Word for Windows)).

* * * * *

Locking and Unlocking Doors

Automatically Unlocking a Door on a Scheduled Basis

If you regularly want a door unlocked during certain hours:

1. If you have not already done so, set up a time zone that corresponds to the days and times you want the door unlocked.
2. Select the reader(s) in the list of readers.
3. Pick *Reader* from the main menu, and then pick *Properties* from the *Reader* menu.
4. Go to the *Configuration* tab.
5. In the *Auto Unlock Time Zone*, choose the time zone when the door should be automatically unlocked. HandNet automatically unlocks the door at the beginning of the time zone, and locks it again at the end of the time zone.

Unlocking a Door on a Non-Scheduled Basis

Unlock on the *Reader* menu lets you unlock a door without setting it up to be regularly unlocked.

1. Select the reader(s) in the list of readers.
2. Pick *Reader* from the main menu, and highlight *Unlock* on the *Reader* menu. You will see another menu with two choices: *Indefinite* and *Timed*.

   To unlock a door so that it stays unlocked until you lock it again: Choose *Indefinite*. This leaves the door unlocked until you lock it again with *Relock* on the *Reader* menu.

   To unlock the door momentarily: Choose *Timed*. This unlocks the door connected to that reader only for the number of seconds specified in *Lock Open For* on the *Configuration* tab in the *Reader Properties* (that is, it unlocks the door for the same number of seconds that the door would be unlocked if it were opened by a reader).

Locking a Door so it cannot be Opened from the Reader

Lockup on the *Reader* menu disables the lock on the door for the selected reader. The reader will still let users enter their ID numbers and still verify hands, but the door will stay locked and will not open even for valid users. No one will be able to open the door from the reader until you choose *Unlock* or *Relock* from the *Reader* menu.

Locking an Unlocked Door

If you have unlocked a door with *Unlock, Indefinite* on the *Reader* menu, *Relock* locks it again (if you unlocked the door using *Unlock, Timed* on the *Reader* menu, the door automatically relocks after the number of seconds specified in *Lock Open For* on the *Configuration* tab in the *Reader Properties* just as it would if the door were unlocked by the reader, so you do not have to anything special to relock it).

If you have disabled access through a door with *Lockup* on the *Reader* menu, *Relock* releases so the reader can open it again.

* * * * *

Turning an Auxiliary Device On or Off

HandNet can be set up to automatically turn on external auxiliary devices when certain conditions occur. For example, it might trigger an alarm, turn on lights or a security camera, and so on.

HandNet can turn an auxiliary device on automatically when certain conditions occur. When this can happen is controlled by the *Auxiliary (AUX) Settings* tab; see page 48 (the HandKey II and HandKey CR support up to three auxiliary devices; this option only controls the first of these, the same one controlled by the *Auxiliary Settings* tab in *Reader Properties*. The other two are only controlled by the *Extended Settings* tab in *Reader Properties*).

Manually Turning an Auxiliary Device On

Auxiliary Output on the *Reader* menu lets you turn manually turn an auxiliary device on or off without anything happening at the reader. For example, suppose a reader, in addition to being connected to a door, is also connected to an auxiliary light. You could use this option to turn the light on without doing anything at the reader.

To turn on an auxiliary device that is connected to a reader:

1. Click a reader in the right pane of the *Network* window (if the *Network* window is not shown, press *CTRL-N* to open it).

2. Click *Reader* from the main menu bar at the top of the screen.

3. Click *Auxiliary Output* on the *Reader* menu, and then click *On*.

Manually Turning an Auxiliary Device Off

If you have manually turned an auxiliary device on, or if an alarm condition has turned it on, you can also turn the device off from HandNet. For example, suppose an auxiliary alarm is connected to the reader, and suppose the alarm is set to sound for fifteen minutes after the condition occurs. You could use this option to turn the alarm off before the fifteen minutes was done.

To turn off an auxiliary device that is connected to a reader:

1. Click a reader in the right pane of the *Network* window (if the *Network* window is not shown, press *CTRL-N* to open it).

2. Click *Reader* from the main menu bar at the top of the screen.

3. Click *Auxiliary Output* on the *Reader* menu, and then click *Off*.

* * * * *

Troubleshooting

Answers to Common Questions

Enroll Option Disabled

If the *Enroll* option on the *Reader* menu is disabled or grayed out, there are several possible reasons. Check each of the following:

1. Make sure you are logged in. If you are not logged in, you cannot change anything.

2. Make sure that you have selected a reader on the list of readers. Since enrollment has to be done at a reader, you must pick the reader to enroll at before the enroll option will work (to see the list of readers, type *CTRL-N* or pick *Network* from the *View* menu).

3. Pick *About HandNet for Windows...* from the *Help* menu. Check the bottom of the box that pops up. To be able to use the enroll feature, the last line must say *You may use all features of this software.* If this line says *Your current license does not let you use the enroll...,* you must contact your dealer and upgrade your license before you can use this feature (once you upgrade, we will send you an access code that makes the feature available). If you do not upgrade to the full feature set, you must start the enrollment process using the command menus in the reader; see page 87.

4. Check with your supervisor to see if you are authorized to enroll users (for you to be authorized to enroll users, *Reader Data Download* must be checked in the *Access Rights* for the operator in *System Settings*).

No Current Record Message

You get the message *No Current Record* when you start HandNet if you have not added any users yet. This message stops occurring once you add a user; see page 74 and following for help adding users.

Problems Connecting to a Site by Modem

If you are having trouble getting HandNet to connect to a site by modem, check each of the following:

1. Click the site in the left pane of the *Network* window, pick *Properties* from the *Site* menu, and click the *Connection* tab.

2. Make sure you have picked the serial port that the modem is connected to; if this is set to *None*, HandNet will not connect.

3. Make sure the *Baud Rate* in *Site Properties* in HandNet matches the baud rate the reader is set up for. We recommend 9,600 for a HandKey II or HandKey CR and 2400 for a HandKey reader.

4. Make sure the phone number is entered correctly. If you have to dial some digit to get an outside line, enter this digit followed by a comma before the phone number. If the number is a long distance number, make sure you have entered the 1 and the area code as appropriate. For example, if you

have to dial *9* for an outside line, and the number was a long distance call that required by *1* and an area code, you would enter the number like this:

9, 18025551212

5. Make sure the modem is hooked up to a phone line.

6. Make sure the phone line is plugged into the right jack on the modem connected to your computer (most modems have two jacks: one labeled *Line* and one labeled *Phone*. The phone wire from the phone jack on the wall must connect to the jack on the modem labeled *Line*.

7. Make sure the phone line has a dial tone (hook up a regular phone to the modem jack labeled *Phone* to see if you hear a dial tone; if you do not, there is a problem with the jack or phone line).

8. Make sure no other phone, fax machine, or modem is trying to use the same phone line.

9. Make sure call waiting is not on for this line.

10. On the *Schedule* tab in *Site Properties*, make sure you have set up a time for this site to connect. Make sure this connection time is enabled (checked).

Program Claims to be a Demonstration Version

When HandNet for Windows is installed, it is in demonstration mode: it gives you full functionality for fourteen days, and after that it limits the use of certain features.

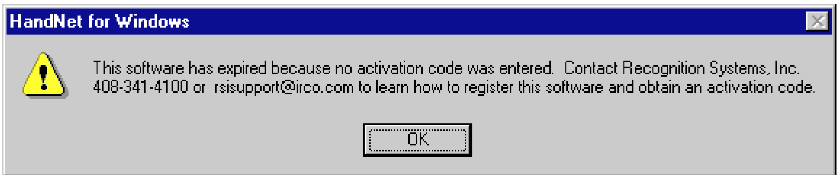
If you purchase a previous Version of HandNet for Windows, you are also authorized to use this Version, but you must register it first, even if you registered your previous Version. Once you send us your registration information, we will give you an authorization code that makes the program permanently functional.

To register this copy of HandNet, please pick *Registration* from the *File* menu and follow the instructions on that screen (we would just repeat the instructions here, but you need the unique ID number that is shown on that screen and you also need to print the registration form).

If you really do have a demonstration Version, please contact us to find out how to purchase a full Version.

Software Expired

After the first time you use this Version of HandNet, you have fourteen days to register it. You must register even if you registered your previous Version of HandNet. If you do not register within fourteen days, you will not be able to log in. When you try to log in, you see this message:



HandNet for Windows

This software has expired because no activation code was entered. Contact Recognition Systems, Inc. 408-341-4100 or rsisupport@irco.com to learn how to register this software and obtain an activation code.

If you get this message, exit HandNet and then restart. This brings up the registration screen. Send us the information requested on that screen. Once we get your information, we will send you an activation code to enter on the registration screen. This will make HandNet permanently functional.

Unable to Acknowledge an Alarm

If you have opened the detail box for an alarm and the *Acknowledge* buttons are disabled or grayed out, check the following:

1. Make sure you are logged in. If you are not logged in, you cannot change anything.

2. Make sure that you are clicking one of the *Acknowledge* buttons at the bottom left of the window; you cannot just click the checkbox by the word acknowledged; you must click one of the buttons.

3. Check with your supervisor to see if you are authorized to acknowledge alarms (for you to be authorized to acknowledge alarms, the *Alarm Acknowledgement* box must be checked in the *Access Rights* for the operator in *System Settings*; see page 24 for more on adding or changing operator settings).

User Often Rejected

If a user is often rejected at readers, you may need to teach the user the correct way to place the hand on the platen; see *Teaching Users How to Place Their Hands on Readers* on page 86.

Creating a new profile of the user's hand

If the user held his/her hand improperly while being enrolled, or if the user has lost or gained a lot of weight, the hand profile may be different enough to prevent recognition. Delete the user (this eliminates the old hand profile), and then add the user again. When you re-enroll the user, this creates a new profile of the hand. Make sure the user correctly places his/her hand. You can usually avoid this situation by allowing HandNet to update the user's hand profile each time the user gains access; see page 23.

If the user has a disability that prevents consistent hand placement

You may need to increase the tolerance for the user. To do this:

1. Double-click the user on the list of users (you could also click once to select the user and then pick *Properties* from the *User* menu).

2. Click the *Security* tab.

3. Check the *Override Reader's Threshold* box if it is not already checked.

4. Drag the pointer to the right (the *Less Sensitive* side).

If many users are rejected at a particular reader

If many users are being rejected at a particular reader, you may need to clean the reader or you may need to recalibrate it; see page 124.

* * * * *

Index

Ingersoll Rand
Security Technologies

Ingersoll Rand's Security Technologies Sector is a leading global provider of products and services that make environments safe, secure, and productive. The Sector's market-leading products include electronic and biometric access control systems; time and attendance and personnel scheduling systems; mechanical locks and portable security, door closures and exit devices, steel doors and frames, architectural hardware and technologies and services for global security markets.

408.341.4110

www.schlage.com www.ingersollrand.com

Schlage
Biometric Solutions
Ingersoll Rand Security Technologies
1520 Dell Avenue
Campbell, CA 95008
Office: 866-861-2480/512-712-1413 (international)
Fax: 866-303-1794/408-341-4111
E-mail: sbssupport@irco.com

P/N HN-MAN Rev. 3.0 10/09

SCHLAGE

HandNet-Lite

Terminal User's Guide

Ingersoll Rand
Security Technologies

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and, if not installed and used in accordance with the Installation Manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at the user's own expense.

This Class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numerique de la classe A respecte toutes les exigences du Reglemente sure le materiel brouilleur du Canada.

Document Part Number: 70100-6210 – Revision 3 – June, 2009

HandPunch is a trademark of Schlage Biometrics, Inc.

The trademarks used in this Manual are the property of the trademark holders. The use of these trademarks in this Manual should not be regarded as infringing upon or affecting the validity of any of these trademarks.

Schlage Biometrics, Inc. reserves the right to change, without notice, product offerings or specifications.

Contents

Getting Started

Introduction

What HandNet Lite Does

HandNet Lite lets you control and monitor many connected FingerKey and/or HandKey readers. In this one program, you can control who can use each reader and when. You can also monitor activity and alarms for all readers at once.

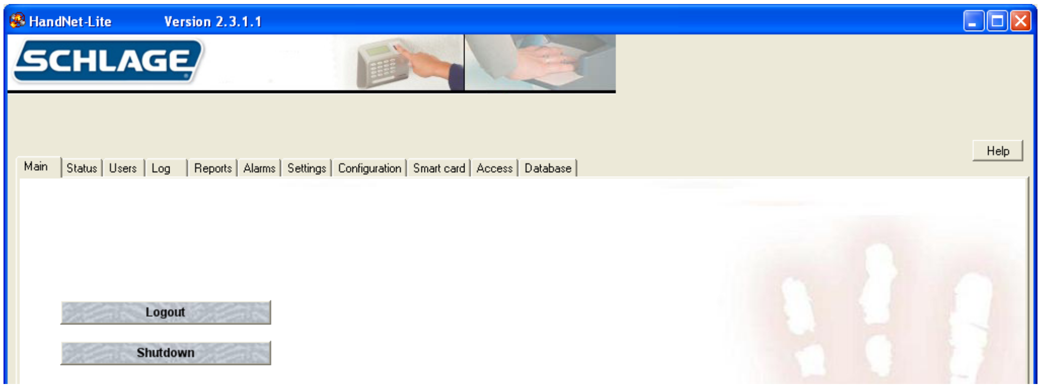
HandNet Lite System Requirements

Operating System: Windows XP SP3, Vista, Windows Server 2003 SP1 or greater, Windows 2000 Professional or Server Editions SP4, and Windows 95 & 98.

Screen Resolution: Screen resolution must be set to at least 1024 x 768; the HandNet Lite window won't fit on your screen if you use a lower resolution. The actual screen size is 1020 x 720, so if your screen resolution is 1024 x 768, your task bar must be on the top or bottom of the screen, and the task bar must be no more than two lines high; if the task bar is three lines or higher or if it is on the side of your screen, part of the HandNet Lite window will run off the screen.

Starting HandNet Lite

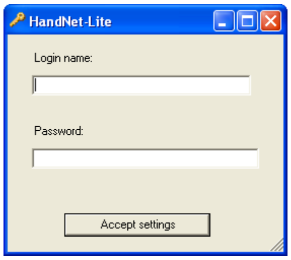
To start HandNet Lite, either double-click the HandNet Lite icon on your Windows desktop or click the Start menu on your Windows taskbar, highlight Programs, highlight Schlage Biometrics, highlight the HandNet Lite folder, and click HandNet Lite. The main window opens.



Logging into HandNet Lite

HandNet Lite requires you to log in before you can make any changes; this prevents unauthorized people from changing information. If you aren’t logged in, you can look at the current status of readers and get on-line help, but you can’t change any information or use any other options.

1. **Click Login on the Main window. You’ll see:**



2. **Type your Login name and Password and click Accept.**

   If this is a new system: Use a Login name of “1234” and a Password of “new.” (After logging in for the first time, you should add one or more new operators. See Managing Operators on page 26 for more information.)

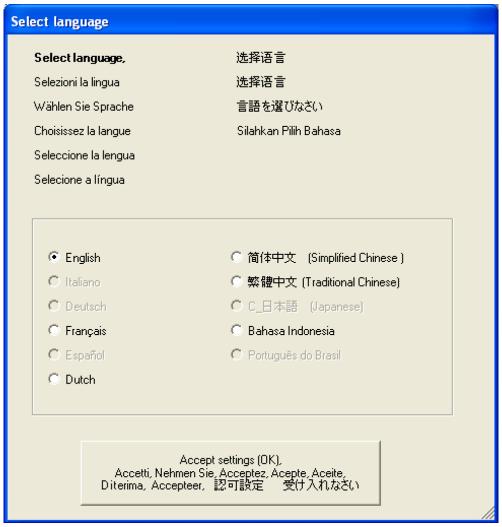
   After initial setup: If you forget your Login name or Password, see your supervisor or security administrator.

   The login name and password are case sensitive. For example, the passwords new, New, and NEW are all different.

After you are done using HandNet Lite, log out so unauthorized people won’t be able to use the program.

Select Language

After HandNet-lite version 2.3 is installed, the first time it is run the following screen will be presented so that the displayed language can be selected. If you do not see the special characters on your computer, use Control Panel, Regional and Language Settings, Advanced tab and select the desired character sets.



● English
○ Italiano
○ Deutsch
○ Français
○ Español
○ Dutch
○ 简体中文 (Simplified Chinese)
○ 繁體中文 (Traditional Chinese)
○ C_日本語 (Japanese)
○ Bahasa Indonesia
○ Português do Brasil

This is the “Select Language” screen. Current language choices are English, French, Dutch, Simplified Chinese, Traditional Chinese, and Bahasa Indonesian.

Getting Help in HandNet Lite

The on-line help has the same information as this manual. To get help in HandNet Lite, click the Help button. Use the contents, index, or search tabs at the left of the help window to find any topic.

For Basic Topics

Click the Contents tab at the top of the left pane, click a book to open, and then click a topic. Not every topic is in the Contents though, so if you don't find what you need, try the Index or Search tabs.

For Groups of Topics on a Single Theme

In addition to the contents you can also click on the pull-down list right under the Previous/Next buttons (in the bottom middle of the header). This list contains a number of important groups of topics. Once you are on one of these topics, the Next and Previous buttons work as well.

Marking a Topic to Return To

In the on-line help, to mark a topic that you want to come back to:

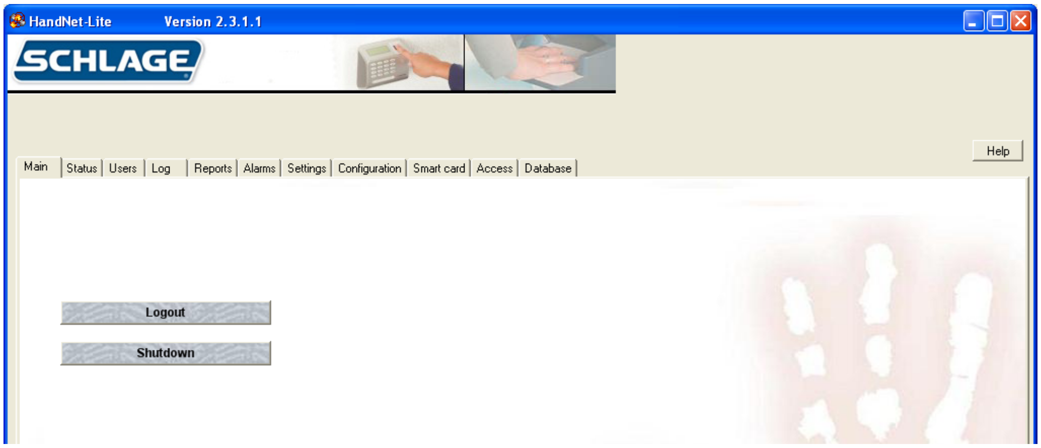
1. Go to the topic that you want to mark.
2. Click the Favorites tab at the top of the left pane.
3. Click the Add button at the bottom of the pane. This adds the topic to your favorites list.

To get back to any marked topic later:

1. Click the Favorites tab at the top of the left pane of the help window.
2. Double-click the topic.

Main HandNet Lite Window

After you log into HandNet Lite, a number of additional tabs appear that let you get to the different parts of the program. Which tabs you see depends on which operator login you used. The screen below shows all of the options.



What You Can Do On Each Tab

Each of the tabs are explained in further detail later in the following chapters.

Status: The Status tab lists every reader in HandNet Lite and the network (group of readers) the reader is connected to. It gives information about each reader and the state of its connection. See page 7 for more information.

Users: The Users tab lists every user that has been added to HandNet Lite, including the user's name, ID, access profile (the group of readers the user has access to), authority level (which reader menus the user can program), and whether the user is enrolled; see page 9. You can add, change, or delete users through the buttons in this tab.

Log: The Log window lists significant events at any connected reader. It doesn't list user accesses, but it lists user additions and enrollment, alarm conditions, and so on. It also lists significant changes made in HandNet Lite. For each event you see the date and time, network and reader, user name and IDs, a brief description of what happened, and an icon showing the type of activity. See page 17 for more information.

Reports: The Reports tab lets you generate reports on all of your users and all of your readers. See page 19 for more information

Alarms: The Alarms tab shows a subset of what you see on the Log tab; this tab lists only those events that are classified as alarm conditions. These generally require immediate attention. See page 23 for more information.

Settings: The Settings tab lets you change HandNet Lite's login name and passwords. It also lets you choose the default Access Profile for users added at a reader, that is, which readers the user has access to. See page 25 for more information.

Configuration: You may add, change, or delete networks and readers. The Configuration tab also allows you to create Wiegand output configurations which can be used for setting FingerKey output. See page 29 for more information.

Smart card: The Smart Card tab is used to manage iCLASS, DESFire and MiFare cards. See page 49 for more information.

Access: The Access tab lets you define access profiles. Access profiles control which readers different groups of people have access through. See page 61 for more information.

Database: The Database Tab is used to backup, restore, delete, detach and attach the database. See page 63 for more information.

Getting Around with the Keyboard

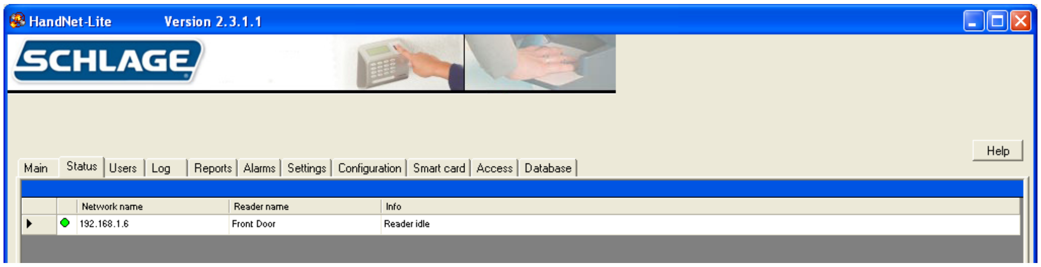
To move from tab to tab: Press ctrl tab.

To move from entry to entry with a tab: Press tab to move to the next entry, and shift tab to move to the previous entry.

Status Tab

The *Status* tab lists every network and reader that has been configured in HandNet Lite.

Figure 4-1: Status Tab



		Network name	Reader name	Info
▸	🟢	192.168.1.6	Front Door	Reader idle

Table 4-1: Reader Status

Column	Description
Status Indicator (untitled)	Indicates the current status of the reader
Network name	Name of the reader's network
Reader name	Name of the reader
Info	Details about the status of the reader's connection

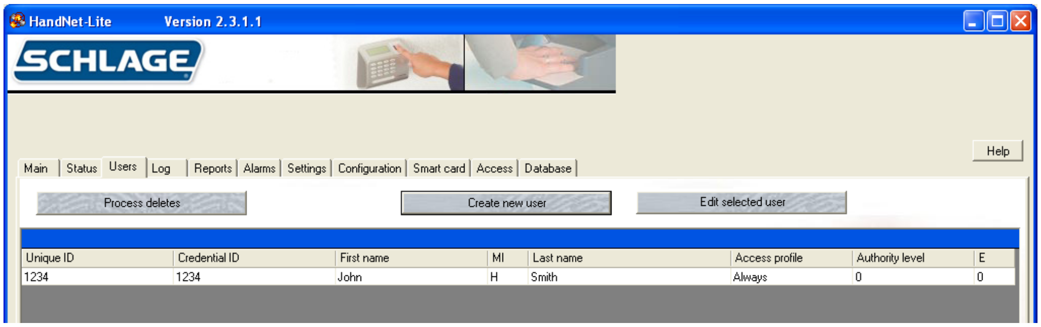
Click the heading of any row to sort the list by that heading. Click the heading again to reverse the sort order.

Table 4-2: Reader Status Indicators

Icon	Description	Additional Information
🟢	Reader is communicating	• Click the green icon to display download and conditionally upload user choices. • If the reader is a FingerKey you will have a Download (Download from PC to the reader) choice. • If the reader is a HandKey you will have both a Download (from the PC to the reader) and Upload (from the reader to the PC) choices.
○	Reader is not enabled	• Readers must be first created (see create new reader) and then enabled (see enable reader).
🔴	Reader is not communicating.	• The reader is not configured correctly, or is disconnected. • Click the red icon for further details.

Users Tab

The *Users* tab lists every user and is used to add or change users. Users are individuals who are enrolled in readers.



Unique ID	Credential ID	First name	MI	Last name	Access profile	Authority level	E
1234	1234	John	H	Smith	Always	0	0

List of Users

Table 5-3: List of Users

Column	Description
Unique ID	ID by which the user is identified in the database
Credential ID	ID the user enters at the reader in order to gain access
First Name	User's first name
MI	User's middle initial
Last Name	User's last name
Access profile	Access profile that is associated with the user (See page 61 for more information.)
Authority Level	• Authority level for the user. • Zero (0) for most users, meaning the user can gain access through the reader, but not use the command menus in the reader to change settings. (See page 14 for more information.)
E	• Indicates enrollment status • Zero (0) indicates that the user is not enrolled. • One (1) indicates that a HandKey template has been captured for the user • Two (2) indicates that a FingerKey template has been captured for the user • Three(3) indicates that HandKey and FingerKey templates have been captured for the user.

Click the heading of any row to sort the list by that heading. Click the heading again to reverse the sort order.

Clicking on a user row will display actions that can be performed for that user.

Enroll Users

Users must be enrolled on a reader. For help enrolling users, see the reader's manual.

A user may be added to HandNet Lite in one of two ways:

- **Enroll the user at a reader before entering the user in HandNet Lite.** If the reader is connected, the user is automatically added to HandNet Lite. If users are enrolled in readers before they are connected to HandNet Lite, when the reader is initially connected to HandNet Lite, all users are imported then.

  If a user is enrolled first, the user ID in the reader (the Credential ID) is used in HandNet Lite for the user's First name, Last name, and Unique ID (an identifier used only by HandNet Lite to help distinguish users with similar names). Edit these entries by selecting the user in the Users window and clicking the Edit selected user button; see Edit Fingerprint Settings page 41.

- **Enter the user in HandNet Lite before enrolling the user in a connected reader.** Enter the user in the User edit window. See Add a User on page 11 for more information. The user will be listed as unenrolled in the Users window (denoted by a zero (0) in column E). See the User Fields table on page 13 for more information. When you enroll the user at a reader, HandNet Lite will import the finer template.

! NOTE *When enrolling users at the reader, you must completely leave the reader's command menus before HandNet Lite will detect the enrollments.*

Problems with User Enrollment

Since bypassing finger or hand recognition gives you reduced security, it should only be used as a last resort. Try these options first:

- The user might have placed the finger or hand badly during the initial enrollment.

  1. Remove the user from the reader.
  2. Instruct the user on correct finger or hand placement. Make sure the user is placing the right finger.
  3. Add the user again.

  This creates a new template for the user.

- If using a FingerKey, Remove the user, and enroll the user again using different fingers. Try the thumb if other fingers don't work

- If the user has a mild disability that prevents consistent finger or hand placement, change the user's reject level. See Biometric threshold on page 13 for more information. See the reader manual for instructions on how to set the appropriate reject setting for the user.

If these options aren't possible, or if you try them and they don't work, then check the Verify on ID only (no biometric verification) box on the User edit screen. See Verify on ID only on page 14 for more information

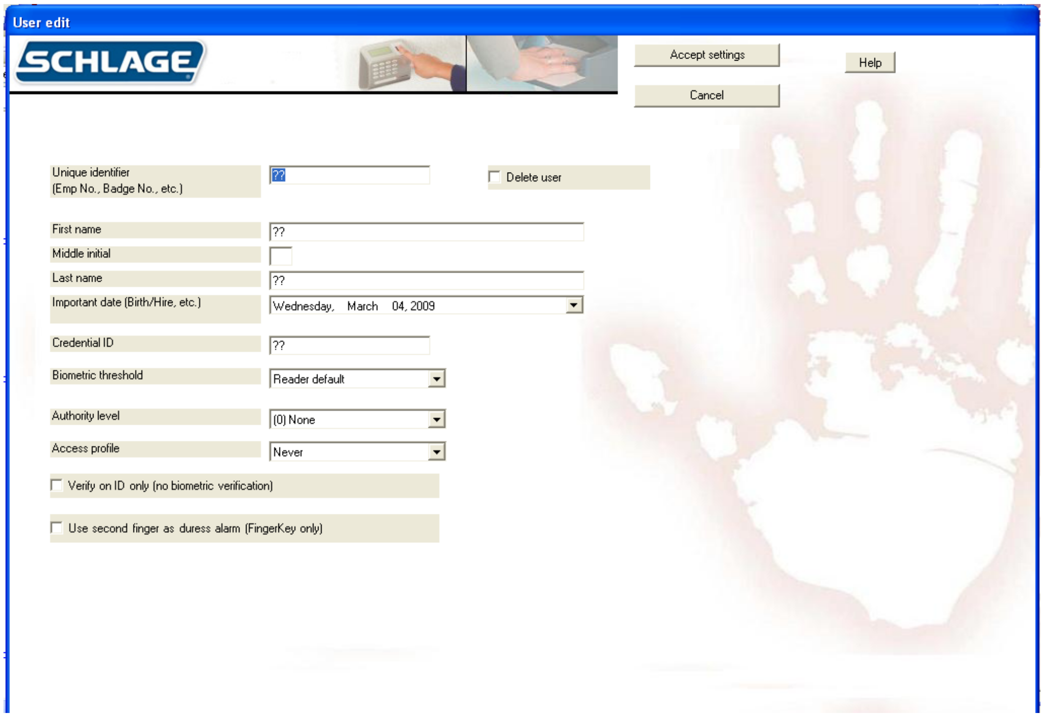
Adding a Special User

When using a FingerKey, if a user's fingerprint cannot be scanned (for any reason), the user can be added as a special user. Special users are still required to place a finger on the scanner, but the scanner does not try to match a finger template.

If a user has unrecognizable fingerprints, severe arthritis, or other conditions that keep the user's finger from being recognized, you can give the user access without finger recognition. If you choose this, the reader still asks the user to place a finger on the reader so it won't be apparent to others that finger recognition isn't required, but the reader doesn't check the finger template; it gives access regardless of whose finger is placed there.

Add a User

1. Click the *Users* tab.
2. Click the *Create new user* button.



Unique identifier (Emp No., Badge No., etc.) ??

☐ Delete user

First name ??

Middle initial

Last name ??

Important date (Birth/Hire, etc.) Wednesday, March 04, 2009

Credential ID ??

Biometric threshold Reader default

Authority level (0) None

Access profile Never

☐ Verify on ID only (no biometric verification)

☐ Use second finger as duress alarm (FingerKey only)

3. Complete the fields on the screen. See the User Fields Table on page 13.
4. Click the *Accept Settings* button.
5. If the user has not been enrolled on a reader, do so now. See Enroll Users on page 10 for more information.

Edit a User

1. Click the *Users* tab.
2. Click to select the name of the user you want to edit.
3. Click the *Edit selected user* button.
4. Complete the fields on the screen. See the User Fields table on page 13 for more information.
5. Click the *Accept Settings* button..

Delete a User

1. Click the *Users* tab.
2. Click to select the name of the user you want to delete.
3. Click the *Edit selected user* button.
4. Click the *Delete user* check box.
5. Click the *Accept Settings* button.

Note: You can also edit, delete, and enroll an existing user by clicking on that user listed on the User's tab and selecting the desired action from the pop-up menu.

User Fields

Table 5-4: User Fields

Field	Req'd?	Description
Unique Identifier	Yes	• Up to 30 characters (any combination of letters, numbers, spaces, or special characters) • If user was added from the reader, will initially match credential ID in the reader but can be changed.
First Name	Yes	• User's first name • If user was added at the reader, will initially match the credential ID
Middle Initial	No	• User's middle initial
Last Name	Yes	• User's last name • If user was added at the reader, will initially match the credential ID
Important Date	No	• Used to distinguish between users with similar names • Type a date directly into the entry box using the format Thursday, January 01, 2009 • Click the drop-down button to select the date from a calendar.
Credential ID	Yes	• User's credential ID • ID number from user's card (when card readers are used) or the number a user enters manually at the reader. See the reader's manual for help with designing an ID numbering system.
Biometric Threshold	Yes	• Controls how closely user's finger or hand must match the stored template in order for access to be granted. • Reader default uses the Reject Threshold from the reader's setup. See Reject Threshold on pages 36 and 38 for more information. In most cases, Reader default is the appropriate choice. • To override the reader's reject threshold, choose from values of 30-250 in the drop down list (common values of 250, 150, 75, 50, and 30 are singled out at the top). • Use a lower number for higher security. • Use a higher number if a user has trouble gaining access. See the reader's manual for more information.
Authority Level	Yes	• Determines what menus the user can access at the reader. • Each level gives access to all the lower levels. • See the Authority Levels table on page 14 for more information.
Access Profile	Yes	• Controls which readers the user can use. • Always allows access to all readers. • Never blocks access to all readers. • Additional choices correspond to the profiles configured in the Access tab. See Access Tab on page 61 for more information.

Field	Req'd?	Description
Verify on ID only (no biometric verification)	No	• Check for users who fingerprints or hand cannot be scanned • Since bypassing finger or hand recognition gives you reduced security, only use this as a last resort. See Adding a Special User on page 11 for more information.
Use Second Finger as Duress Alarm (FingerKey only)	No	• When checked, user's second finger will be used as a duress indicator.
Delete User	No	• Check to delete user from HandNet Lite. • User will be deleted from HandNet Lite and from all connected readers when you click the *Accept* button.

Authority Levels

Table 5-5: Authority Levels

Authority Level	Description
(0) None:	• Allows user to gain access through the reader, but not use the command menus in the reader to change the reader's settings. • This choice is appropriate for most users.
(1) Service:	• Allows the master reader to display the status of all readers on the network. • Not relevant on readers that are not configured as a master.
(2) Setup:	• Allows user to control reader setup • See reader's manual for more information.
(3) Management:	• Allows user to list all of the users in the reader • Allows master reader to send/acquire user databases to/from readers in a network.
(4) Enrollment:	• Allows user to add or remove users.
(5) Security:	• Allows user to modify security settings • See reader's manual for more information.

See the reader's manual for information on directly changing settings through the reader.

Process Deletes Button

When the Process Deletes button is pressed, HandNet-Lite looks for a RemoveUserXML. Xml file in the root directory of the C: Drive.   If this file is found, any users listed in that file will be removed from Handnet-lite.   Figure 3.1 provides a sample C:\RemoveUserXML. Xml file which would remove users with UserIDs of 1000, 1001, 1002, 1003, and 1004 when the Process Deletes button is pressed.

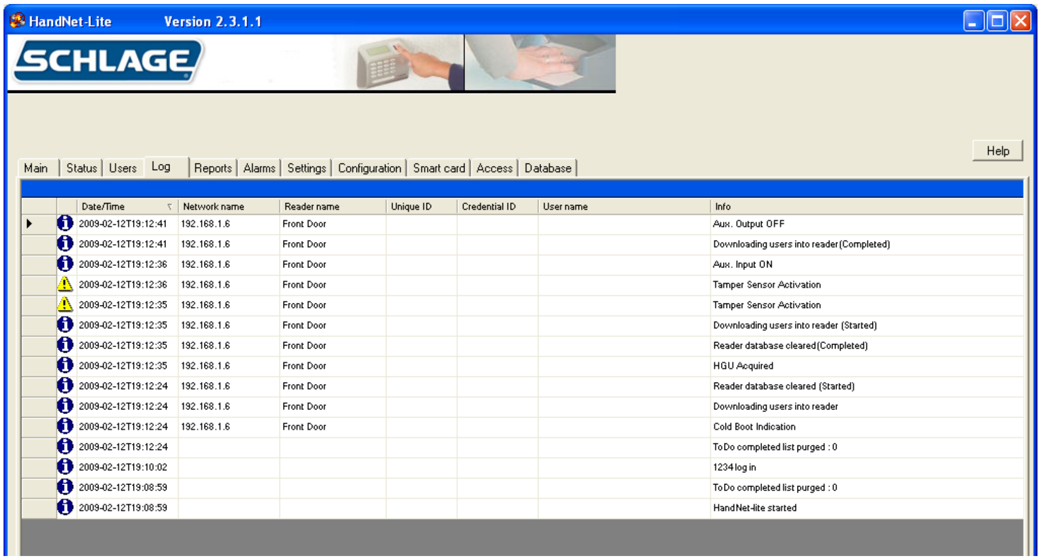
Figure 5-1: Example of RemoveUserXML.xml

```
<?xml version=”1.0” standalone=”yes”?>
<RemoveUser xmlns=”http://tempuri.org/RemoveUser.xsd”>
  <CRsiRemoveUser>
    <UserID>1000</UserID>
  </CRsiRemoveUser>
  <CRsiRemoveUser>
    <UserID>1001</UserID>
  </CRsiRemoveUser>
  <CRsiRemoveUser>
    <UserID>1002</UserID>
  </CRsiRemoveUser>
  <CRsiRemoveUser>
    <UserID>1003</UserID>
  </CRsiRemoveUser>
  <CRsiRemoveUser>
    <UserID>1004</UserID>
  </CRsiRemoveUser>
  <CRsiRemoveUser>
    <UserID>1005</UserID>
  </CRsiRemoveUser>
</RemoveUser>
```

Log Tab

The *Log* tab lists events that occur in any connected reader. It also lists any changes made in HandNet Lite.

Figure 6-1: Log Tab



	Date/Time	Network name	Reader name	Unique ID	Credential ID	User name	Info
ⓘ	2009-02-12T19:12:41	192.168.1.6	Front Door				Aux. Output OFF
ⓘ	2009-02-12T19:12:41	192.168.1.6	Front Door				Downloading users into reader(Completed)
ⓘ	2009-02-12T19:12:36	192.168.1.6	Front Door				Aux. Input ON
⚠	2009-02-12T19:12:36	192.168.1.6	Front Door				Tamper Sensor Activation
⚠	2009-02-12T19:12:35	192.168.1.6	Front Door				Tamper Sensor Activation
ⓘ	2009-02-12T19:12:35	192.168.1.6	Front Door				Downloading users into reader (Started)
ⓘ	2009-02-12T19:12:35	192.168.1.6	Front Door				Reader database cleared(Completed)
ⓘ	2009-02-12T19:12:35	192.168.1.6	Front Door				HGU Acquired
ⓘ	2009-02-12T19:12:24	192.168.1.6	Front Door				Reader database cleared (Started)
ⓘ	2009-02-12T19:12:24	192.168.1.6	Front Door				Downloading users into reader
ⓘ	2009-02-12T19:12:24	192.168.1.6	Front Door				Cold Boot Indication
ⓘ	2009-02-12T19:12:24						ToDo completed list purged : 0
ⓘ	2009-02-12T19:10:02						1234log in
ⓘ	2009-02-12T19:08:59						ToDo completed list purged : 0
ⓘ	2009-02-12T19:08:59						HandNet-lite started

Log Tab Fields

Table 6-6: Log Tab Fields

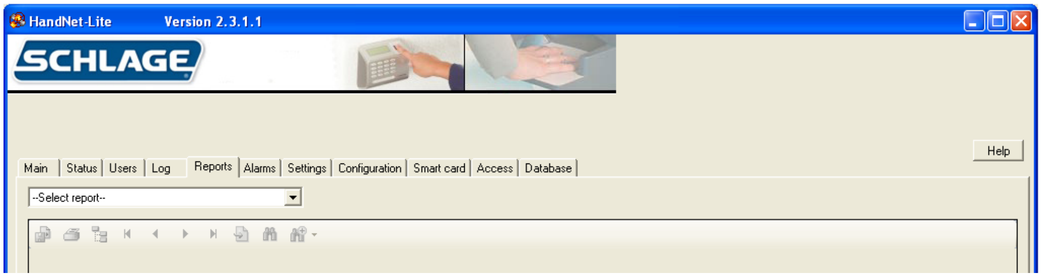
Column	Description
Event type (untitled)	One of the following icons: ⓘ: Indicates a standard informational message. ⚠: Indicates that the condition is important and warrants further investigation. These conditions are also listed on the Alarms tab.
Date/Time	Shows the date and time when the event occurred. The date is listed in year-month-day order, and the time lists hours:minutes:seconds
Network name	Network name if activity occurred at a reader
Reader name	Reader name if activity occurred at a reader
Unique ID	User's unique ID if event is associated with a particular user
Credential ID	User's credential ID if event is associated with a particular user
User name	User's name if message is event with a particular user
Info	Explanation of event

Click the heading of any row to sort the list by that heading. Click the heading again to reverse the sort order.

Reports Tab

The Reports tab is used to generate and view reports on users and readers.

Figure 7-1: Reports Tab


HandNet-Lite Version 2.3.1.1
SCHLAGE
Help
Main | Status | Users | Log | Reports | Alarms | Settings | Configuration | Smart card | Access | Database
--Select report--

Generate a Report

1. Click the *Reports* tab.
2. Click the drop-down list at the top of the reports tab and choose the report you want to generate.

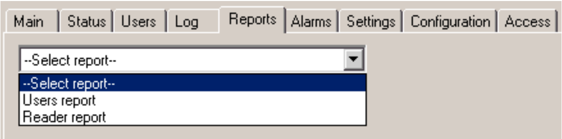
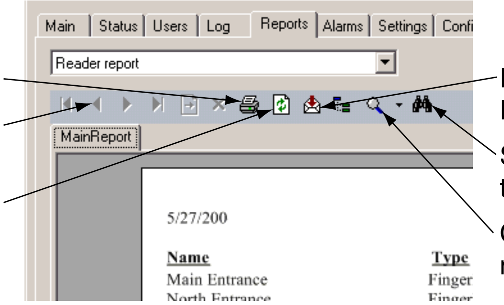

Main | Status | Users | Log | Reports | Alarms | Settings | Configuration | Access
--Select report--
--Select report--
Users report
Reader report

Table 7-7: Report Types

Report Type	Description
Users Report	Lists key information about every user in the system
Readers Report	Lists key information about every reader in the system

3. To print or move around in the report, click the corresponding icon in the bar above the report window.



Print

Move from page to page

Refresh report to reflect changes

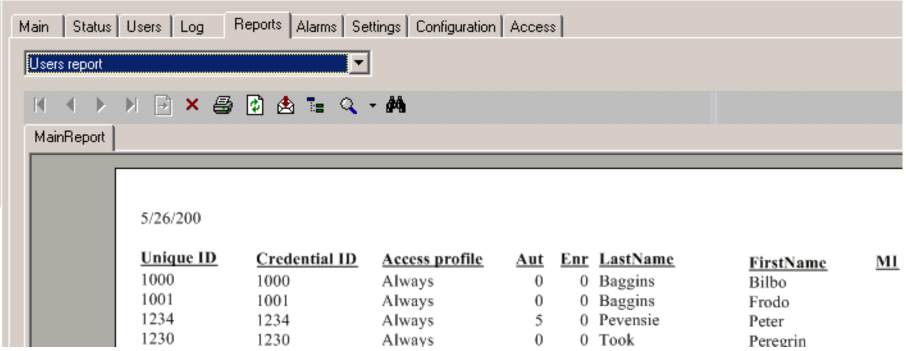
Export to Word, Excel, .pdf, etc.

Search for text in the report

Change the magnification

Users Report

The Users report lists the information for each user in the program.



5/26/200

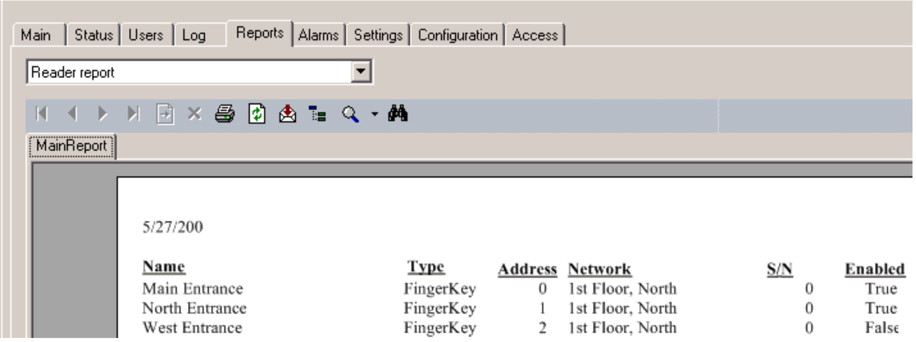
Unique ID	Credential ID	Access profile	Aut	Enr	LastName	FirstName	MI
1000	1000	Always	0	0	Baggins	Bilbo	
1001	1001	Always	0	0	Baggins	Frodo	
1234	1234	Always	5	0	Pevensie	Peter	
1230	1230	Always	0	0	Took	Peregrin	

Table 7-8: Users Report

Column	Description
Unique ID	User's Unique identifier
Credential ID	User's credential ID (card or manual ID)
Access Profile	Access profile associated with the user
Aut	User's authority level
LastName	• User's last name • If you added the user at the reader and have not changed the name, user ID is listed
FirstName	• User's first name • If you added the user at the reader and have not changed the name, user ID is listed
MI	User's middle initial.

Reader Report

The Reader report lists information for each reader in the program.



5/27/200

Name	Type	Address	Network	S/N	Enabled
Main Entrance	FingerKey	0	1st Floor, North	0	True
North Entrance	FingerKey	1	1st Floor, North	0	True
West Entrance	FingerKey	2	1st Floor, North	0	False

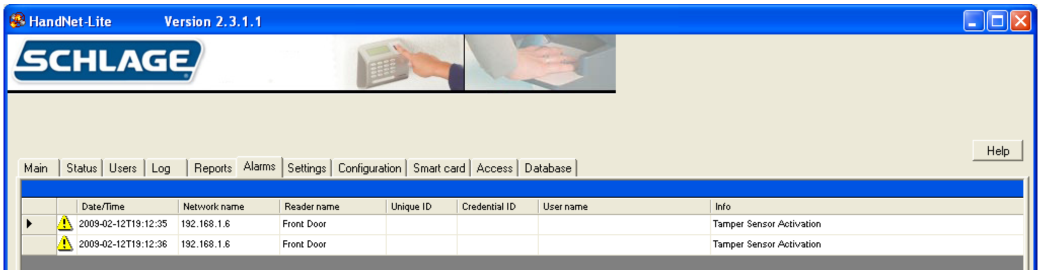
Table 7-9: Reader Report

Column	Description
Name	Reader's name
Type	Indicates whether the reader is a hand or fingerprint reader
Address	Reader's address
Network	Network to which reader is connected
S/N	Reader's internal serial number
Enabled	• true: program attempts to communicate with the reader • false: program does not attempt to communicate with the reader

Alarms Tab

The *Alarms* tab shows all alarms that have been recorded in the system. Alarms are also listed with the rest of the activity in the *Log* tab

Figure 8-1: Alarms Tab



Date/Time	Network name	Reader name	Unique ID	Credential ID	User name	Info
2009-02-12T19:12:35	192.168.1.6	Front Door				Tamper Sensor Activation
2009-02-12T19:12:36	192.168.1.6	Front Door				Tamper Sensor Activation

Alarms Fields

Table 8-10: Alarms Fields

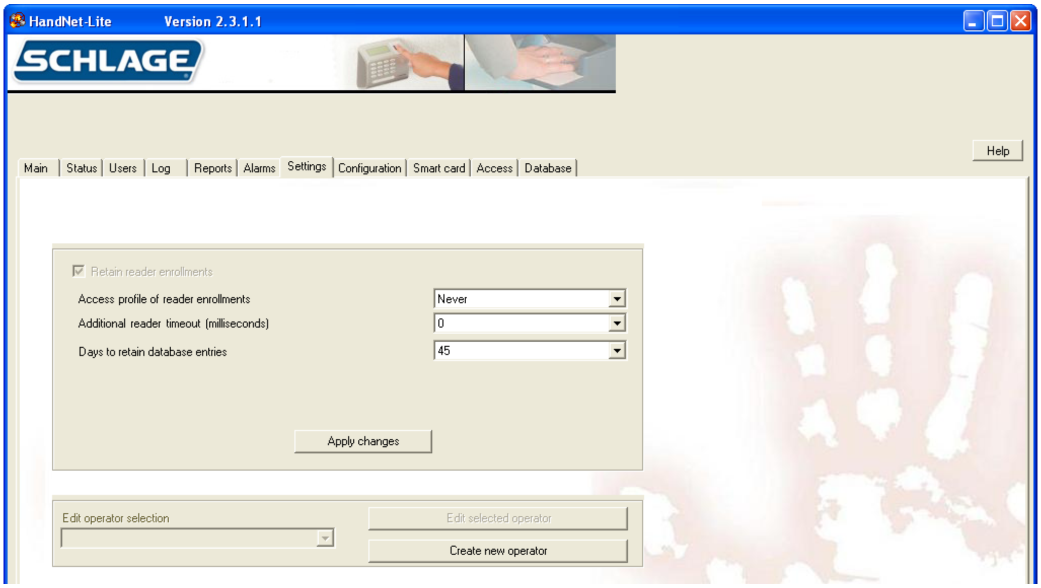
Column	Description
Date/Time	Date and time when the alarm occurred. The date is listed in year-month-day order, and the time lists hours:minutes:seconds
Network name	Network name if alarm is associated with a particular reader
Reader name	Reader name if alarm is associated with a particular reader
Unique ID	User’s unique ID if alarm is associated with a particular user
Credential ID	User’s credential ID if alarm is associated with a particular user
User name	User’s name if alarm is associated with a particular user
Info	Description of alarm

Click the heading of any row to sort the list by that heading. Click the heading again to reverse the sort order.

Settings Tab

The *Settings* tab allows you to set default settings and add operators to the system.

Figure 9-1: Settings Tab



HandNet-Lite Version 2.3.1.1
SCHLAGE
Help
Main | Status | Users | Log | Reports | Alarms | Settings | Configuration | Smart card | Access | Database
Apply changes
Edit operator selection
Edit selected operator
Create new operator

☑ Retain reader enrollments

Access profile of reader enrollments: Never

Additional reader timeout (milliseconds): 0

Days to retain database entries: 45

Settings Fields

Table 9-11: Settings Fields

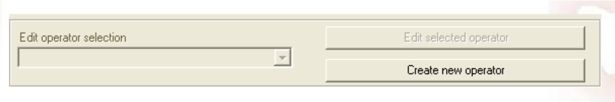
Setting	Description
Retain reader enrollments	This box is always checked and cannot be changed.
Access profile of reader enrollments	• Access profile assigned to users by default when users are added at a reader before being added in the system. • Choices are Always, Never or any custom profiles created by an operator. See Access Tab on page 61 for more informaiton.
Additional reader timeout	• Additional time that is added globally to the command timeout. • Select additional time if command timeout errors are generated on the network. These errors would be displayed on the Alarms tab. See Alarms Tab on page 23 for more information.
Days to retain expired database entries	• Number of days expired database entries are retained • Choose default of 45 days initially. If database becomes too large, make this number smaller.

Managing Operators

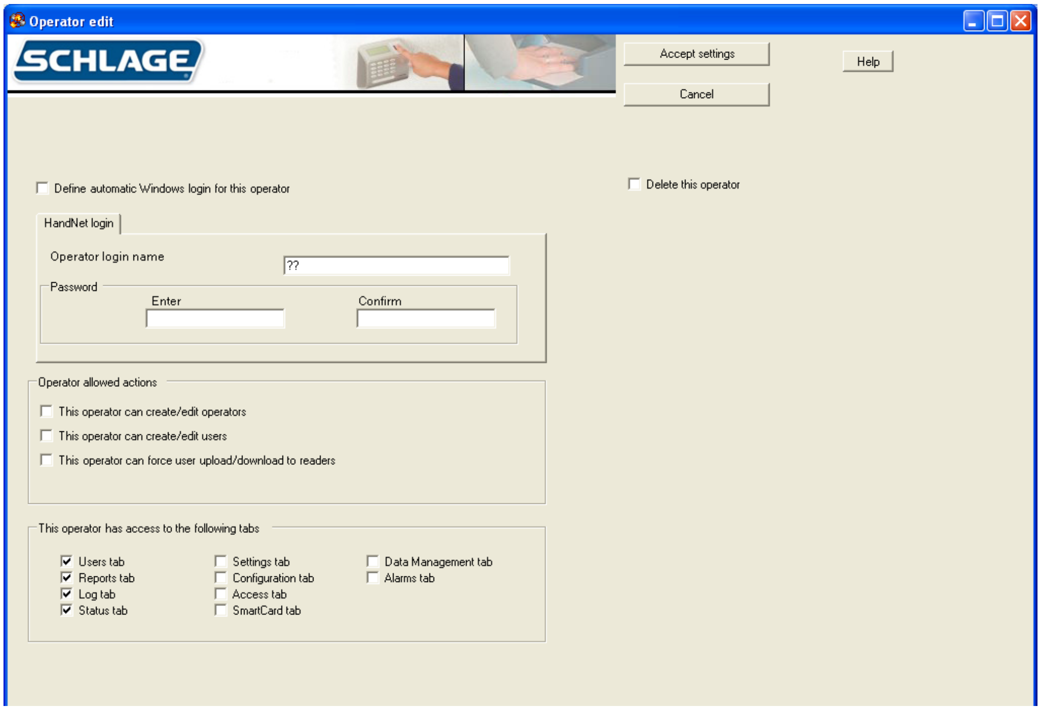
Operators are individuals who can control the system. The level of control can be set individually for each operator.

Add a New Operator

1. Click the *Settings* tab.
2. Click the *Create new operator* button.



The Operator edit screen will appear:



☐ Define automatic Windows login for this operator

☐ Delete this operator

Operator login name ??

Operator allowed actions

☐ This operator can create/edit operators
☐ This operator can create/edit users
☐ This operator can force user upload/download to readers

This operator has access to the following tabs

☑ Users tab
☑ Reports tab
☑ Log tab
☑ Status tab
☐ Settings tab
☐ Configuration tab
☐ Access tab
☐ SmartCard tab
☐ Data Management tab
☐ Alarms tab

3. Click the *Define automatic Windows login for this operator* box to use Windows login information for this operator. See Enable Automatic Windows Login 27.
4. Enter a login name in the operator login name box. This name is case sensitive.
5. Enter the password and confirmation in the enter and confirm boxes. The password is case sensitive.
6. Choose the operator allowed actions by clicking the corresponding check box(es).
7. Choose the tabs to which the operator has access by clicking the corresponding check box(es).
8. Click the *Accept Settings* button.

Edit an Operator

1. Click the *Settings* tab.
2. Select the operator you want to edit from the *Edit operator selection* drop-down box.
3. Click *Edit selected operator* button.
4. Edit the necessary settings. See Add a New Operator on page 26 for more information.
5. Click the *Accept Settings* button.

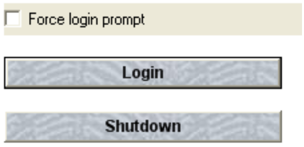
Delete an Operator

1. Click the *Settings* tab.
2. Select the operator you want to delete from the *Edit operator selection* drop-down box.
3. Click the *Delete this operator* check box.
4. Click the *Accept Settings* button.

Enable Automatic Windows Login

If you wish to allow automatic Windows login for HandNet Lite:

1. Click the *Main* tab.
2. Log off.
3. Click to un-check the *Force login prompt* checkbox.
4. Shut down HandNet Lite. The next time you start HandNet Lite, you will be automatically logged in.



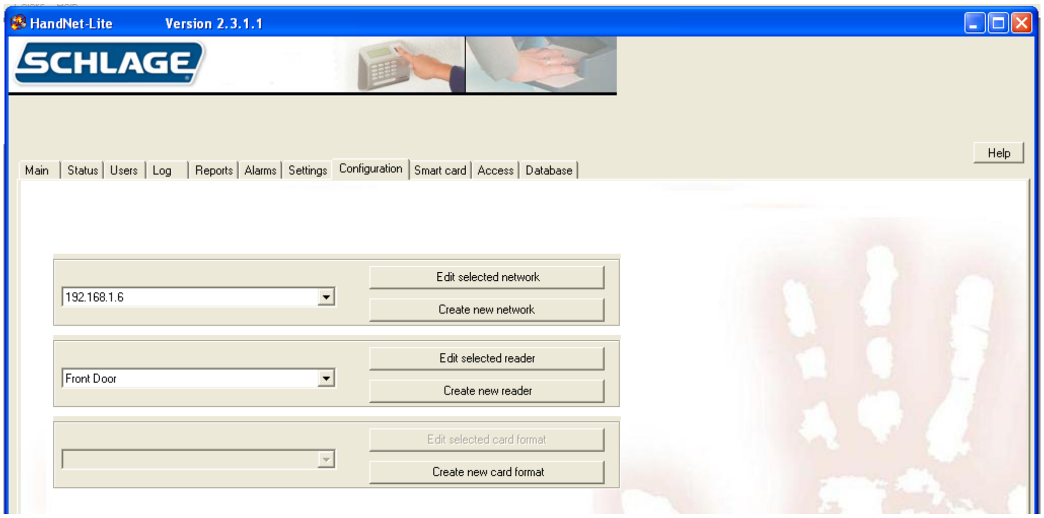
Disable Automatic Windows Login

1. Click the *Main* tab
2. Log off.
3. Click to check the *Force login prompt* checkbox.
4. Shut down HandNet Lite. The next time you start HandNet Lite, you will be prompted for login name and password.

Configuration Tab

The *Configuration* tab is used to add or edit networks, readers and card formats.

Figure 10-1: Configuration Tab



HandNet-Lite Version 2.3.1.1
SCHLAGE
Help
Main | Status | Users | Log | Reports | Alarms | Settings | Configuration | Smart card | Access | Database
192.168.1.6
Edit selected network
Create new network
Front Door
Edit selected reader
Create new reader
Edit selected card format
Create new card format

Managing Networks

A network is a group of up to 32 daisy-chained readers connected though a single serial port using 2 wire RS485, a single reader connected to a computer with RS232, or a single TCP/IP (ethernet) reader. (See the reader manual for wiring and connection detail.)

You control access to each reader separately using HandNet Lite, so having readers with unrelated purposes in one network is fine.

There are two parts to setting up a network and readers: you must physically set the readers up and connect them to each other and to the computer, and you must add the network and readers in HandNet Lite. This manual only explains how to set up the network and readers in HandNet Lite. For help setting up and connecting the readers, see the manual that came with the readers.

Add a Network

1. Click the *Configuration* tab.
2. Click the *Create new network* button
3. Choose the Network type from the drop-down box. The remaining fields displayed will be determined by this selection.
4. Complete the fields on the screen. See page 30 for TCP/IP network. See page 32 for Serial network.
5. Click *Accept settings*.

Edit a Network

1. Click the *Configuration* tab.
2. Select the network you want to edit from the drop-down box.
3. Click the *Edit selected network* button
4. Complete the fields on the screen. See page 30 for TCP/IP network. See page 32 for Serial network.
5. Click *Accept settings*.

Delete a Network

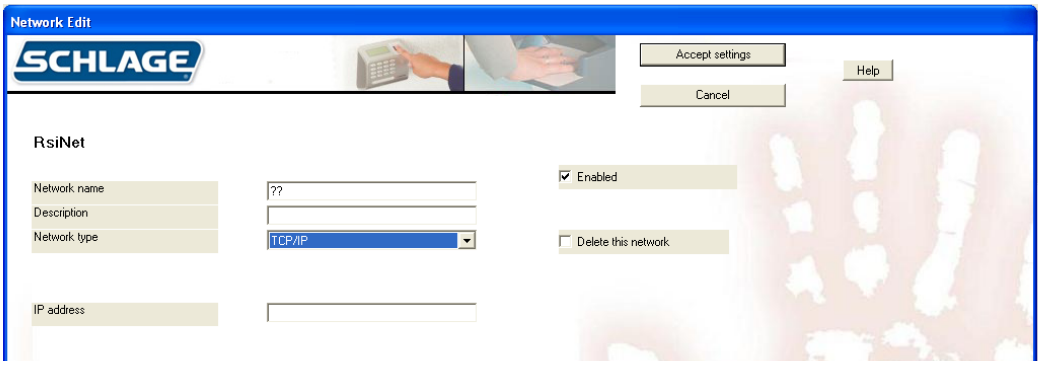
Only networks with no readers can be deleted.

1. Click the *Configuration* tab.
2. Select the network you want to delete from the drop-down box.
3. Click the *Edit selected network* button
4. Click the *Delete this network* check box.
5. Click *Accept settings*.

Connecting through a TCP/IP network

To connect to a site through the network, you must have a TCP/IP network with static IP addresses. Your computer must have a network card and be connected to the network. If the network is faster than 10baseT, you must have a switching hub. To use TCP/IP, you must have either ordered readers with the Ethernet option enabled or purchased an Ethernet upgrade.

Figure 10-2: Edit a TCP/IP Network



RsiNet

Network name: ??
Description:
Network type: TCP/IP
IP address:

☑ Enabled
☐ Delete this network

Table 10-12: TCP/IP Network Fields

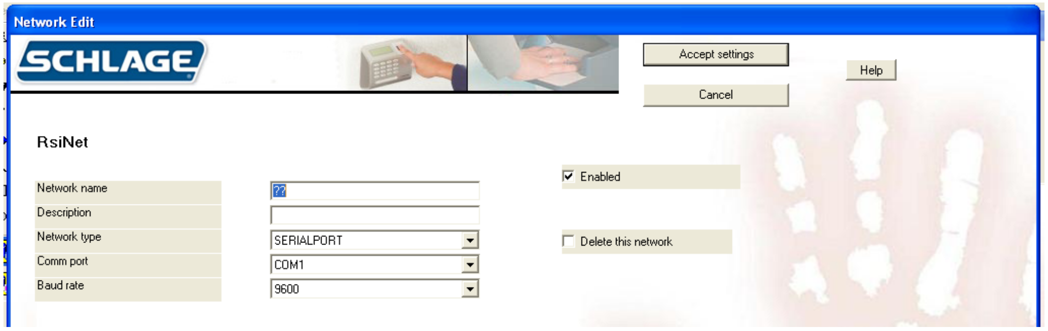
Field	Req'd?	Description
Network Name	Yes	• Name of the network • Any combination of letters, numbers, spaces, and special characters, up to 30 characters long
Description	No	Brief description of the network

Field	Req'd?	Description
Enabled	No	• Must be checked for HandNet Lite to communicate with the network and monitor any readers connected to it. • Generally you would only uncheck this if you were in the process of setting up or reconfiguring the network and didn't want the program to try to communicate • Having the Enabled box checked if the network isn't really connected to HandNet Lite causes the program to slow down significantly. Make sure that this is only checked if the network is actually set up and connected
Delete This Network	No	• Check to delete this network and remove it from the Schlage Biometrics network selection list. If there are no readers in the network, it will be deleted when you click Accept settings. • You can't delete a network with readers on it
Network Type	Yes	• Choose Serial port or TCP/IP • The remaining fields will be determined by this selection.
IP address	Yes	• Only available if TCP/IP was chosen in the Network type field. • The IP address (xxx.xxx.xxx.xxx) of the reader • Must match the IP address set in the reader. See the reader manual for more information • Ask your network administrator for an appropriate address

Connecting through a serial port

To connect to a site by running a cable from your computer to the reader, you must have a free serial port on your computer. See the reader manual for more on the requirements for the cable.

Figure 10-3: Serial Network Edit Screen



RsiNet

Network name: ??

Description:

Network type: SERIALPORT

Comm port: COM1

Baud rate: 9600

☑ Enabled

☐ Delete this network

Table 10-13: Serial Network Fields

Field	Req'd?	Description
Network Name	Yes	• Name of the network • Any combination of letters, numbers, spaces, and special characters, up to 30 characters long
Description	No	• Brief description of the network
Enabled	No	• Must be checked for the system to communicate with the network and monitor any readers connected to it. • Uncheck when in the process of setting up or reconfiguring the network to keep the program from trying to communicate • If checked when the network is not really connected, the system will slow down significantly.
Delete This Network	No	• Check to delete this network and remove it from the network selection list. • You cannot delete a network with readers in it
Network Type	Yes	• Choose Serial port or TCP/IP • The remaining fields will be determined by this selection.
Comm Port	Yes	• Only available if Serial port was chosen in the Network type field. • Must match the serial port to which the reader is connected • Only the ports that are currently available on your computer are listed.

Field	Req'd?	Description
Baud Rate	Yes	• Only available if Serial port was chosen in the Network type filed. • Choose from values of 4800, 9600, 19200, 28800, 38400, or 57600. • Choose 9600 initially. Increase the rate after a working connection has been established. Longer wire distances require lower rates. • Must match the rate set in all readers on the network. See the reader manual for more information.

Managing Readers

There are two parts to setting up readers: physically setting up the readers and connecting them to each other and to the computer, and adding the network and readers in HandNet Lite. This manual only explains adding the network and readers in HandNet Lite. For help setting up and wiring readers, see the manual that came with the readers.

Before you add readers, you must set up the network to which they are connected. See Add a Network on page 29 for more information.

If You've Been Using Readers Already

If you've been using readers without HandNet Lite, when you add the network and readers to the system, HandNet Lite automatically gets the users from the readers and adds them to the system; see How Users Are Enrolled and Added to HandNet Lite on page 39.

Add a Reader

1. Click the *Configuration* tab.
1. Select the network in which the new reader will exist from the network drop-down box.
2. Click the *Create new reader* button.
3. Choose the *Reader type* from the drop-down box. The entries on the screen will differ depending on the reader type chosen.
4. Fill in the entries on the Reader Edit screen. See page 35 for FingerKey. See page 37 for HandKey.
5. Click the *Test reader* button. If the reader is properly configured, the reader will be able to communicate.
6. To change the security settings for the reader, click the *Security settings* button. See Security Settings Screen on page 40 for more information.
7. If you are editing a FingerKey and want to edit the fingerprint settings, click the *Fingerprint settings* button. See Fingerprint Settings Screen on page 41 for more information.
8. Click the *Accept settings* button.

Edit a Reader

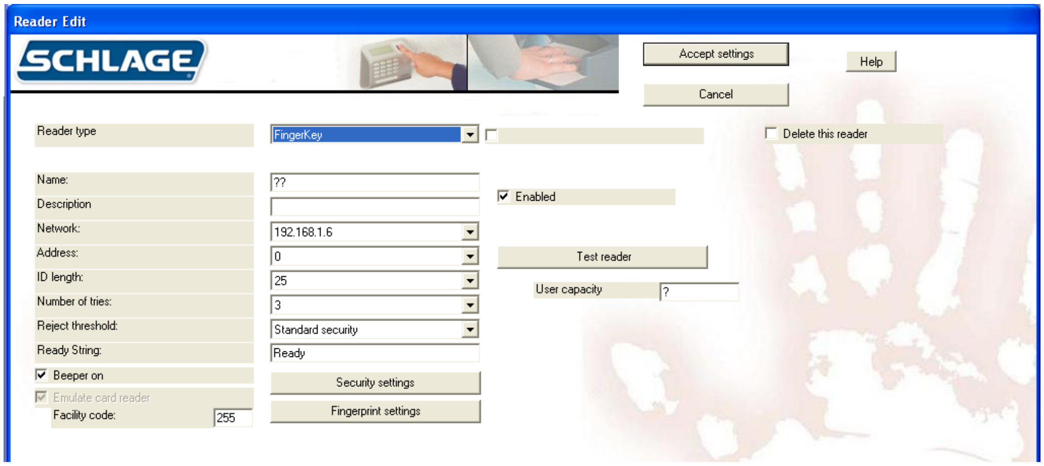
1. Click the *Configuration* tab.
1. Select the network in which the reader you want to edit exists in the network drop-down box.
2. Click the *Edit selected reader* button.
3. The entries on the screen will differ depending on the reader type chosen.
4. Fill in the entries on the Reader Edit screen. See page 35 for FingerKey. See page 37 for HandKey.
5. Click the *Test reader* button. If the reader is properly configured, the reader will be able to communicate.
6. To change the security settings for the reader, click the *Security settings* button. See Security Settings Screen on page 40 for more information.
7. If you are editing a FingerKey and want to edit the fingerprint settings, click the *Fingerprint settings* button. See Fingerprint Settings Screen on page 41 for more information.
8. Click the *Accept settings* button.

Delete a Reader

1. Click the *Configuration* tab.
1. Select the network in which the reader you want to delete exists in the network drop-down box.
2. Click the *Edit reader* button.
3. Click the *Delete this reader* check box.
4. Click the *Accept settings* button.

FingerKey Reader Edit Screen

Figure 10-4: FingerKey Reader Edit Screen



Reader type: FingerKey □

□ Delete this reader

Name: ??

Description:

Network: 192.168.1.6

Address: 0

ID length: 25

Number of tries: 3

Reject threshold: Standard security

Ready String: Ready

☑ Beeper on

☑ Emulate card reader

Facility code: 255

☑ Enabled

User capacity ?

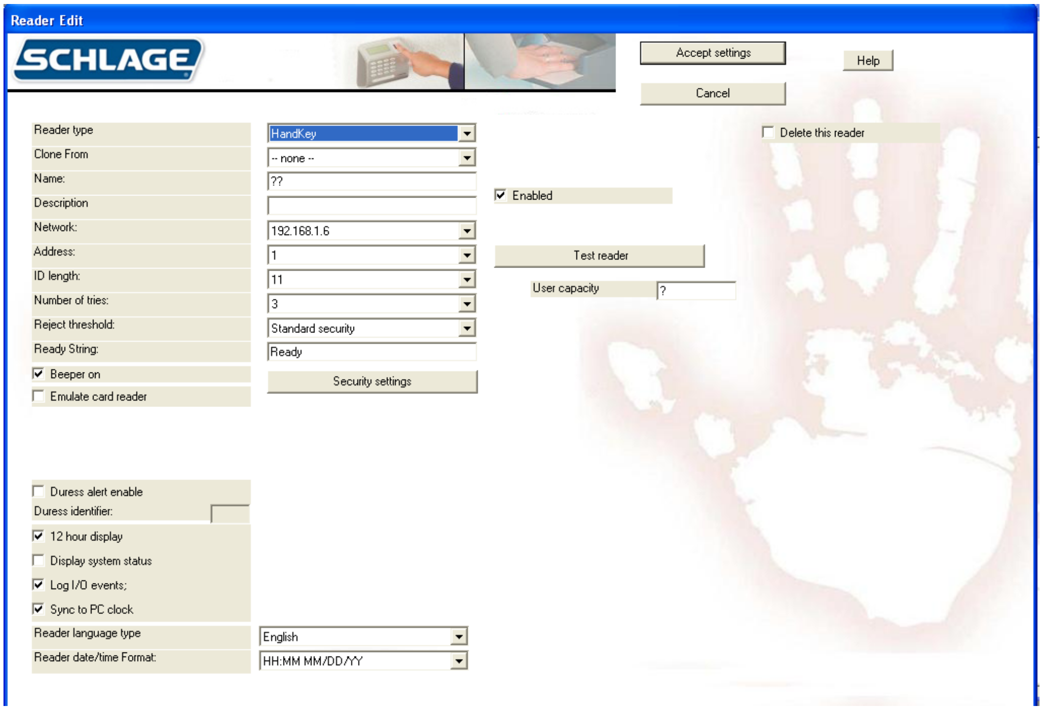
Table 10-14: FingerKey Reader Fields

Field	Req'd?	Description
Clone From	No	• Appears only after at least one reader has been configured. • Allows you copy the settings from another reader, including the underlying Fingerprint and Security Settings. • If this option is chosen, all of the following fields will be populated automatically.
Name	Yes	Any combination of letters, numbers, spaces, and special characters, up to 30 characters.
Description	No	Briefly describe the reader.
Network	Yes	• Select the network in which the reader exists. • Network must be set up before you can add the reader. See Add a Network on page 29 for more information.
Address	Yes	• Must match the address set in the reader. See the reader's manual for information on setting the address in the reader. • Field will be automatically populated with the first available address that hasn't been used. Choose another number from the pull-down list if desired. • Changing the address on this screen does NOT change the address in the physical reader. If you change an address here, you must also change the address in the reader.
ID Length	No	• If all user IDs are the same length, choose the number of digits here (any value from 1-25) so users don't have to press enter after typing the ID at the reader. • If user IDs are different lengths, choose the longest number of digits. Users with the longest IDs will not have to press ENTER after typing the ID at the reader. • Entry does not affect the length of IDs on cards. It only affects IDs entered at the keypad.

Field	Req'd?	Description
Number of Tries	Yes	• Controls how many times the user can try to get access before the reader will block the user's ID and not allow further tries. • Prevents someone from making repeated tries to gain access with someone else's ID. • Normally 3 is a good setting.
Reject threshold	Yes	• The lower this number is, the more closely the user's finger must match the template of the finger stored in the FingerKey. • 30 (the lowest possible number) requires the fingerprint to match very closely; 250 (the highest possible number) will grant access if the finger match is close but not exactly the same. • 75 is good for most contexts. Choose a lower number if you have an especially high security situation. • If particular users have trouble placing their fingers consistently, you can override the reader's setting for an individual user on the User edit screen in the Users window. See Edit a User on page 12 for more information.
Ready String	Yes	• This text appears in the reader display when the reader is ready and waiting for the user to enter an ID. • Any combination of letters, numbers, spaces, and special characters, up to 20 characters
Beeper On	No	• When checked, the reader beeps each time you press a button • In a high security setting, you might want the beeps off to make it harder for a casual observer to figure out how many digits are in the ID number.
Emulate Card Reader	Yes	• FingerKey readers always emulate a card reader, so you can't uncheck this box
Facility Code	Yes	• Facility code that should be passed to the access control panel. • Numeric value from 0 (zero) to 65535
Enabled	No	• Check if the reader is physically set up and ready to be used. • Checking the Enabled box if the reader is not really connected slows the program down significantly. Make sure this is only checked if the reader is actually set up and connected
User capacity	Yes	• Will be filled in automatically by the reader.
Delete This Reader	No	• Check ONLY to delete reader and remove it from the reader selection list.

HandKey Reader Edit Screen

Figure 10-5: HandKey Reader Edit Screen



Reader type	HandKey
Clone From	-- none --
Name:	??
Description	
Network:	192.168.1.6
Address:	1
ID length:	11
Number of tries:	3
Reject threshold:	Standard security
Ready String:	Ready

☑ Beeper on

□ Emulate card reader

□ Delete this reader

☑ Enabled

User capacity ?

□ Duress alert enable

Duress identifier:

☑ 12 hour display

□ Display system status

☑ Log I/O events;

☑ Sync to PC clock

Reader language type	English
Reader date/time Format:	HH:MM MM/DD/YY

Table 10-15: HandKey Reader Fields

Field	Req'd?	Description
Clone From	No	• Appears only after at least one reader has been configured. • Allows you copy the settings from another reader, including the underlying Fingerprint and Security Settings. • If this option is chosen, all of the following fields will be populated automatically.
Name	Yes	Any combination of letters, numbers, spaces, and special characters, up to 30 characters.
Description	No	Briefly describe the reader. You may leave this blank if you wish
Network	Yes	• Select the network in which the reader exists. • Network must be set up before you can add the reader. See Add a Network on page 29 for more information.

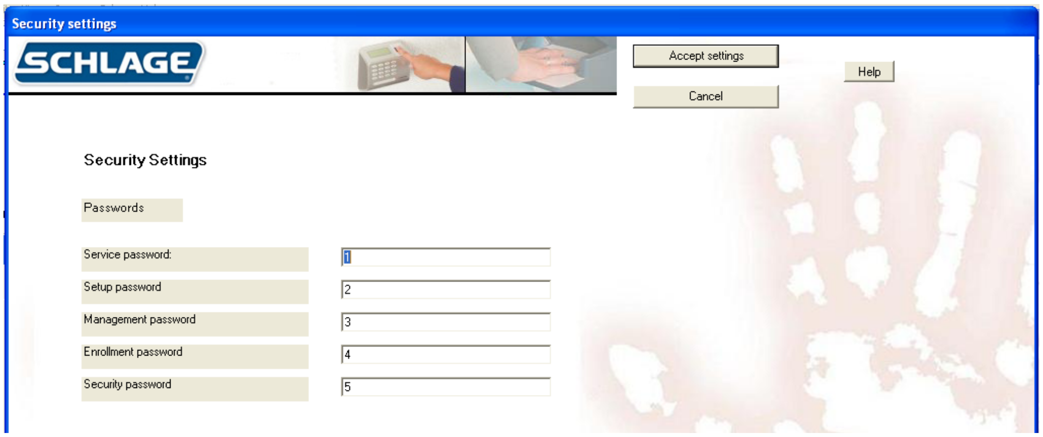
Field	Req'd?	Description
Address	Yes	• Must match the address set in the reader. See the reader's manual for information on setting the address in the reader. • Field will be automatically populated with the first available address that hasn't been used. • Choose another number from the pull-down list if desired. • Changing the address on this screen does NOT change the address in the physical reader. If you change an address here, you must set the reader to the same address or the program won't be able to communicate with the reader
ID Length	No	• If all user IDs are the same length, choose the number of digits here (any value from 1-25) so users don't have to press enter after typing the ID at the reader. • If user IDs are different lengths, choose the longest number of digits. Users with the longest IDs will not have to press ENTER after typing the ID at the reader. • Entry does not affect the length of IDs on cards. It only affects IDs entered at the keypad.
Number of Tries	Yes	• Controls how many times the user can try to get access before the reader will block the user's ID and not allow further tries. • Prevents someone from making repeated tries to gain access with someone else's ID. • Normally 3 is a good setting.
Reject threshold	Yes	• The lower this number is, the more closely the user's finger must match the template of the finger stored in the FingerKey. • 30 (the lowest possible number) requires the fingerprint to match very closely; 250 (the highest possible number) will grant access if the finger match is close but not exactly the same. • 75 is good for most contexts. Choose a lower number if you have an especially high security situation. • If particular users have trouble placing their fingers consistently, you can override the reader's setting for an individual user on the User edit screen in the Users window. See Edit a User on page 12 for more information.
Ready String	Yes	• This text appears in the reader display when the reader is ready and waiting for the user to enter an ID. • Any combination of letters, numbers, spaces, and special characters, up to 20 characters

Field	Req'd?	Description
Beeper On	No	• When checked, the reader beeps each time you press a button • In a high security setting, you might want the beeps off to make it harder for a casual observer to figure out how many digits are in the ID number.
Emulate Card Reader	Yes	• Controls the Output Mode of teh reader (Lock Output mode if unchecked, Card Reader Emulation Output if checked).
Enabled	No	• Check if the reader is physically set up and ready to be used. • Checking the Enabled box if the reader is not really connected slows the program down significantly. Make sure this is only checked if the reader is actually set up and connected
User capacity	Yes	• Contains the number of users the reader is capable of storing (this field is filled in after the Test Reader button is pressed)
Delete This Reader	No	• Check ONLY to delete reader and remove it from the reader selection list.
Duress alert enable	No	• If checked, duress activates AUX output
Duress identifier	No	• This is the key which, when pressed, will generate the DURESS event. • Must be a digit 0 through 9. Other values will disable the duress feature.
12 hour display	No	• If checked, displays terminal time in 12 hour format, otherwise 24 hour time format.
Display system status	No	• If checked, the reader's LCD will display system status on line 2. If unchecked, line 2 of the LCD will display the unit's date and time.
Log I/O events	No	• Currently ignored by HandKey units, I/O Events will always generate a DataLog
Sync to PC clock	No	• The reader's clock will be synchronized to this PC's system time.
Reader language type	No	• Selects the language used on the reader for LCD prompts.
Reader date/time Format	No	• Selects the format that the reader will display date & time on the LCD display.

Security Settings Screen

The Security Settings Screen controls the passwords needed to access the menus in the reader.

Figure 10-6: Security Settings Screen



Security Settings

Passwords

Service password: 1

Setup password 2

Management password 3

Enrollment password 4

Security password 5

Generally the default passwords shown above are adequate since a user must be set up with the appropriate Authority level on the User edit screen in the Users window (see page 12 for more information), and the user must know how to get to these menus in the reader before the passwords below would do any good.

Edit Security Settings

1. Click the *Configuration* tab.
2. Select the network in which the reader you want to edit exists in the network drop-down box.
3. Select the reader you want to edit from the reader drop-down box.
4. Click the *Edit selected reader* button.
5. Click the *Security settings* button.
6. Edit the passwords. See the Security Settings Fields Table on page 40 for more information.
7. Click the *Accept settings* button.

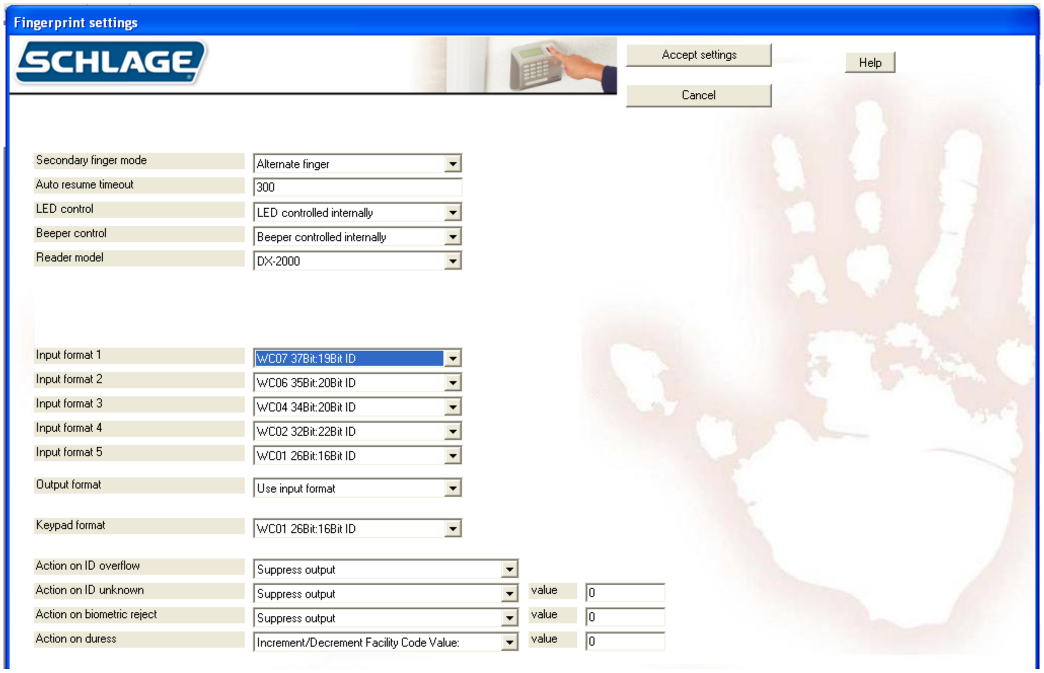
Table 10-16: Security Settings Fields

Field	Req'd	Description
Service	Yes	Allows the master reader display the status of all readers on the network
Setup	Yes	Controls reader setup including the reader's address, ID length, auxiliary output settings, facility codes, network configuration, the duress indicator, etc. It also contains an option to upgrade the maximum number of users
Management	Yes	Allows display of a list all of the users in the reader and lets the master reader send/acquire user databases to/from readers in a network
Enrollment	Yes	Allows you to add or remove users
Security	Yes	Allows you to customize user settings, control how closely user fingerprints must match templates, set the menu passwords, clear all the users from reader, etc

For more detail on the reader menus, see the reader manual.

Fingerprint Settings Screen

The Fingerprint Settings screen controls a number of the reader's internal settings.



Secondary finger mode	Alternate finger		
Auto resume timeout	300		
LED control	LED controlled internally		
Beeper control	Beeper controlled internally		
Reader model	DX-2000		
Input format 1	WC07 37Bit:19Bit ID		
Input format 2	WC06 35Bit:20Bit ID		
Input format 3	WC04 34Bit:20Bit ID		
Input format 4	WC02 32Bit:22Bit ID		
Input format 5	WC01 26Bit:16Bit ID		
Output format	Use input format		
Keypad format	WC01 26Bit:16Bit ID		
Action on ID overflow	Suppress output		
Action on ID unknown	Suppress output	value	0
Action on biometric reject	Suppress output	value	0
Action on duress	Increment/Decrement Facility Code Value:	value	0

Figure 10-7: Fingerprint Settings Screen

Edit Fingerprint Settings

1. Click the *Configuration* tab.
2. Select the network in which the reader you want to edit exists in the network drop-down box.
3. Select the reader you want to edit from the reader drop-down box.
4. Click the *Edit selected reader* button.
5. Click the *Fingerprint settings* button.
6. Edit the necessary fields. See the Fingerprint Settings Fields table on page 41 for more information.
7. Click the *Accept settings* button.

Table 10-17: Fingerprint Settings Fields

Field	Req'd?	Description
Secondary Finger Mode	Yes	• Disabled: reader collects only one finger for each user. • Alternate finger: Scan of second finger grants access exactly as the first does. If user cannot verify with one finger, the other enrolled finger can be used. • Duress finger: Scan of second finger grants access and triggers a duress alarm. (Accomplished by either sending an alternate facility code or with reverse parity, depending on how your access control panel is set up.)

Field	Req'd?	Description
Auto Resume Timeout	Yes	• Number of seconds that reader stays in idle mode after being set into idle mode by a host command. • Number between 60 and 65535 • Default value is 300. • DO NOT change this setting unless advised to by technical support
LED Control	Yes	• Determines what controls the reader's LED display. • LED controlled internally: reader controls the LED display • LED controlled externally: access control panel control the LED display • For more information on setting up the LED control, see the reader's manual.
Beeper Control	Yes	• Determines what controls the reader's beeper. • Beeper controlled internally: reader controls beeper • Beeper controlled externally: access control panel controls beeper • For more information on setting up the beeper control, see the manual that came with the readers.
Reader Model	Yes	• Select the FingerKey model type from the drop down choices which are: • DX-2000 - Select this if you are using a DX-2000 model FingerKey. • DX-2100 HID Prox - Select this if you are using a DX-2100 model FingerKey using HID Prox cards. • DX-2200 HID iClass - Select this if you are using a DX-2200 model FingerKey with HID iClass cards. • DX-2400 Philips Mifare Standard - Select this if you are using a DX-2400 model FingerKey with Mifare Standard cards and settings. • DX-2400 Philips Mifare DESFire - Select this if you are using a DX-2400 model FingerKey with Mifare DESFire cards and settings.
iCLASS Configuration	Yes	• Choose None unless you are using iCLASS readers and cards. • If using iCLASS readers and cards, choose any iCLASS configuration that you've defined. • See Add an iCLASS Definition on page 50 for more information.
Mifare standard Configuration	Yes	• Choose None unless you are using Mifare Standard readers and cards. • If using Mifare Standard readers and cards, choose any Mifare Standard definition that you've defined. • See Add a Mifare Standard Definition on page 57 for more information.

Field	Req'd?	Description
DESFire Configuration	Yes	• Choose None unless you are using Mifare DESFire readers and cards. • If using Mifare DESFire readers and cards, choose any Mifare DESFire definition that you've defined. • See Add a DESFire Definition on page 55 for more information.
Input Format 1-5	Yes	• Card formats reader will accept from an internal or external card reader. • Choose either Wiegand or Magstripe formats but not both. Most companies use only one format. See the Card Formats table on page 65 for more information. • If you change from Wiegand to Magstripe format, or from Magstripe to Wiegand, you must reboot the reader. See the reader manual for further detail
Output Format	Yes	• Format reader sends to the access control panel if you use an internal or external card reader. • Use Input Format: Passes through whatever format is received • None: Reader sends no output when the ID is entered with a card. • Formats 1-11: Choose one of the formats from the Card Formats table on page 65.
Keypad Format	Yes	• Format the reader sends to the access control panel when a user enters his ID on the keypad instead of using a card. • None: Reader sends no output when the ID is entered with the keypad. • Formats 1-11: Choose one of the formats from the Card Formats table on page 65.
Action on ID Overflow	Yes	• Indicates what reader sends to access panel when card ID is longer than maximum length permitted by selected formats. • Suppress Output: Reader sends no output • Substitute all 1 bits: All 1 (one) bits are sent instead of the ID that was entered • Substitute all 0 bits: All 0 (zero) bits are sent instead of the ID that was entered

Field	Req'd?	Description
Action on ID Unknown	Yes	• Controls what the reader sends the access panel when ID is not recognized • Suppress Output: reader sends no output • Alternate Facility Code Value: reader sends facility code entered in the value entry, instead of the normal facility code • Increment/Decrement Facility Code Value: Reader sends facility code increased or decreased by the amount in the Value entry. • Toggle All Parity Bits: reader toggles the output parity bits.
Action on Biometric Reject	Yes	• Controls what the reader sends the access panel when a valid ID is entered but the finger doesn't match the template. • Same four options here as for Action on ID Unknown
Action on Duress	Yes	• Controls what the reader sends the access panel when a user places a duress finger • Same four options here as for Action on ID Unknown
Value	Yes	• Number between 0 and 32767 • Used when either Alternate Facility Code Value, Increment/Decrement Facility Code Value is chosen in the previous three fields • Enter a minus (-) sign before the number if you want to decrement the value.

Enabling a Secondary Finger Later

If users are enrolled with Seconday finger mode disabled, only one finger will be collected. If Secondary finger mode is later changed, all users need to be removed and re-enrolled in order to obtain a template for the second finger. The first finger will still function normally, but the second finger functionality will not be available until the user is re-enolled.

Interpreting the Format Detail

In the explanation of the format detail, you'll see an elaboration on the format that looks like this:

```
         1         2
12345678901234567890123456
PFFFFFFFFIIIIIIIIIIIIIIIIP
EXXXXXXXXXXXX.............
.............XXXXXXXXXXXXO
```

The numbers at the top: Identify the bit numbers; this example has 26 bits.

F: Indicates which bits contain the facility code; in this example, bits 2-9 have the facility code.

I: Indicates which bits contain the ID; in this example, bits 10-25 contain the ID.**P/E/O/X/.:** P indicates a parity bit; the E under the first parity bit here indicates that this parity is even. The X's following indicate which bits are used to determine that parity bit; the periods following indicate that those bits are not used in determining that parity bit; in this example, bits 2-13 are used to determine parity bit 1, and bits 14-26 do not affect this parity bit. The O under the second parity bit (bit 26) indicates this parity bit is odd; the preceding X's indicate that bits 14-25 are used to determine this parity bit.

For a list of available card formats, see the Card Formats table on page 65.

Managing FingerKey Card Formats

Most users don’t need to define additional formats; the predefined formats that we initially provide cover almost all situations. However, if you need some other Wiegand format, you can define any format that you want.

We don’t recommend changing or deleting any of our standard card formats. If you need a format that is similar to one of our existing formats, choose to add a new format; there’s an option on the screen that lets you clone (copy) an existing format; you can then change the copy rather than changing the original.

Add a Card Format

1. Click the *Configuration* tab.
2. Click the *Create new card format* button.
3. Complete the fields on the screen. See the Card Format Fields table on page 46 for more information.
4. Click the *Accept settings* button.

Edit a Card Format

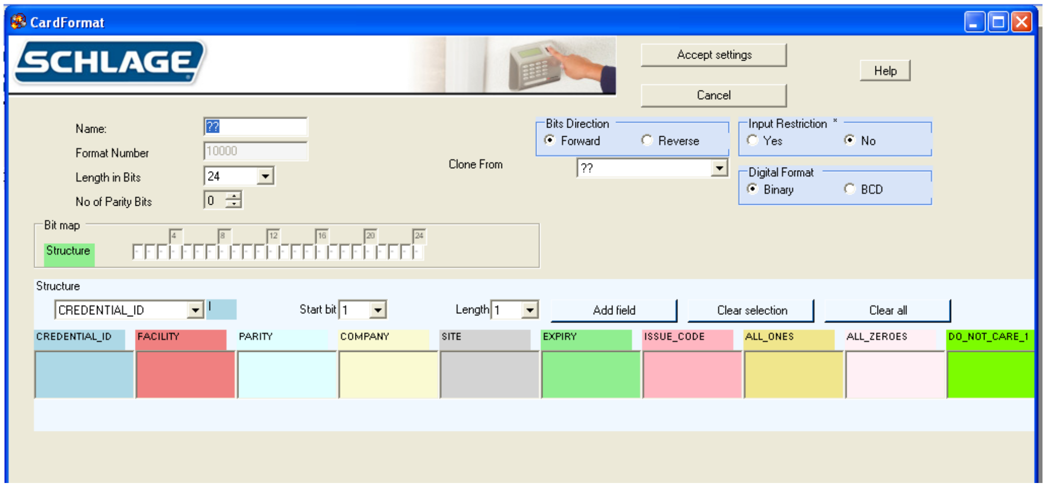
1. Click the *Configuration* tab.
2. Select the card format you want to edit from the drop-down box.
3. Click the *Edit selected card* format button.
4. Make changes to the fields on the screen. See the Card Format Fields table on page 46 for more information.
5. Click the *Accept settings* button.

Delete a Card Format

1. Click the *Configuration* tab.
2. Select the card format you want to edit from the drop-down box.
3. Click the *Edit selected card format* button.
4. Click the *delete* check box.
5. Click the *Accept settings* button.

Card Format Screen

Figure 10-8: The Card Format Screen



Name: ??

Format Number 10000

Length in Bits 24

No of Parity Bits 0

Clone From ??

Bits Direction ● Forward ○ Reverse

Input Restriction * ○ Yes ● No

Digital Format ● Binary ○ BCD

Structure

CREDENTIAL_ID

Start bit 1

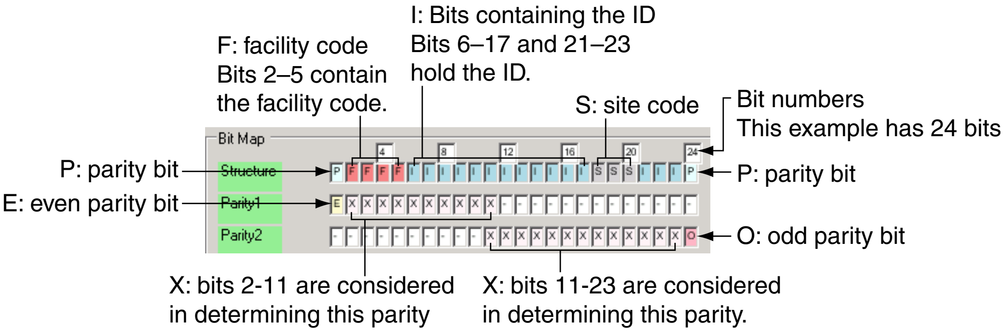
Length 1

The appearance of this screen varies depending on what you choose. The width of the Bit Map section changes based on the length you define for the ID. The Parity sections at the bottom only appear if you indicate that there are parity bits

Table 10-18: Card Format Fields

Field	Req'd?	Description
Name	Yes	Name that clearly identifies the format
Format Number	Yes	Internally generated number to identify the format. Cannot be changed.
Length in Bits	Yes	Number of bits in the format. This is the total number of bits, not just the number of bits in the ID
No of Parity Bits	No	If there are any parity bits, enter the number (1-4) here. For each parity bit specified here, a Parity section appears below
Bit Map	Yes	Structure of the format and how each bit is used. To change how different bits are used, see Card Format Structure on page 47, and the Bit Map example on page 47 for more information.
Delete	No	Deletes the current format.
Bits Direction	Yes	Forward: bits will be read in from left to right Reverse: bits will be read in from right to left
Clone From	No	Only appears if you are creating a new format. Allows you to make a copy of an existing format. Entries on the screen will be set to match the settings for the format you choose.
Input Restriction	Yes	Yes: only an exact format match will be accepted. Gives higher security since cards that are not issued by you will not be accepted. No: any input and parses will be accepted
Digital Format	Yes	Leave this set to Binary unless you understand what BCD is and have a specific reason for choosing it

Figure 10-9: Bit Map Example



Card Format Structure

1. Under Structure, choose the type of bit you want to add from the drop-down box.
    - Credential ID
    - Facility
    - Parity
    - Company
    - Site
    - Expiry
    - Issue Code
    - All Ones
    - All Zeros
    - Do Not Care 1
    - Do Not Care 0

    To add parity bits, see Set Up the Parity Bits on page 48 for more information
2. Choose the first bit you want to use for the structure from the *Start bit* drop-down box.
3. Choose the number of sequential bits from the *Length* drop-down box.
    - For example, if bits 2-11 should contain the ID, select 2 from the Start Bit drop-down box, and 10 from the Length drop-down box.
    - If a particular structure is broken up, the structure will be added in multiple steps. For example, if you have a 15 bit ID, but that ID is contained in bits 2–6, 8–12, and 14–18, add the Credential ID three times: the first time with a Start Bit of 2 and a Length of 5, the second time with a Start Bit of 8 and a Length of 5, and the third time with a Start Bit of 14 and a Length of 5.
    - Similarly, suppose a particular structure is scrambled. For example, suppose bit 2-11 are used for the ID, but instead of being in order, bit 9 is the first bit of the ID, bit 3 is the second, etc. You would simply add this one bit at a time, starting with the first bit (bit 9), then the second, etc. Bits are considered in the order they appear in the structure list. (If you add bits in the wrong order, there's no way to rearrange them. You must delete the incorrect bits and then add them again in the correct order.)
    - If the Start Bit is disabled, then you have used all available bits; if you want to change the function of an existing bit, you must delete the incorrect bits before you can add them elsewhere.
4. Click *Add Field*.

    The bit numbers will be added in the corresponding columns in the structure table, and the bits will be reflected in the Bit Map representation above.
5. To remove an incorrect bit, check the box next to the bit and then click the *Clear Selection* button.
6. To clear (delete) the entire structure, click the *Clear All* button.

Set Up the Parity Bits

1. Add the Parity Bit to the Structure
   a. Under Structure, choose *Parity* from the drop-down box.
   b. Choose the first bit you want to use for the parity bit from the *Start bit* drop-down box.
   c. Choose the number of sequential bits (usually 1) from the *Length* drop-down box.
   d. Click the *Add Field* button.

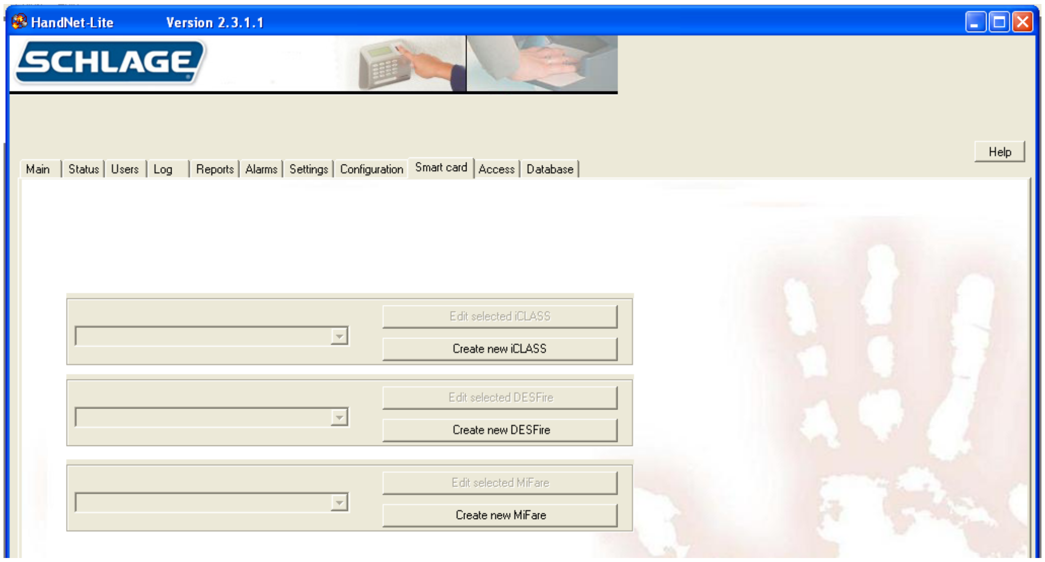
2. Indicate whether that parity bit is even or odd
   a. Under *Parity 1*, choose *Even* or *Odd* from the drop-down box.
   b. Under Start Bit, choose the bit for which you want to identify parity from the drop-down box.
   c. Click *Add Field*.

3. Identify which bits are considered to determine that parity bit
   a. Under *Parity 1*, choose *Included*
   b. Under *Start Bit*, choose the first bit that is used to determine this parity
   c. Under *Length*, indicate the number of bits to consider
   d. Click *Add Field*.
   e. If the bits to consider are broken up (for example, if you want to consider bits 2–10 and bits 14–18), simply repeat this step to add the additional bits.

Smart Card Tab

The Smart Card tab is used only with FingerKeys. It is used to manage FingerKey iCLASS, DESFire and MiFare cards.

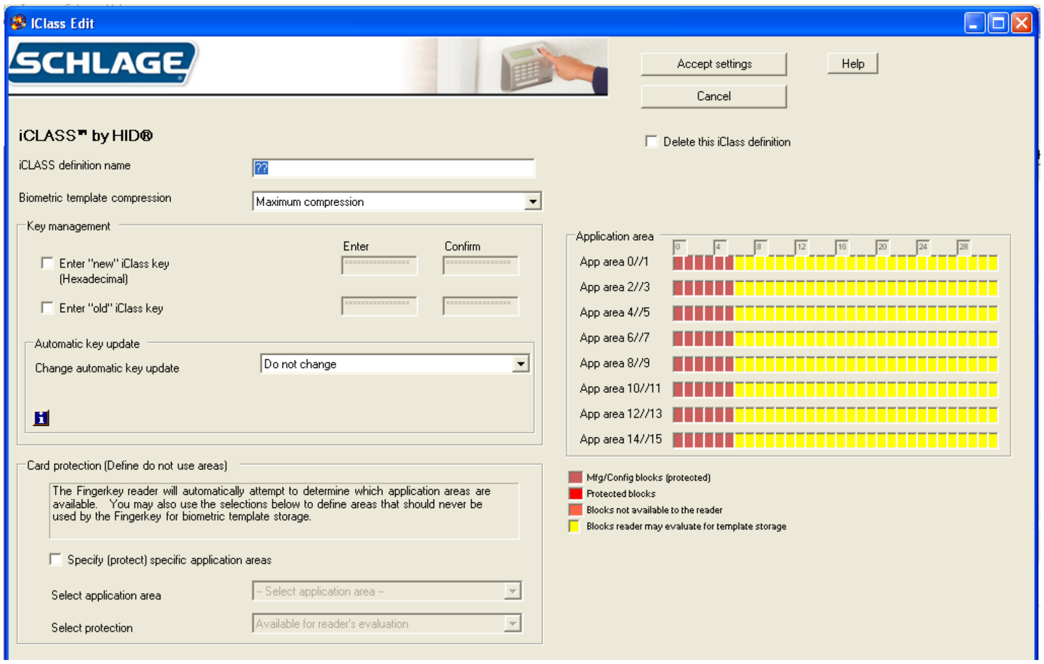
Figure 11-1: Smart Card Tab



Managing FingerKey iCLASS Definitions

iCLASS Definition Screen

Figure 11-2: iCLASS Definition Screen



iCLASS™ by HID®

☐ Delete this iClass definition

iCLASS definition name: ??

Biometric template compression: Maximum compression

Key management

	Enter	Confirm
☐ Enter "new" iClass key (Hexadecimal)	****************	****************
☐ Enter "old" iClass key	****************	****************

Automatic key update

Change automatic key update: Do not change

Card protection (Define do not use areas)

The Fingerkey reader will automatically attempt to determine which application areas are available. You may also use the selections below to define areas that should never be used by the Fingerkey for biometric template storage.

☐ Specify (protect) specific application areas

Select application area: -- Select application area --

Select protection: Available for reader's evaluation

Application area

App area 0//1
App area 2//3
App area 4//5
App area 6//7
App area 8//9
App area 10//11
App area 12//13
App area 14//15

🟥 Mfg/Config blocks (protected)
🟥 Protected blocks
🟥 Blocks not available to the reader
🟨 Blocks reader may evaluate for template storage

Add an iCLASS Definition

1. Click the *Smart Card* tab.
2. Click the *Create new iCLASS* button.
3. Complete the fields on the screen. See the iCLASS Definition Fields table on page 50 for more information.
4. Click the Accept settings button.

Edit an iCLASS Definition

1. Click the *Smart Card* tab.
2. Choose the iCLASS definition you want to edit from the drop-down box.
3. Click the *Edit selected iCLASS* button.
4. Complete the fields on the screen. See the iCLASS Definition Fields table on page 50 for more information.
5. Click the *Accept settings* button.

Delete an iCLASS Definition

1. Click the *Smart Card* tab.
2. Choose the iCLASS definition you want to delete from the drop-down box.
3. Click the *Edit selected iCLASS* button.
4. Click the *Delete this iCLASS definition* check box.
5. Click the *Accept settings* button.

iCLASS Definition Fields

Table 11-19: iClass Definition Fields

Field	Req’d?	Description
iCLASS definition name	Yes	• Name of the iCLASS definition • Any name that distinguishes this definition from others
Biometric template compression		• Controls the amount of compression of the finger template before it is written to the iCLASS card • Maximum compression should be used initially • See the iCLASS Card Compression table on page 51 for more information
Enter “new” iClass key		• A password that encrypts the areas used by the readers on iCLASS cards • Protects the fingerprint data from being read if the same cards are used with other devices. • 16 hex digits (0–9 and A–F.) • A default key is used when a new iCLASS definition is defined. Can be used permanently if desired. • For increased security, change this key periodically.
Confirm “new” iClass key		Confirmation of previous field

Field	Req'd?	Description
Enter "old" iClass key		• Old reader key, usually populated automatically. • Required for the reader to change the key. • All cards should be updated each time the key is changed, to ensure they key is always up-to-date. • See Resetting Old Card Keys on page 52 for more information.
Automatic Key Update		• Indicates whether readers using this definition can automatically change the key on a card. • Defaults to Do Not Change. Whatever setting was previously entered will continue to be used. If you're editing a previously created definition, click the i button to see what the current settings are. • Options: • Do Not Change: Use the previously entered setting. • Disable Auto Key Update: Prevents the reader from changing a key. • Start Unlimited Auto Key Update: Any card with the old key will be automatically updated when used at the reader. • Start Limited Auto Key Update: Any card with the old key will be automatically updated at the reader, until the number of cards and/or date specified is reached. • See Automatic Key Update on page 53 for more information.
Specify (protect) application areas		• Only check this box if you are sharing the iCLASS card with another iCLASS device that does not automatically determine the template location on the card. • See iCLASS Card Protection on page 52 for more information.

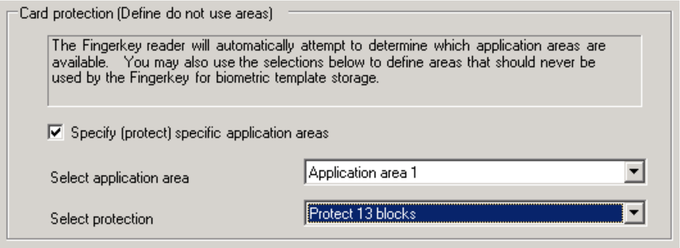
iCLASS Card Compression

Table 11-20: iCLASS Card Compression

	Number of Enrolled Fingers	
	1	2
No Compression	854 bytes	1654 bytes
Minimum Compression	566	1078
Medium Compression	454	854
Maximum Compression	310	566

iCLASS Card Protection

Figure 11-3: iCLASS Card Protection



Card protection (Define do not use areas)

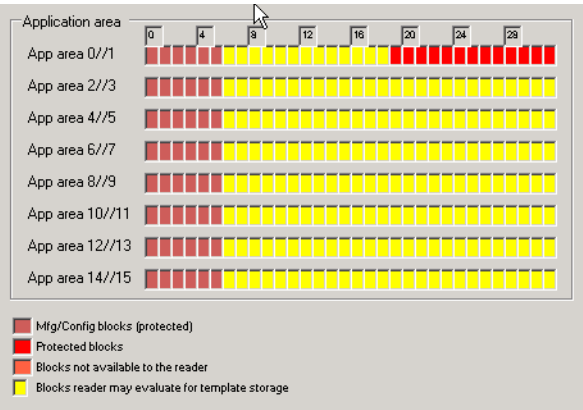
The Fingerkey reader will automatically attempt to determine which application areas are available. You may also use the selections below to define areas that should never be used by the Fingerkey for biometric template storage.

☑ Specify (protect) specific application areas

Select application area: Application area 1

Select protection: Protect 13 blocks

The grid on the right shows the protected blocks in red:



Application area

🟥 Mfg/Config blocks (protected)
🟥 Protected blocks
🟧 Blocks not available to the reader
🟨 Blocks reader may evaluate for template storage

You can protect multiple areas simply by choosing new values for each of these entries. You can clear any protected area by choosing the application area and choosing Available for Reader's Evaluation in the Select Protection drop down menu.

When you protect blocks in even application areas (0, 2, 4, etc.), blocks are used from the left to the right, that is, starting at block 6 and working up; when you protect areas in odd application areas (1, 3, 5, etc.), blocks are used from right to left, that is, starting at 31 and working down.

If you protect both even and odd sections in any pair (for example, if you protect parts of both area 0 area 1), then the fingerprint reader can't use that pair at all so the entire area is marked as protected.

! NOTE *Programmed iCLASS cards require application area 0 to be blocked off. To do this, click Select Application Area and pick Application Area 0 from the drop down menu. Then click Select Protection and choose Protect 26 blocks.*

Resetting Old Card Keys

To change the key for a previously used iCLASS card, the reader must know what the old key is—this prevents unauthorized people from converting other cards to work with your system. HandNet Lite keeps track of what the last key you used was, so most of the time, you don't need to change this entry.

For example, suppose you originally set the key to 1234123412341234 and then you entered a New Reader Key of 5678567856785678. HandNet Lite remembers the old key; it would automatically change cards to the new key if you set it to automatically update keys (see Automatic Key Update on page 53).

However, suppose in January you set the key to 1234123412341234, in February change it to 5678567856785678, and in March change it again to 9ABC9ABC9ABC9ABC. Cards that got used during February would have been updated to 5678567856785678; cards that didn't get used during February would still have January's key of

1234123412341234. The reader can automatically update those cards with the most recent old key (5678567856785678), but it would no longer recognize the prior old key of 1234123412341234. If you have a situation like this, to update the older cards, you must manually indicate what old key to use by checking the Reset Old Key checkbox and then entering the appropriate value in the old key entries.

If you have an older card and know that one of several keys was used on it but aren't sure which one, enter the various old keys in turn here, trying to update the card each time.

You can avoid ever having to do this if you make sure that all cards get updated each time you change your key.

Automatic Key Update

Some administrators want any reader to update the key; other administrators prefer to only let selected readers update cards. For example, for top security, you might only let a non-networked reader in a security office update cards so that was the only place they could be updated. To do this, the administrator would create one iCLASS definition for the public readers (with Automatic Key Update unchecked), and another iClass definition (Automatic Key Update checked) for the administrative reader.

If you disable automatic updates here, you can still manually update keys using the reader command menus.

If you return to this screen, this entry defaults to Do Not Change; this means that whatever setting was previously entered will continue to be used. If you're editing a previously created definition, click the ℹ button to see what the current settings are. (This button doesn't do anything when creating a new definition.)

Your choices are:

Do Not Change: Use the previously entered setting.

Disable Auto Key Update: This prevents the reader from ever changing a key. With this setting, to update cards, you would have to use a reader associated with another iCLASS definition that allowed updates, or you would have to manually update cards with the reader's command menus.

Start Unlimited Auto Key Update: If any card with the old key is used, this automatically updates the card to the new key. There's no limit to the number of cards that can be updated, and no limit on the date range.

Start Limited Auto Key Update: If any card is used that currently has this old key, this automatically updates the card to the new key until the number of cards and/or date specified in the following two entries is reached. For example, if you had 20 employees, you might set this to only automatically update 20 cards; once that was done, cards would not be automatically updated until you changed the key again. You could also specify a date; cards would then be automatically updated until that date, but would not be updated after that date.

Specify (protect) application areas

Only check this box if you are sharing the iCLASS card with another iCLASS device that doesn't automatically determine the template location on the card. If fingerprint readers are the only iCLASS device that you use with your cards, or if you use other device that also automatically choose an available space to store information, then you don't need to change this setting.

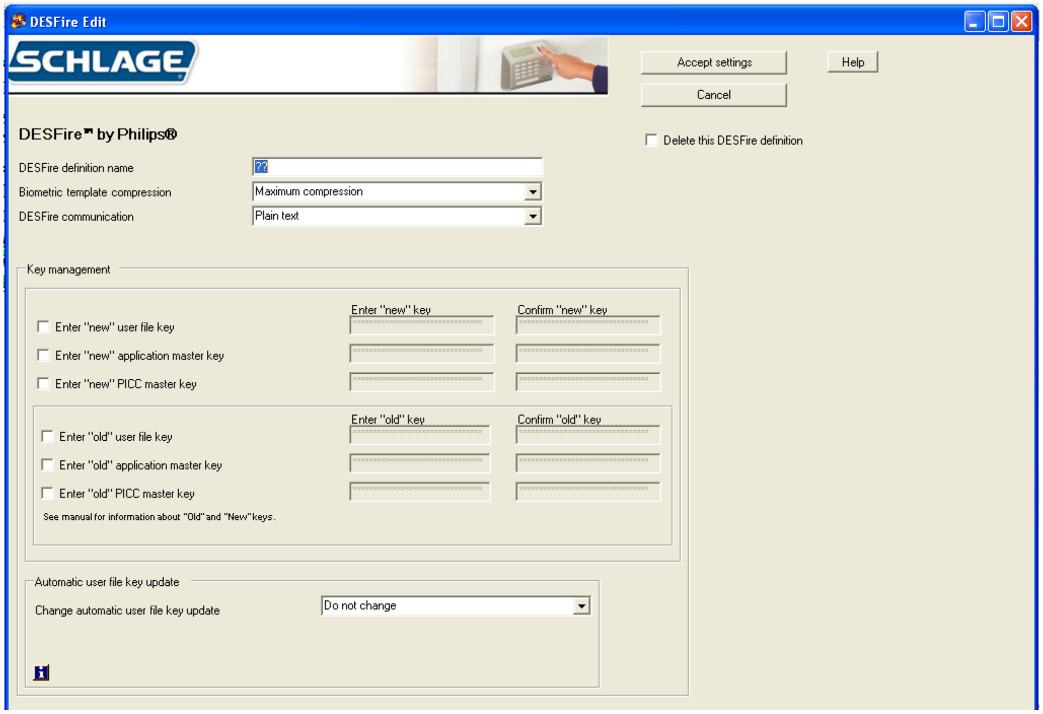
For example, Schlage Biometrics hand readers always store their templates in blocks 19–31 of area 1. If you were using the same iCLASS cards with both Schlage Biometrics hand readers and Schlage Biometrics fingerprint readers, you'd have to protect these blocks so a fingerprint template wouldn't get written in this area; if it did, the hand reader would write a template over it.

To protect these blocks, check the box by Specify (protect) application areas, click Select Application Area and pick Application Area 1 from the drop down menu, and click Select Protection and choose Protect 13 blocks from the menu:

Managing FingerKey DESFire Card Definitions

DESFire Definition Screen

Figure 11-4: DESFire Definition Screen



DESFire™ by Philips®

☐ Delete this DESFire definition

DESFire definition name: ??

Biometric template compression: Maximum compression

DESFire communication: Plain text

Key management

	Enter "new" key	Confirm "new" key
☐ Enter "new" user file key		
☐ Enter "new" application master key		
☐ Enter "new" PICC master key		

	Enter "old" key	Confirm "old" key
☐ Enter "old" user file key		
☐ Enter "old" application master key		
☐ Enter "old" PICC master key		

See manual for information about "Old" and "New" keys.

Automatic user file key update

Change automatic user file key update: Do not change

Add a DESFire Definition

1. Click the *Smart Card* tab.
2. Click the *Create new DESFire* button.
3. Complete the fields on the screen. See the DESFire Definition Fields table on page 56 for more information.
4. Click the *Accept settings* button.

Edit a DESFire Definition

1. Click the *Smart Card* tab.
2. Choose the DESFire definition you want to edit from the drop-down box.
3. Click the *Edit selected DESFire* button.
4. Complete the fields on the screen. See the DESFire Definition Fields table on page 56 for more information.
5. Click the *Accept settings* button.

Delete a DESFire Definition

1. Click the *Smart Card* tab.
2. Choose the DESFire definition you want to delete from the drop-down box.
3. Click the *Edit selected DESFire* button.
4. Click the *Delete this DESFire* definition check box.
5. Click the *Accept settings* button.

DESFire Definition Fields

Table 11-21: DESFire Definition Fields

Field	Req'd?	Description
DESFire definition name	Yes	• Name of the DESFire definition • Any name that distinguishes this definition from others
Biometric template compression	Yes	• Controls the amount of compression of the finger template before it is written to the DESFire card • Maximum compression should be used initially • See the DESFire Card Compression table on page 56 for more information
DESFire communication	Yes	Select either *Plain Text* or *DESFire* ciphered
Enter "new" user file key	Yes	• Check the box to edit these fields. • Key entered must be exactly the same in both boxes.
Enter "new" application master key	Yes	• Check the box to edit these fields. • Key entered must be exactly the same in both boxes.
Enter "new" PICC master key	Yes	• Check the box to edit these fields. • Key entered must be exactly the same in both boxes.
Enter "old" user file key	Yes	• Check the box to edit these fields. • Key entered must be exactly the same in both boxes.
Enter "old" application master key	Yes	• Check the box to edit these fields. • Key entered must be exactly the same in both boxes.
Enter "old" PICC master key	Yes	• Check the box to edit these fields. • Key entered must be exactly the same in both boxes.
Change automatic user file key update	Yes	The automatic user key update choices are: • Do not change • Disable auto key update • Start unlimited auto key update • Start limited auto key update (displays two additional fields) • With limited auto key update the operator can select the number of cards to be updated and/or the number of cards to automatically update.

DESFire Card Compression

Table 11-22: DESFire Card Compression

	Number of Enrolled Fingers	
	1	2
No Compression	854 bytes	1654 bytes
Minimum Compression	566	1078
Medium Compression	454	854
Maximum Compression	310	566

Managing FingerKey Mifare Standard Card Formats

Add a Mifare Standard Definition

1. Click the *Smart Card* tab.
2. Click the *Create new Mifare* button.
3. Complete the fields on the screen. See the Mifare Standard Definition Fields table on page 58, and the Mifare Standard Sector Fields on page 59 for more information.
4. Click the *Accept settings* button.

Edit a Mifare Standard Definition

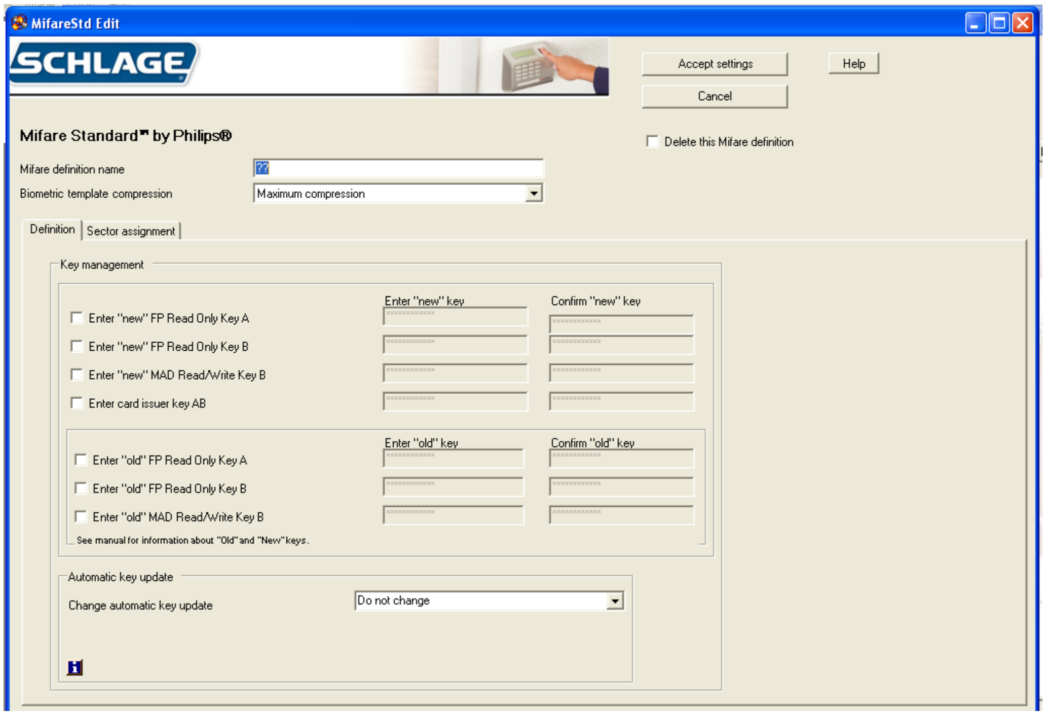
1. Click the *Smart Card* tab.
2. Choose the Mifare definition you want to edit from the drop-down box.
3. Click the *Edit selected Mifare* button.
4. Complete the fields on the screen. See the Mifare Standard Definition Fields table on page 58, and the Mifare Standard Sector Fields on page 59 for more information.
5. Click the *Accept settings* button.

Delete a Mifare Standard Definition

1. Click the *Smart Card* tab.
2. Choose the Mifare definition you want to delete from the drop-down box.
3. Click the *Edit selected Mifare* button.
4. Click the *Delete this Mifare* definition check box.
5. Click the *Accept settings* button.

Mifare Standard Definition Screen

Figure 11-5: Mifare Standard Definition Screen



Mifare Standard™ by Philips®

Mifare definition name: ??

Biometric template compression: Maximum compression

Change automatic key update: Do not change

See manual for information about "Old" and "New" keys.

MifareStd Edit
SCHLAGE
Accept settings
Help
Cancel
□ Delete this Mifare definition
Definition
Sector assignment
Key management
Enter "new" key
Confirm "new" key
□ Enter "new" FP Read Only Key A
□ Enter "new" FP Read Only Key B
□ Enter "new" MAD Read/Write Key B
□ Enter card issuer key AB
Enter "old" key
Confirm "old" key
□ Enter "old" FP Read Only Key A
□ Enter "old" FP Read Only Key B
□ Enter "old" MAD Read/Write Key B
Automatic key update

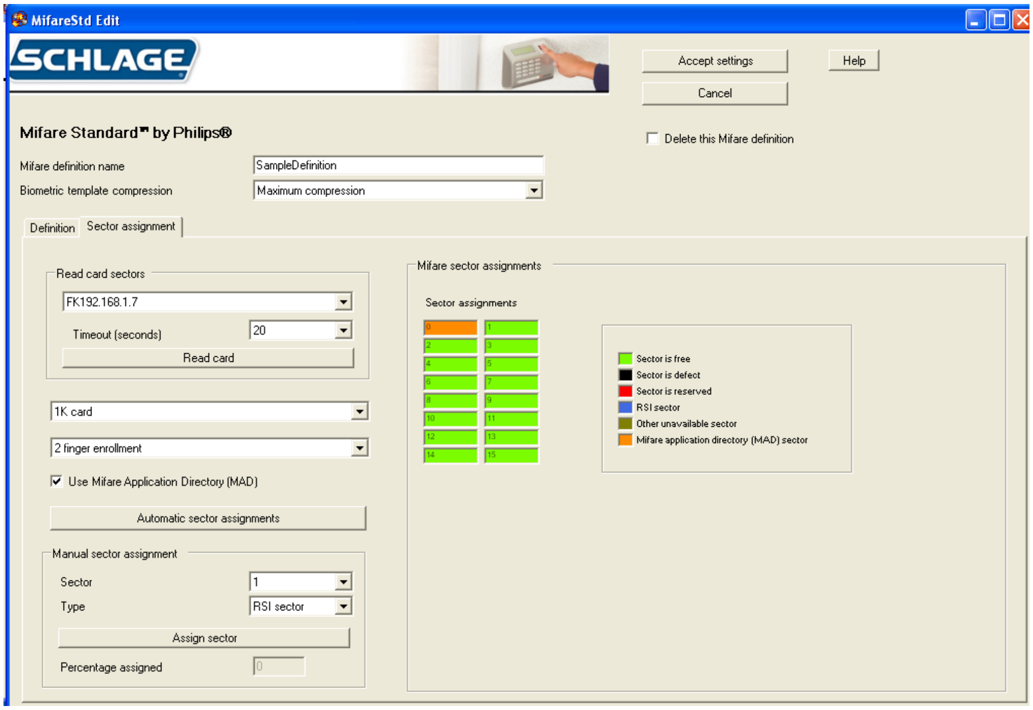
Mifare Standard Definition Fields

Table 11-23: Mifare Standard Definition Fields

Field	Req'd?	Description
Mifare definition name	Yes	• Name of the Mifare definition • Any name that distinguishes this definition from others
Biometric template compression	Yes	• Controls the amount of compression of the finger template before it is written to the Mifare card • Maximum compression should be used initially • See the Mifare Card Compression table on page 60 for more information
Enter "new" FP Read Only Key A	Yes	• Check the box to edit these fields • Key entered must be the same in both boxes
Enter "new" FP Read Only Key B	Yes	• Check the box to edit these fields • Key entered must be the same in both boxes
Enter "new" MAD Read/Write Key B	Yes	• Check the box to edit these fields • Key entered must be the same in both boxes
Enter card issuer key AB	Yes	• Check the box to edit these fields • Key entered must be the same in both boxes
Enter "old" FP Read Only Key A	Yes	• Check the box to edit these fields • Key entered must be the same in both boxes
Enter "old" FP Read Only Key B	Yes	• Check the box to edit these fields • Key entered must be the same in both boxes
Enter "old" MAD Read/Write Key B	Yes	• Check the box to edit these fields • Key entered must be the same in both boxes

Field	Req'd?	Description
Change automatic key update	Yes	The automatic key update choices are: • Diable auto key update • Start unlimited auto key update • Start limited auto key update (displays two additional fields) • With limited auto key update, the operator can select the number of cards to be updated and/or the number of cards to automatically update.

Figure 11-6: Mifare Standard Sector Assignment Screen



□ Delete this Mifare definition

Mifare definition name: SampleDefinition

Biometric template compression: Maximum compression

FK192.168.1.7

Timeout (seconds): 20

1K card

2 finger enrollment

☑ Use Mifare Application Directory (MAD)

Sector: 1

Type: RSI sector

Percentage assigned: 0

🟧 0	🟩 1
🟩 2	🟩 3
🟩 4	🟩 5
🟩 6	🟩 7
🟩 8	🟩 9
🟩 10	🟩 11
🟩 12	🟩 13
🟩 14	🟩 15

🟩 Sector is free
⬛ Sector is defect
🟥 Sector is reserved
🟦 RSI sector
▨ Other unavailable sector
🟧 Mifare application directory (MAD) sector

Mifare Standard Sector Fields

Table 11-24: Mifare Standard Sector Fields

Field	Req'd?	Description
Read card sectors		• Select the desired FingerKey to use in reading an existing Mifare Standard card • Select a card read timeout in seconds • Click the *Read card* button and present the Mifare Standard card to the reader • The card characteristics will be displayed • Use either Automatic Sector Assignment or Manual Sector Assignment to determine where the FingerKey will place the biometric template.
1K Card or 4K Card	Yes	• Allows you to tell HandNet Lite if the Mifare Standard cards you will be using have 1K or 4K capacity. • If you have used the *Read card* button described above, this will be filled in automatically.

Field	Req'd?	Description
Two finger enrollment or One finger enrollment	Yes	• Allows for storage of either one or two fingerprint biometric templates on the card.
Use Mifare Application Directory (MAD)	Yes	• Allows for use of a MAD (Mifare Application Directory) on the card. A MAD is stored in sector 0 (and 16 if a 4K card) and tells devices how the sectors on the card are allocated. • If unchecked, then you can assign any card sectors to fingerprint template storage.
Automatic sector assignments		• If *Use Mifare Application Directory* is checked, then clicking this button will instruct HandNet Lite to automatically assign the sectors on the card to be used for biometric template assignment (Schlage Biometrics Sector).
Manual Sector Assignment		• Allows you to manually assign the sectors for either biometric template assignment (Schlage Biometrics sector) or a free/available sector. You will need to assign sectors as Schlage Biometrics sectors until the percentage assigned is 100%.

As you use either Automatic or Manual sector assignment the display in the Mifare sector assignments group will change showing you the current assignment.

If your installation is currently using Mifare Standard cards with another device and you wish to add FingerKey biometrics to your existing cards you will wish to:

a. Determine if your current cards are formatted to use a Mifare Application Directory. Contact your existing device manufacturer. You can attempt to use the "Read card sectors" button in HandNet lite to attempt to read an existing MAD on the card.

b. If your current cards are not formatted to use a MAD, then you will need to determine which sectors your current device manufacturer uses on your card. It is normal that sector 0 will be used, but your current cards may also contain data in additional sectors. Check with your existing device manufacturer to determine which sectors on your cards are available and begin the Schlage Biometrics sector assignment at the first free sector.

Once you are satisfied with the card definition, click the "Accept settings" button to record the definition. You will then need to go back to the "Configuration" tab, and for each FingerKey to use this Mifare Standard definition you will need to "Edit selected reader", click "Fingerprint settings" and use the drop down for "Mifare standard configuration" and select the saved Mifare Standard Definition.

It is important that each FingerKey be assigned the correct Mifare standard configuration setting.

Mifare Card Compression

Table 11-25: Mifare Card Compression

	Number of Enrolled Fingers	
	1	2
No Compression	854 bytes	1654 bytes
Minimum Compression	566	1078
Medium Compression	454	854
Maximum Compression	310	566

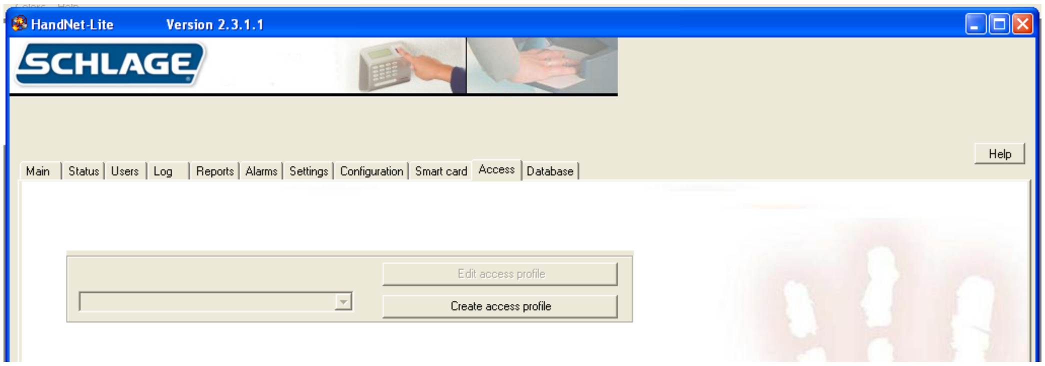
Access Tab

The Access Tab is used to add or edit access profiles. Access profiles define which type of user can use each reader.

For example, suppose your maintenance staff should have access to the maintenance rooms, your office staff should have access to the office, and your supervisors should have access to everything. You would create three access profiles: one for supervisors, one for office staff, and one for maintenance personnel. These profiles would identify which readers each group could use. After creating these profiles, whenever you added a user, you would identify which group the user was a part of, and the access profile for that group would automatically give the appropriate access.

If you want all users to be able to use every reader, you don't need to set up access profiles. HandNet Lite comes set up with an Always profile that lets users use any reader in the system. (It also has a Never profile that doesn't let the user verify at any reader.) You can't change or delete the Always or Never profile.

Figure 12-1: Access Tab



Add an Access Profile

1. Click the *Access* tab.
2. Click the *Create access profile* button.
3. Enter the access profile name.
4. Check the boxes next to the readers you want users with this access profile to be able to access.
5. Click the *Accept settings* button.

Edit an Access Profile

1. Click the *Access* tab.
2. Select the name of the access profile you want to edit from the drop-down box.
3. Click the *Edit access profile* button.
4. Edit the access profile name, if necessary.
5. Check the boxes next to the readers you want users with this access profile to be able to access.
6. Click the *Accept settings* button.

Delete an Access Profile

1. Click the *Access* tab.
2. Select the name of the access profile you want to delete from the drop-down box.
3. Check the box next to *Delete this access profile*.
4. Click the *Accept settings* button.

Figure 12-2: Access Profile Edit Screen

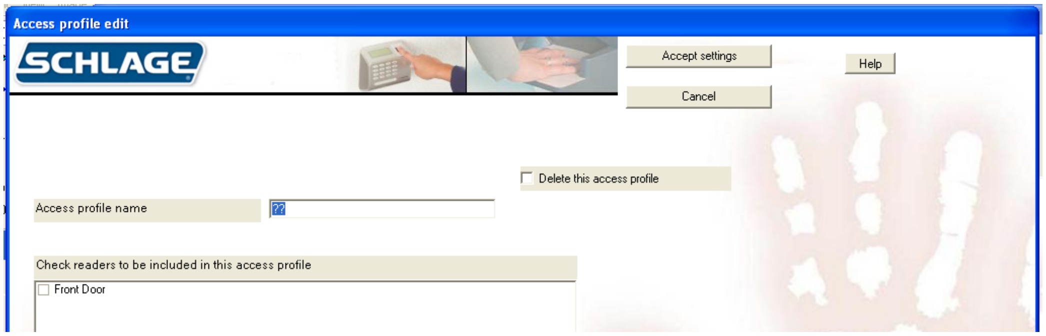


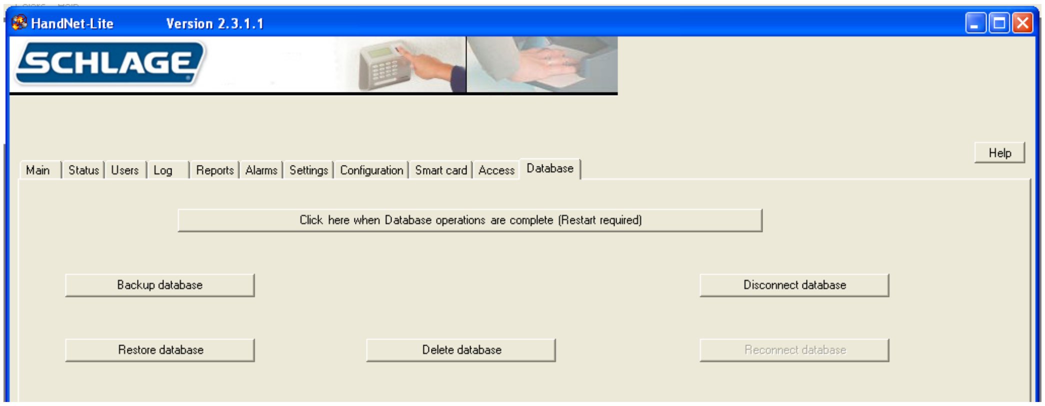
Table 12-26: Access Profile Fields

Field	Req'd?	Description
Access profile name	Yes	• Name of the access profile • Use a name that describes the group of users for which this access profile will be used. • Any combination of letters, numbers, spaces, and special characters up to 30 characters
Check readers to be included in this access profile	No	• Lists all the readers in the system • Check the box next to each reader you want users with this profile to be able to access. • Uncheck the box next to each reader you do not want users with this access profile to be able to access.
Delete this access profile	No	• Check to delete this access profile and remove it from the access profile list. • Access profiles that are assigned to users cannot be deleted. To remove an access profile from a user, see Edit a User on page 12. • If you delete the profile that is the default profile for reader enrollments, the next profile in the list will be selected. To choose a different default profile, go to the Settings window and choose the correct profile; see Settings Fields on page 25 for more information..

Database Tab

The Database Tab is used to backup, restore, delete, detach and attach the database.

Figure 13-1: Database Tab



Back Up the Database

The Backup database button is used to create a backup of the HandNet-lite database. The location of the backup will be displayed at the bottom of the screen:

1. Click the *Database* tab.
2. Click the *Backup database* button.
3. If you have completed all database operations you want to perform at this time, click the *Click here when Database operations are complete* button. See Finish Database Operations and Restart on page 64 for more information.

Restore the Database

The Restore database button is used to restore a backup file of the database.

1. Click the *Database* tab.
2. Click the *Restore database* button.
3. Select the backup file you want to use from the pop-up window and click the *Open* button.
4. If you have completed all database operations you want to perform at this time, click the *Click here when Database operations are complete* button. See Finish Database Operations and Restart on page 64 for more information..

Delete the Database

The Delete database button is used to delete the working copy of the database.

1. Click the *Database* tab.
2. Click the *Delete database* button.
3. Click the *Yes* button on the pop-up window.

   If you delete the database, you will lose all configuration and user information in the system. A new, empty database will replace the current database.

4. If you have completed all database operations you want to perform at this time, click the *Click here when Database operations are complete* button. See Finish Database Operations and Restart on page 64 for more information..

Disconnect the Database

The Disconnect database button is used to disconnect the database from the MS SQL Server Express database engine.

1. Click the *Database* tab.
2. Click the *Disconnect database* button.
3. If you have completed all database operations you want to perform at this time, click the *Click here when Database operations are complete* button. See Finish Database Operations and Restart on page 64 for more information..

Reconnect the Database

The Connect database button is used to reconnect the database to the MS SQL Server Express database engine.

1. Click the *Database* tab.
2. Click the *Reconnect database* button.
3. If you have completed all database operations you want to perform at this time, click the *Click here when Database operations are complete* button. See Finish Database Operations and Restart on page 64 for more information..

Finish Database Operations and Restart

Once you have completed all database operations you want to perform at this time, click the Click here when Database operations are complete button. This will cause HandNet-lite to exit. When you restart HandNet-lite it will take the following actions:

1. If a database is currently attached, HandNet Lite will use that database.
2. If a database is not currently attached, but database files exist, HandNet Lite will reattach the database files and continue.
3. If a database is not currently attached, and there is no database file, HandNet Lite will create a new database.

Appendix A

Table A-27: Card Formats

Type	Format	Description	Format detail
Wiegand formats	1	WC01 26 bit: 16 bit ID	Facility code: 8 bits, bit 2-9 ID: 16 bits, bit 10-25 1 2 12345678901234567890123456 PFFFFFFFFIIIIIIIIIIIIIIIIP EXXXXXXXXXXXX............. .............XXXXXXXXXXXXO
	2	WC02 32 bit: 22 bit ID	Facility code: 8 bits, bit 2-9 ID: 22 bits, bit 10-31 1 2 3 12345678901234567890123456789012 PFFFFFFFFIIIIIIIIIIIIIIIIIIIIIIP EXXXXXXXXXXXXXXX................ ................XXXXXXXXXXXXXXXO
	3	WC03 34 bit: 16 bit ID	Facility code: 16 bits, bit 2-17 ID: 16 bits, bit 18-33 1 2 3 1234567890123456789012345678901234 PFFFFFFFFFFFFFFFFIIIIIIIIIIIIIIIIP EXXXXXXXXXXXXXXXX................. .................XXXXXXXXXXXXXXXXA
	4	WC04 34 bit: 20 bit ID	Facility code: 12 bits, bit 2-13 ID: 20 bits, bit 14-33 1 2 3 1234567890123456789012345678901234 PFFFFFFFFFFFFIIIIIIIIIIIIIIIIIIIIP EXXXXXXXXXXXXXXXX................. .................XXXXXXXXXXXXXXXXO
	5	WC05 34 bit: 32 bit ID	ID: 32 bits, bit 2-33 1 2 3 1234567890123456789012345678901234 PIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIP EXXXXXXXXXXXXXXXX................. .................XXXXXXXXXXXXXXXXO
	6	WC06 35 bit: 20 bit ID	Facility code: 12 bits, bit 3-14 ID: 20 bits, bit 15-34 1 2 3 12345678901234567890123456789012345 PPFFFFFFFFFFFFIIIIIIIIIIIIIIIIIIIIP .EXX.XX.XX.XX.XX.XX.XX.XX.XX.XX.XX. .XX.XX.XX.XX.XX.XX.XX.XX.XX.XX.XX.O OXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
	7	WC07 37 bit: 19 bit ID	Facility code: 16 bits, bit 2-17 ID: 19 bits, bit 18-36 1 2 3 1234567890123456789012345678901234567 PFFFFFFFFFFFFFFFFIIIIIIIIIIIIIIIIIIIP EXXXXXXXXXXXXXXXXXX.................. ..................XXXXXXXXXXXXXXXXXXO
	8	WC08 37 bit: 35 bit ID	ID: 35 bits, bit 2-36 1 2 3 1234567890123456789012345678901234567 PIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIP EXXXXXXXXXXXXXXXXXX.................. ..................XXXXXXXXXXXXXXXXXXO

Type	Format	Description	Format detail
MagStripe formats	9	MS09 MAG1	ABA Track 2 Input ID len 25 Output min len 1 Output max len 25 Do trim leading zeroes Oriented right, no offset
	10	MS10 MAG2	ABA Track 2 Input ID len 25 Output min len 1 Output max len 25 Do trim leading zeroes Oriented left, no offset
	11	MS11 MAG3 Octal 7	ABA Track 2 Input ID len 7 Output min len 1 Output max len 25 Do trim leading zeroes Oriented right, no offset MS11 MAG3 Octal 7 is the format used for FingerKeys with a ProxIF reader.
	12	MS12 MAG 6 AT 5	ABA Track 2 Input ID len 6 Output min len 1 Output max len 25 Do trim leading zeroes Oriented left, offset 5

While these are the most common formats, you can define any additional formats that you need; see Managing Card Formats starting on page 45 for more information.

Custom Splash Screen

1. Shut down HandNet Lite
2. Create a bitmap (.bmp) image that is 100 x 100 pixels.
3. Save the image to the program directory: C:\Program Files\Schlage\HandNet_Lite\Splash100x100.bmp. This path may vary depending on your individual installation.
4. Restart HandNet Lite. The image should appear on the splash screen.

Index

Ingersoll Rand
Security Technologies

Ingersoll Rand's Security Technologies Sector is a leading global provider of products and services that make environments safe, secure, and productive. The Sector's market-leading products include electronic and biometric access control systems; time and attendance and personnel scheduling systems; mechanical locks and portable security, door closures and exit devices, steel doors and frames, architectural hardware and technologies and services for global security markets.

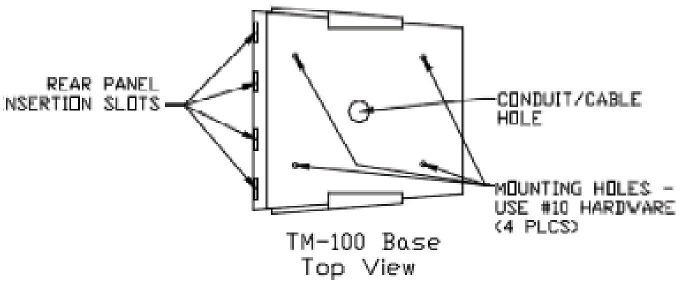
408.341.4110

www.schlage.com www.ingersollrand.com

Schlage
Biometric Solutions
Ingersoll Rand Security Technologies
1520 Dell Avenue
Campbell, CA 95008
Office: 866-861-2480/512-712-1413 (international)
Fax: 866-303-1794/408-341-4111
E-mail: sbssupport@irco.com

Installation Instructions

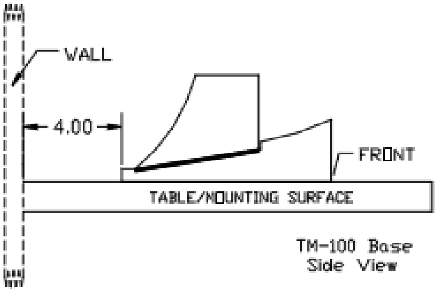
1. Secure the TM-100 base to table, pedestal or any other flat surface using #10 hardware.



TM-100 Base
Top View

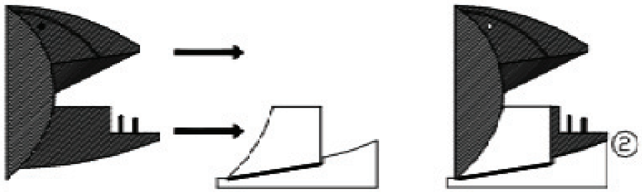
Note: If the reader is to be mounted near a wall, a minimum of four (4) inches must be maintained between the rear edge of the base and the wall.

2. If you plan to route cable through the base, insert cables up through the conduit/cable hole in the base. Guide the cables out past the rear edge of the TM-100 base.

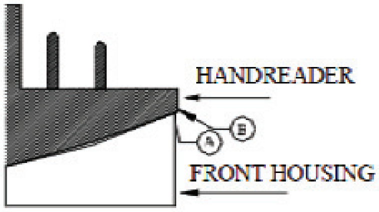


TM-100 Base
Side View

3. Slide the Handreader into the base. If the base is mounted near a wall the reader must be rotated into position.

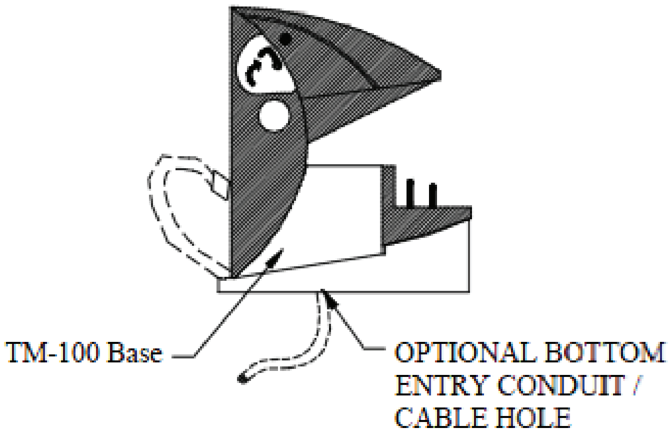


Note: Make sure the upper lip on the base (A) snaps under the lower lip of the Handreader (B).

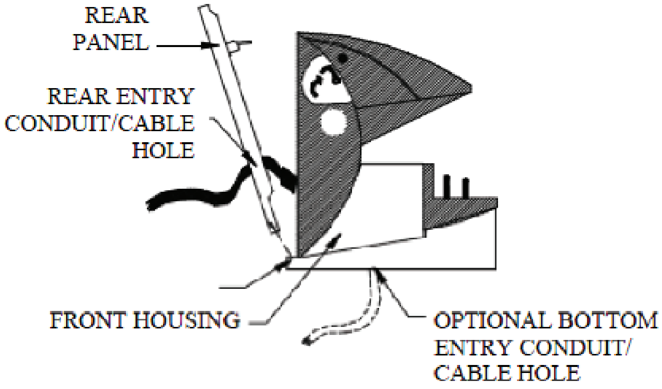


4. If you have not routed cabling through the base, insert cables through the conduit / cable hole in the rear panel. Connect the cables to the proper jacks on the Handreader. (See Handreader Installation Manual)

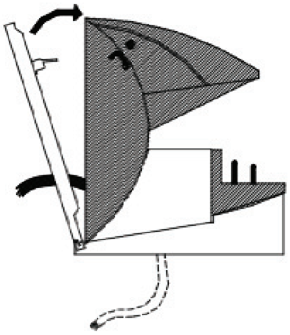
OR



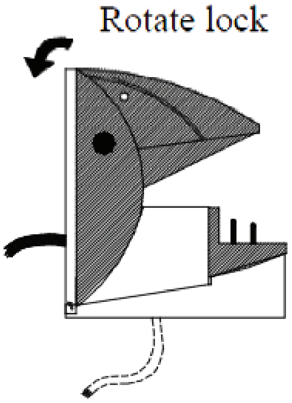
5. Insert the rear panel into the base. Align tabs on rear panel with slots on the base.


REAR PANEL
REAR ENTRY CONDUIT/CABLE HOLE
FRONT HOUSING
OPTIONAL BOTTOM ENTRY CONDUIT/ CABLE HOLE

6. Make sure the Handreaders lock is in the open position. While guiding the cables rotate the rear panel into the back of the Handreader.



7. Hold the rear panel against the Handreader making sure that the rear panel has fit into the base properly. Rotate the Handreaders lock into the locked position.



Installation of the TM-100 is complete.

SCHLAGE

HandNet for Windows

Terminal User's Guide

Ingersoll Rand
Security Technologies

Table of Contents

##

Getting Started

Introduction

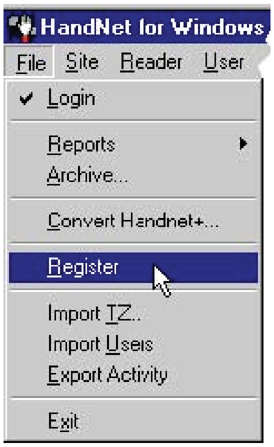
What HandNet Does

HandNet for Windows lets you control and monitor many connected HandKey readers. In this one program, you can control who can use each reader and when. You can also monitor activity and alarms for all readers at once.

Registering HandNet

After the first time you use this Version of HandNet, you have fourteen days to register it. You must register it even if you registered your previous Version of HandNet. If you do not register it within fourteen days, you will not be able to log into the program. The process should only take a minute.

1. If you have not logged into HandNet yet, log in; see page 4.
2. If the registration screen is not shown, pick *Register* from the *File* menu, and click the *Print the registration form* button on that screen.
3. Fill the form out and fax it to the number at the top of the form. Once we receive your completed form, we will fax an activation code back to you within two business days (since it could take two days for us to send your code back, please print and send the registration form now; do not wait until day fourteen).
4. Pick *Register* from the *File* menu, enter the activation code we sent, and click the *Activate* button. Once you do this, HandNet is permanently functional.



New Features in Version 2.0

HandNet for Windows Version 2.0 provides a number of new features, but these are only available to you if you purchased the upgrade to the full feature set. If you did not purchase this upgrade and you would like to, please contact your dealer; once you pay for the upgrade, we will send you a new access code to enter on the *Registration* screen. Once you enter this code, all the new features are immediately available to you.

How to tell if I have access to the new features

1. From the main menu bar, click the *Help* menu, and then click *About HandNet for Windows*.
2. Check the bottom of the box that pops up. To be able to use the new features, the last line must say *You may use all features of this software*. If this line says *Your current license does not let you use the enroll*..., you must contact your dealer and upgrade your license before you can use the new features (once you upgrade, we willsend you an access code that makes these feature available).

The new features

Enrolling Users from HandNet: Previously, to enroll a user you had to go to a features reader, enter command mode on the reader, and enroll the user. Now, if you have a reader that is near the computer, you can add the user in HandNet, select the reader to enroll at, and pick *Enroll* from the *Reader* menu without ever having to deal with command mode on the reader; see page 87.

User Access for a Limited Time Period: HandNet now lets you specify that a user's access should start and stop at certain days or times. For example, if a contractor needs access to your facility, you can now set the access to expire on the day that the contract ends. This gives you more complete control of who can access readers and when; see page 93.

Import/Export Users: If you have more than one computer system running HandNet and you want users added on one system to be available to the others, HandNet now lets you export user information from one program and import it into another; see page 99.

Exporting Activity for External Report Generation: If you want to create custom activity reports using some external report tool, *Export Activity* on the *File* menu sends all of your current activity to an access database file called expactvt.mdb; see page 116. While the main HandNet database files are password protected for security reasons, this file is not so you can open it and access any information in it at will. You can also set HandNet up to automatically export activity whenever you archive activity.

* * * * *

Getting Help in HandNet

The online help has the same information that is in this manual. To get help in HandNet, press F1. This brings up help for the screen you are on. From there, you can use the contents, index, or search tabs at the left of the help window to find any topic.

For Basic Topics

Click the *Contents* tab at the top of the left pane, click a book to open and click a topic. Not every topic is in the *Contents* tab, so if you do not find what you need, try the *Index* or *Search* tabs.

For Groups of Topics on a Single Theme

In addition to the contents you can also click on the pull-down list right under the *Previous/Next* buttons (in the bottom middle of the header). This list contains a number of important groups of topics. Once you are on one of these topics, the *Next* and *Previous* buttons work as well.

Screens and Menus

On menus and screens in this help, click any option on the screen to jump to help on that item.

When to Use the Index and When to Search

Use the index for main themes like adding a reader or enrolling a user. Use the search for minor points. For example, if you type *enroll* on the *Index* tab, you get three main topics that deal with enrolling users. On the *Search* tab, *enroll* gets you nearly thirty topics where *enroll* appears somewhere in the text. For main topics, the index gets you to what you want more directly. On the other hand, if you remembered that a screen somewhere said something about the number of tries a user gets before having access denied, the *Search* tab would check the entire text and find this detail for you. Use the *Index* tab to find items that are likely to be a main topic; use the search tab to find minor points.

Marking a Topic to Return to

To mark a topic in the help that you want to come back to:

1. Go to the topic that you want to mark.
2. Click the *Favorites* tab at the top of the left pane.
3. Click the *Add* button at the bottom of the pane. This adds the topic to your favorites list.

To get back to any marked topic later:

1. Click the *Favorites* tab at the top of the left pane of the help window.
2. Double-click the topic.

Getting In and Getting Out

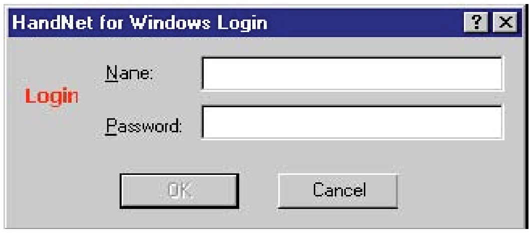
Starting HandNet

To start HandNet, either click the HandNet icon on your Windows desktop, or click the *Start* menu on your Windows taskbar, highlight *Programs*, and highlight and click *HandNet for Windows*.

Logging into HandNet

HandNet requires you to log in before you can make any changes; this prevents unauthorized people from changing information. If you are not logged in, you can look at the lists of activity, users, and readers (network), but you cannot change any information and cannot use any other options.

1. Click *Login* on the *Toolbar,* or pick *Login* from the *File* menu. The program brings up this box:



2. Type your name and password, and click *OK*.

If this is a new system: Use a name of *1234* and a password of *new* (change this name and password immediately so unauthorized people cannot user the program).

After initial setup: If you forget your name or password, see your supervisor or security administrator.

Passwords are NOT case sensitive. For example, if your password is *narnia*, then *Narnia* and *NARNIA* would also work.

After you are done using HandNet, be sure to log out again so unauthorized operators will not be able to use the program.

Changing the Initial Login Name and Password

HandNet comes set up with a login name of *1234* with a password of *NEW*. This lets you get into HandNet when you first start using it, but this is not secure; anyone may read this manual and find this name and password. To keep unauthorized users from using HandNet, change this password before you add any other information.

1. Click the *View* menu.
2. Click *Settings*.
3. Click the *Operators* tab.
4. Click the operator named *1234* and then click *Edit*. This takes you to the *Operator Definition* screen, which has settings for this user.
5. Change the *Name* to your name, and change the *Password* to something you will remember but that no one else will be able to guess. Click *OK* to return to the list of operators.

Remember the name and password you enter; if you forget it, you will not be able to get into HandNet. Do not change any other settings; this user is set up to use any option in HandNet; if you uncheck any boxes, you will not be able to use the corresponding options.

6. Click the *Close* button at the bottom of the box to close *System Settings*.

Logging out of HandNet

Log out of HandNet when you are done using it. This prevents unauthorized people from changing information. Someone who is not logged in can look at the lists of activity (including alarms), users, and readers, but cannot change any information or use any other options.

To log out, click the *Logout* button on the *Toolbar* or pick *Login* again from the *File* menu to uncheck it.

Exiting HandNet

For security purposes, you should generally log out of HandNet when you are done making changes so unauthorized people cannot add users or make changes. However, unless you are going to install a new Version of the HandNet software, or you need to restart the computer HandNet is running on, you do not typically want to exit from the HandNet program. If you exit (that is, shut down the program), you disconnect it from all readers. While all readers will continue to record activity and give access as appropriate, the program will not receive any information from the readers or process any alarms during the time that HandNet is not running. Because of this, you would usually leave HandNet running all the time.

* * * * *

Getting Started Overview

Procedure for Getting Started and Setting Up

QUICK STEPS

Getting Started with HandNet for Windows

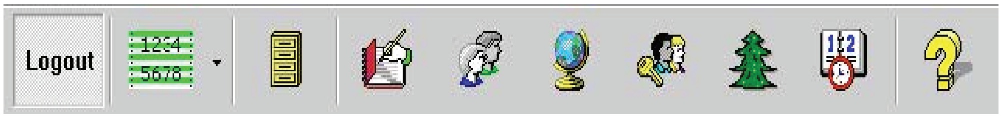
1. Log in; see page 4.
2. If you have not done so yet, register HandNet. HandNet will not let you log in after fourteen days if you do not register it; see page 1.
3. Change the initial password so unauthorized users will not be able to use the program; see page 4.
4. If you have been using readers without HandNet and you want to get the users from the reader(s):
    1. Pick *Settings* from the *View* menu.
    2. Click the *Security* tab.
    3. Check the box by *Do not delete unauthorized enrollments.*

    This prevents HandNet from deleting the users from the readers when you enable them (you will import the users from the reader later, after setting up the readers and sites). If you did not change this setting, when you enabled the site and reader, HandNet would regard all of the users in the reader as unauthorized (because they were not in HandNet yet), and it would delete them from the reader.
5. Set up site(s), that is, groups of connected readers; see page 33.
6. Set up readers; see page 42.
7. If you want to control which days and times users can access readers, set up time zones (see page 61) and holidays (see page 65).
8. If you have set up time zones and holidays, or if you want to give some users access through some readers but not others, set up access profiles; see page 67.
9. If you have previously been using one of our older MS-DOS products (HandNet Plus or HandNet), convert the users; see page 98 (if you have been using HandNet for Windows 1.09 or later, you do not need to convert anything; this Version of HandNet automatically updates information for the new Version).
10. If you have been previously using readers without one of the HandNet products and you need to get users from the reader(s), upload users from the reader(s); see *Getting User Information from a Reader* on page 99.
11. Add users; see page 74.
12. Enroll the users; see page 87.
13. When you are done using HandNet, be sure to log out so unauthorized people will not be able to add or change anything; see page 5.

Menus and Navigation

Toolbar

The toolbar looks like this:

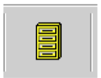
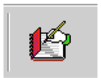
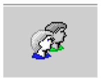
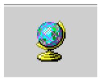


If you are not logged in yet, the first button will be a login button and a number of the other will be disabled.

Turning the Toolbar On and Off

Toolbar on the *View* menu turns it on or off.

Options on the Toolbar

Login	You see this button if you are not logged in yet. Click this button to login to HandNet; see page 4. Without logging in, you cannot make any changes or do anything other than look at basic information.
Logout	Once you log in, the first button changes to the *Logout* button. If you are going away from the computer, logging out prevents making unauthorized changes. If anyone could possibly get access to the computer in your absence, logging out is an important security precaution.
1234 5678 ▾	The main button lets you generate a custom activity report; see *Creating a Custom Activity Report from the Reports* Menu on page 105. The small arrow to the right pulls down the *Reports* menu; see page 13.
	This lets you archive older activity; see page 113.
	This opens the *Activity* window; see page 101. The *Activity* window lists all actions you take in HandNet, and actions or alarms from each reader. If the *Activity* window is already open and behind another window, this brings it to the front.
	This opens the *Users* window; see page 71. This lists everyone who is potentially able to access readers. If the *Users* window is already open and behind another window, this brings it to the front.
	This opens the *Network* window; see page 31. The *Network* window lists all of your sites, readers, and their current status. If the network window is already open and behind another window, this brings it to the front.

🔑	This takes you to the access profile settings; see page 67. Access profiles let you control which readers different types of users have access to and when.
🌲	This takes you to the holidays settings; see page 65. If users have different access on holidays than on other days, the holidays settings identify when those days are.
⏰	This takes you to the settings that let you define different periods of time when users can have access; see page 61 (in HandNet, we call these time zones, but there is no connection to the time zones we usually think of that have to do with different times around the world).
?	This pops up the online help for HandNet. The help contains the same information as this manual but arranged in a slightly different format. To get help for the screen you are on, you can also press F1 anywhere in HandNet. The help has a complete index and also lets you search for specific text; see page 3.

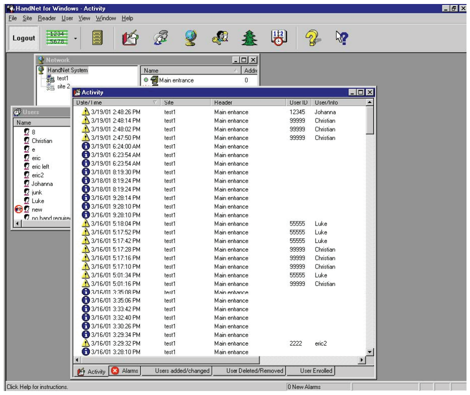
* * * * *

Tiling the Display Windows

HandNet lets you keep open the *Activity* window, the *Users* window, and the *Network* window (which shows sites and readers). If you have more than one window open, *Tile Horizontally* on the *Window* menu adjusts the open windows so they fill the Handnet window from side to side, and so they do not overlap and cover each other up.

Example of Windows that are NOT Tiled

Notice that the front windows cover up parts of the windows behind them and that the windows do not fill up the screen from side to side.



HandNet System
- test1
- site 2

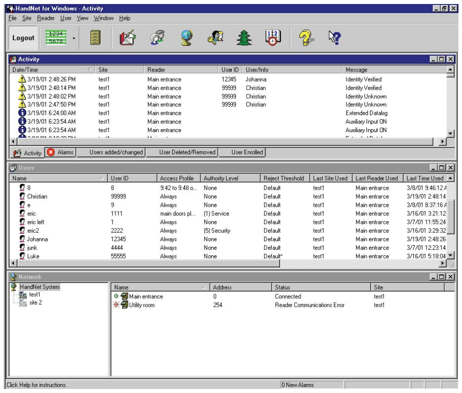
Name	Addr
Main entrance	0

Name
8
Christian
e
eric
eric left
eric2
Johanna
junk
Luke
new
no hand require

Date/Time	Site	Reader	User ID	User/Info
3/19/01 2:48:26 PM	test1	Main entrance	12345	Johanna
3/19/01 2:48:14 PM	test1	Main entrance	99999	Christian
3/19/01 2:48:02 PM	test1	Main entrance	99999	Christian
3/19/01 2:47:50 PM	test1	Main entrance	99999	Christian
3/19/01 6:24:00 AM	test1	Main entrance		
3/19/01 6:23:54 AM	test1	Main entrance		
3/19/01 6:23:54 AM	test1	Main entrance		
3/18/01 8:19:30 PM	test1	Main entrance		
3/18/01 8:19:24 PM	test1	Main entrance		
3/18/01 8:19:24 PM	test1	Main entrance		
3/16/01 9:28:14 PM	test1	Main entrance		
3/16/01 9:28:10 PM	test1	Main entrance		
3/16/01 9:28:10 PM	test1	Main entrance		
3/16/01 5:18:04 PM	test1	Main entrance	55555	Luke
3/16/01 5:17:52 PM	test1	Main entrance	55555	Luke
3/16/01 5:17:42 PM	test1	Main entrance	55555	Luke
3/16/01 5:17:28 PM	test1	Main entrance	99999	Christian
3/16/01 5:17:16 PM	test1	Main entrance	99999	Christian
3/16/01 5:17:10 PM	test1	Main entrance	99999	Christian
3/16/01 5:01:34 PM	test1	Main entrance	55555	Luke
3/16/01 5:01:16 PM	test1	Main entrance	99999	Christian
3/16/01 3:35:08 PM	test1	Main entrance		
3/16/01 3:35:06 PM	test1	Main entrance		
3/16/01 3:33:42 PM	test1	Main entrance		
3/16/01 3:32:40 PM	test1	Main entrance		
3/16/01 3:30:26 PM	test1	Main entrance		
3/16/01 3:29:34 PM	test1	Main entrance		
3/16/01 3:29:32 PM	test1	Main entrance	2222	eric2
3/16/01 3:28:10 PM	test1	Main entrance		

Example of Windows that ARE Tiled

Notice that none of these windows cover any parts of the other, and that the windows now fill up the screen from side to side.



Date/Time	Site	Reader	User ID	User/Info	Message
3/19/01 2:48:26 PM	test1	Main entrance	12345	Johanna	Identity Verified
3/19/01 2:48:14 PM	test1	Main entrance	99999	Christian	Identity Verified
3/19/01 2:48:02 PM	test1	Main entrance	99999	Christian	Identity Unknown
3/19/01 2:47:50 PM	test1	Main entrance	99999	Christian	Identity Unknown
3/19/01 6:24:00 AM	test1	Main entrance			Extended Datalog
3/19/01 6:23:54 AM	test1	Main entrance			Auxiliary Input ON
3/19/01 6:23:54 AM	test1	Main entrance			Auxiliary Input ON

Name	User ID	Access Profile	Authority Level	Reject Threshold	Last Site Used	Last Reader Used	Last Time Used
8	8	9:42 to 9:48 o...	None	Default	test1	Main entrance	3/8/01 9:46:12 A
Christian	99999	Always	None	Default	test1	Main entrance	3/19/01 2:48:14
e	9	Always	None	Default	test1	Main entrance	3/8/01 8:37:16 A
eric	1111	main doors pl...	(1) Service	Default	test1	Main entrance	3/16/01 3:21:12
eric left	1	Always	None	Default	test1	Main entrance	3/7/01 11:55:24
eric2	2222	Always	(5) Security	Default	test1	Main entrance	3/16/01 3:29:32
Johanna	12345	Always	None	Default	test1	Main entrance	3/19/01 2:48:26
junk	4444	Always	None	Default	test1	Main entrance	3/7/01 12:23:14
Luke	55555	Always	None	Default*	test1	Main entrance	3/16/01 5:18:04

HandNet System
- test1
- site 2

Name	Address	Status	Site
Main entrance	0	Connected	test1
Utility room	254	Reader Communications Error	test1

* * * * *

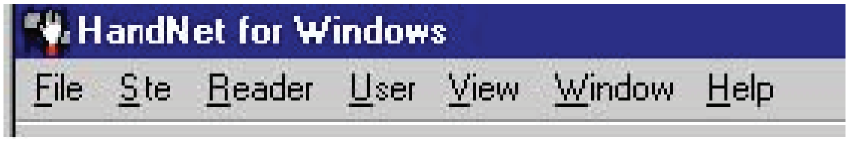
Menu Overviews

Pulling Down Menus with the Keyboard instead of the Mouse

If you prefer working from the keyboard rather than clicking with the mouse, you can hold the *ALT* key down and then type the underlined letter in the choice. For example, to open the *View* menu, you would hold *ALT* down and type *V* (this is often the first letter in the option, but not always).

Main Menu Bar

The main menu bar looks like this:



These menu options are briefly summarized below. The following pages contain more detail on the options on these menus.

File: The *File* menu lets you log in and out, generate reports, archive older activity, import setup information, and shut the program down; see page 11.

Site: The *Site* menu lets you add and change settings for sites (groups of connected readers); see page 14.

Reader: The *Reader* menu lets you add new readers, delete readers, and rename readers in the HandNet network. You can also unlock, relock, and lockup the selected reader, enroll a user at the selected reader, activate and deactivate an auxiliary device, and send (download) time, time zones, users, and setup configuration to selected readers; see page 15.

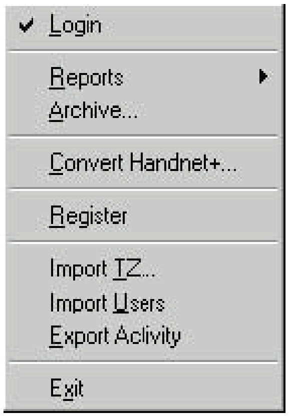
User: The *User* menu lets you add users, delete users, rename users, change information for a selected user, and create custom entries to collect additional information about users; see page 17.

View: The *View* menu lets you open the *Users, Activity, and Network* windows (the *Activity* window lists both activity and alarms; the *Network* window lists all of your sites and readers). The *View* menu also lets you turn the toolbar on or off. And it lets you get to access profiles, holidays, activity filters, time zones, and system settings (you do not need these options on an ongoing basis; these are normally only used when setting the program up); see page 18.

Window: The *Window* menu lets you switch between open windows, tile open windows horizontally on the screen, or switch panes within the *Network* window; see page 20.

Help: The *Help* menu lets you pop up the help system you are looking at now (you can also press F1 to pop up *Help*); see page 21.

File Menu



The *File* menu lets you log in and out, generate reports, archive older activity, import setup information, and shut the program down.

Login: You must log in to HandNet before you can do anything other than look at information; see page 4. You must log in to acknowledge alarms, add sites and readers, add or change users. When you are done using the program, click this same option again to log out so unauthorized operators cannot use the program.

Reports: This brings up another menu that lists several standard reports, and that lets you create custom reports based on the activity that you see in the *Activity* window; see page 13.

Archive: This takes older information from the current activity file and stores it in a separate file. Once you archive information, the activity is no longer visible in the *Activity* window, but you can still generate reports based on the archives.

Convert Handnet+: If you have been using HandNet+ or HandNet (our older MS-DOS programs), and are just switching to HandNet for Windows, this converts user information from HandNet+ and adds it to the user list in HandNet for Windows. Information imported includes: user name, user ID number, authority level, and reject threshold; see page 98.

Register: After the first time you use this Version of HandNet, you have fourteen days to register it. You must register it even if you registered your previous Version of HandNet. If you do not register it within fourteen days, you will not be able to log into the program. The process should only take a minute. To register HandNet:

1. If the registration screen is not shown, pick *Register* from the *File* menu, and print the registration form.

2. Fill the form out and fax it to the number at the top of the form. Once we receive your completed form, we will fax an activation code back to you within two business days (since this could take two days for us to send your code back, please print and send the registration form now; do not wait until day fourteen).

3. Pick *Register* from the *File* menu, enter the activation code we sent, and click the *Activate* button. Once you do this, HandNet is permanently functional.

Import TZ: This lets you change the access profile to *Always* or *Never* for many users based on information in a text file; see *Changing Access for Many Users at Once* on page 95.

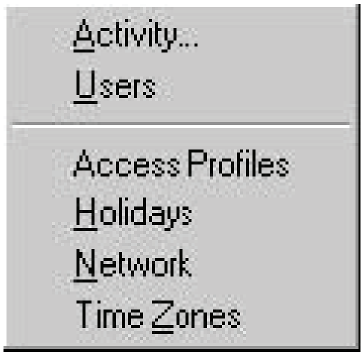
Import Users: If you have readers connected to several different computers (each with its own copy of HandNet) and if users added to one system need to be available on the others, *Import Users* lets you bring in users that were added or changed in another copy of HandNet; see page 99. If all of your readers are connected to a single copy of HandNet, you do not need this feature.

Export Activity: If you want to create custom activity reports using some external report tool, *Export Activity* sends all of your current activity to an access database file called *expactvt.mdb*; see page 115. The main HandNet database files are password protected for security reasons, but this file is not, so you can open it and access any information in it. If you are only going to generate reports with *Activity Reports* on the *File* menu, you do not need this option; using it would only create a file that you do not need.

Exit: This closes the HandNet program, disconnecting it from all readers. All readers will continue to be able to open doors, but the program will not receive any information from the readers or process any alarms while HandNet is not running. Unless you are going to install a new Version of the HandNet software, or you need to restart the computer that HandNet is running on, you do not want to exit the HandNet program. For security purposes, you would generally logout so unauthorized people cannot add users or make changes, but you would leave the HandNet program running all the time.

Reports Menu

To get to the reports menu, click *Reports* on the *File* menu. This menu lets you create custom activity reports and print several stock reports.



Activity: This lets you create reports based on any activity recorded by HandNet. This includes any information in the *Activity* window and any activity that you have chosen to archive. You can customize these reports to include only the information you need; see *Creating and Printing Custom Activity Views* on page 105.

Users: This lists all of the users in the system. The report includes each user's name, ID number, authority level, reject level, and access profile. It also indicates the last reader used, the last access time, and whether the user is enrolled. You can use this report to see if a user is enrolled and to make sure one user is not enrolled with multiple ID numbers. If you have created custom user entries, this report does NOT show any of them.

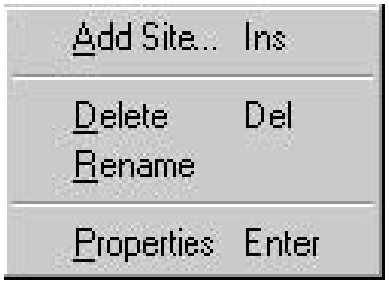
Access Profiles: If you have set up different access profiles to give different types of users access to different readers or at different times, then this report can help you see whether you have set your access profiles up the way you wanted. This report lists each access profile, sites and readers the profile gets access to, and the time zone that users can access each reader; see page 67 for more about setting up access profiles.

Holidays: This list all of the holidays you have set up in HandNet. It lists the name of each holiday, the month, and the date. This report helps you make sure you have correctly added all holidays for the year (if you have set up any time zones to prevent access on holidays, or to give different access on holidays than on other days, the *Holidays* list identifies when those holidays are. If you do not give different access on holidays than on other days, you do not need to set holidays up or print this report); see page 65 for more about setting up holidays.

Network: This report tells whether each site is enabled and connection information (communications port, baud rate, phone number or IP address, time adjustment, and modem speaker status). It also lists readers at the site, whether they are enabled, and their addresses. This report is used during setup to make sure the network is set up properly.

Time Zones: This lists all of the different user access period that you have set up (though we call these access periods *time zones*, they have no connection to the time zones we usually think of that have to do with different times around the world). The report includes the name of each time zone, the time periods it includes, and the days of the week those time periods apply. During setup, this report helps you see if you have set up all of the necessary time zones and configured them correctly (if you do not need to limit access by day or time -that is, if all users may use the readers twenty-four hours a day, seven days a week if they wanted- then you do not need time zones); see page 61 for more about setting up time zones.

Site Menu



In HandNet, a site refers to a group of up to thirty-two connected readers. Put another way, one reader is physically connected to the computer (by network, serial cable, or modem), and up to thirty-one additional readers can be daisy chained to that first reader; that is, a cable runs from the first reader to the second, another cable runs from the second to the third, and so on. We call this chain of readers a site. A site does not have any connection to a particular building or location; these readers could be in one building or in more than one building (if the buildings are close enough to run a cable from one to the other), and one building could have one or many sites.

Add Site: This adds a new site to the HandNet network; see page 34. You must set up a site in HandNet before you can set up readers.

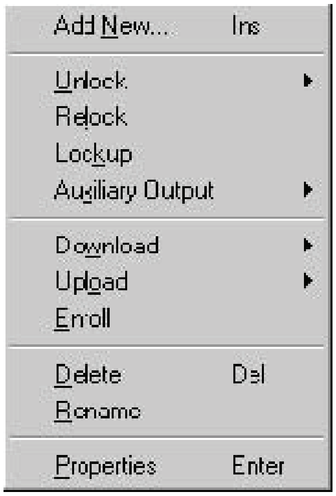
Delete: If you have selected a site in the Network window, *Delete* removes the site and all readers assigned to it. HandNet will ask you to confirm that you want to delete the site. Make sure that you have selected the appropriate site since, if you continue, you will not be able to undo the deletion unless you have made a backup of the files that contain your site and reader information (see page 126 for more about making backups).

Rename: If you have selected a site in the *Network* window, this lets you rename that site (you can also just click once on the site name in the *Network* window and rename it there without using this option). Renaming a site does not change any of its properties, and does not require you to set anything up again; it only changes the name that appears in the lists on the screen and in reports that you generate. You might want to rename a site if you discovered that the original name is not clear.

Properties: This takes you to a window with three tabs that let you look at or change settings related to how the site is connected to the computer with the HandNet software; see *Changing a Site* on page 34 for further detail.

Reader Menu

The *Reader* menu lets you add new readers, delete readers, and rename readers in the HandNet network. You can also unlock, relock, and lockup the selected reader, enroll a user at the selected reader, activate and deactivate auxiliary output, and send (download) time, time zones, users, and setup configuration to selected readers.



To do anything here, except add a reader, you must select one or more readers first.

Add Reader: This lets you add and configure a reader to the HandNet network; see page 42 (you must set up a site before you can add readers in HandNet).

Unlock: When you highlight *Unlock* on the *Reader* menu, you see another menu with two choices: *Indefinite* and *Timed*.

Indefinite unlocks the door connected to that reader and leaves it unlocked until you choose *Relock* on the *Reader* menu to lock it again. If you regularly want a door unlocked during certain hours, pick properties from the *Reader* menu and go to the *Configuration* screen. In the *Auto Unlock Time Zone* you can indicate when the door should be automatically unlocked. The program will automatically lock the door again at the end of the time zone.

Timed unlocks the door connected to that reader and leaves it unlocked only for the number of seconds specified on the *Configuration* page in the *Reader Properties* (that is, it unlocks the door for the same number of seconds that the door would be unlocked if it were opened by a reader).

See *Locking and Unlocking Doors* on page 130 for more about these options.

Relock: If you have unlocked a door with *Unlock, Indefinite* option, this locks it again; see page 128.

Lockup: This disables the lock on the door for the selected reader. The reader will still let users enter their ID numbers and still verify hands, but the door will stay locked even for valid users. The door will stay locked until you choose *Unlock* or *Relock*; see page 128.

Auxiliary Output: If an auxiliary device is connected to a reader, this lets you turn that device on or off for the selected reader; see page 129. *Auxiliary Output* can control local lighting, trigger a third party alarm system, activate a bell, and so on.

Download: This lets you send information to the selected readers. While HandNet automatically sends the appropriate information to readers, occasionally you will need to use this when correcting a problem with a reader; see *Resending Information to a Reader* on page 60.

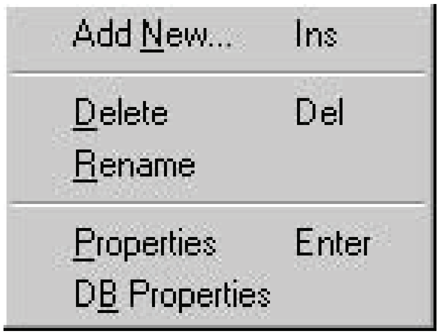
Upload (Users): This lets you get user information from the selected readers. You would do this if you had been using a reader independent of the HandNet program and now wanted to add all of the users stored in that reader to the program; see *Getting User Information from a Reader* on page 99.

Delete: This removes the selected readers from the HandNet network.

Rename: This renames the selected reader. Renaming the reader does not change any of its properties and does not require you to set anything up again; it only changes the name that appears in the lists on the screen and in reports that you generate. You might rename a reader if you discovered that the original name was not clear or if you changed the purpose of the areas the reader gave access to.

Properties: This takes you to a window with a number of tabs that let you look at or change a number of settings related to the reader; see *Changing Reader Settings with Reader Properties* on page 45.

User Menu



The *User* menu lets you add users, delete users, rename users, change information for a selected user, and create custom entries to collect additional information about users (if you have already set up users in a reader that you are connecting to HandNet, do not recreate those users; you can *Upload Users* from the reader; see *Getting User Information from a Reader* on page 99).

To change, delete, or rename users, select a user first on the list of users (for the list of users, pick *Users* from the *View* menu, or press *CTRL-U*).

Add New: This lets you add new users; see page 74. After you add the user, you must enroll the user (see page 87) before the user will have access through the readers.

Delete: This lets you remove a user from the program. You would do this if you never wanted that user to be able to use any of the readers in the HandNet network (if you might need the user again but want to keep the user from using any of the readers, you can also change the user's access profile to *Never*).

Rename: This lets you rename the selected user. You would use this if you entered the user's name incorrectly. You would also use this if you added multiple users at once. When you use *Add multiple new users* to add a number of users automatically, the program uses the ID number for the name. You would want to rename these users so you could identify which ID is for which user.

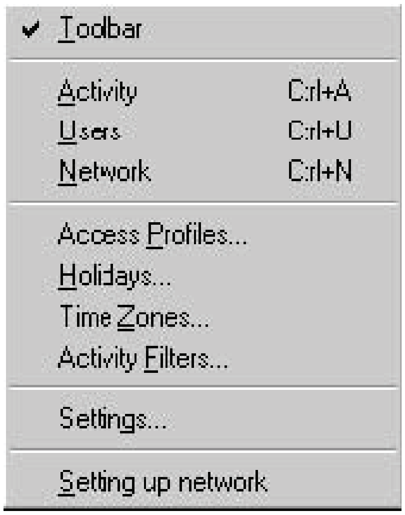
Properties: This lets you look at or change information for the selected user; see *Changing Users* on page 90.

DB Properties: This gives you a summary of the total numbers of enrolled and unenrolled users. It also lets you add custom entries so you can collect additional information about users. For example, depending on your needs, you might collect emergency phone numbers, birthdays, employment start dates, or any other information you needed about your users; see *Adding Custom User Entries* on page 97.

View Menu

The *View* menu lets you open the *Users, Activity,* and *Network* windows (the *Activity* window lists both activity and alarms; the *Network* window lists all of your sites and readers). The *View* menu also lets you turn the toolbar on or off.

It also lets you get to access profiles, holidays, activity filters, time zones, and system settings. You do not need these options on an ongoing basis; they are normally only used when setting HandNet up.



Toolbar: This turns the toolbar off if it is on and turns it on if it is off. The toolbar has icons that help you quickly get to common options; see page 7. The toolbar is shown when you start HandNet. A check is shown by this option when the toolbar is displayed.

Activity: This opens the *Activity* window (or brings it to the front if it is already open and behind other windows). This lets you see recent activity and alarms. If you have created any activity filters to create lists of specific types of activities, these views are also available here. The tabs at the bottom of this window let you switch between the activity list, the alarm list, and any custom views you have created; see page 101 for more about the *Activity* window.

Users: This opens the *Users* window (or brings it to the front if it is already open and behind other windows). This window lists everyone who could potentially gain access through a hand reader; see page 71 for more about the users window (there is no connection between this list and the operators authorized to use HandNet; for people who can use HandNet, see the *Operators* tab in *System Settings* on page 24).

Network: This opens the *Network* window (or brings it to the front if it is already open and behind other windows). This window lists all of your sites and readers; see page 31 for more about the *Network* window.

Access Profiles: If some users can only use certain hand readers and/or only use them at certain times or on certain days, access profiles define when each type of user can use each reader. For example, suppose your maintenance staff should have access to the maintenance rooms seven days a week, your office staff should have access to the office but only during business hours, and your supervisors should have access to everything at any time. You would create three access profiles: one for supervisors, one for office staff, and one for maintenance personnel. These profiles would identify which readers each group could use. In these profiles you would also identify which time periods each group could use the different readers (you would set up these time periods first using time zones). After creating these different profiles, whenever you added a user, you would just identify which group the user was a part of, and the access profile for that group would automatically give the appropriate access; see page 67 for more on setting up access profiles.

To limit access to certain days or times, you must set up time zones before creating access profiles.

If you want all users to be able to use every reader any time, you do not need to set up access profiles. HandNet comes set up with an *Always* profile that lets users use any reader in the system twenty-four hours per day, seven days per week. It also has a *Never* profile that does not let the user verify at any reader at any time.

Holidays: If you have set up any time zones to prevent access on holidays or to give different access on holidays than on other days, the holidays list identifies when those holidays are. If you do not give different access on holidays than on other days, you do not need to use this option; see page 65 for more on setting up holidays.

Time Zones: If you want some users to be able to use certain readers only during certain hours or on certain days of the week, time zones let you identify when access is available. For example, suppose some users should only to be able to gain access through certain readers between 8:00 AM and 5:00 PM, Monday through Friday. You would create a time zone that identified these times and days, associate that time zone with appropriate readers using an access profile, and then assign that access profile to the users. After you did this, users with that access profile would only have access during the times you identified in the time zone; see page 61 for more on setting up time zones.

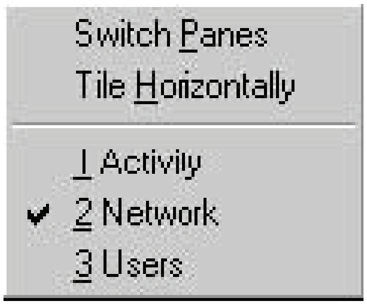
If you do not need to limit access by day or time (that is, if users could use the readers twenty-four hours a day, seven days a week if they wanted), then you do not need to set up time zones.

Activity Filters: This lets you customize the information you see in an activity window by letting you identify the dates, times, sites, readers, users, message types, and messages you want to see. For example, suppose you want to see who's come in through the main entrance without having to wade through messages related to activity at other readers. You could create an activity profile that listed activity only from the main entrance reader and only if the activity was *Identity verified* (the message you get when someone enters an ID and the hand is recognized). You would then be able to choose this view and see only this activity. Activity filters can be much more complex than this; they can filter or limit an activity list to include any subset of information you need (after you create an activity filter, a tab at the bottom of the activity window will list the name of the filter; just click that tab for the corresponding information); see *Creating a Custom Activity View* on page 105 for more information.

Settings: This lets you look at or change system-wide settings; see page 22. This includes the name of the system, security, who can use HandNet, which messages trigger alarms, when old messages should be archived, and settings for importing and exporting users.

Window Menu

The *Window* menu lets you switch between open windows, tile open windows horizontally on the screen, or switch panes within the *Network* window.



You will see a check mark to the left of the window that is currently active.

Switch Panes: If the *Network* window is open, *Switch Panes* switches you back and forth between the list of sites in the left pane of the window, and the list of readers in the right pane of the window. This is primarily useful for users who cannot use a mouse; if you can use a mouse, it is easier to just click the pane you want. If the *Network* window is not open, this choice does not do anything.

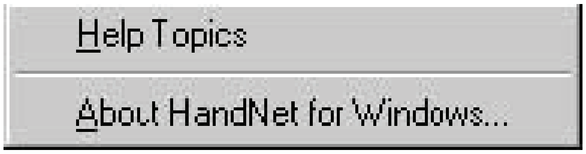
Tile Horizontally: This adjusts any open windows so they fill the HandNet window from side to side and so they do not overlap and cover each other up. If you are not sure what tiling is, see the example on page 9.

Activity: This choice is only here if you have the *Activity* window open. This makes the *Activity* window the active window (if the *Activity* window is not open, open it by typing *CTRL-A* or by picking *Activity* from the *View* menu). The *Activity* window shows the activity log, error messages, and any custom activity views you have created; see page 101 for more about the *Activity* window.

Network: This choice is only here if you have the *Network* window open. This makes the *Network* window the active window. The *Network* window lists sites and readers (if the *Network* window is not open, open it by typing *CTRL-N* or by picking *Network* from the *View* menu); see page 31 for more about the *Network* window.

Users: This choice is only here if you have the *Users* window open. This makes the *Users* window the active window (if the *Users* window is not open, open it by typing *CTRL-U* or by picking *Users* from the *View* menu); see page 71 for more about the *Users* window.

Help Menu



Instead of going to the *Help* menu, you can press *F1* from any screen in HandNet. This takes you to help for the screen you are on. If you need help on something else, you can use the *Contents, Index*, or *Search* tabs at the left of the window to find what you need.

Help Topics: This brings you into the help for HandNet. The *Help* menu contains the same information as this manual, but it lets you more easily search and jump from topic to topic; see page 3.

About HandNet for Windows: This brings up a screen with copyright information, the Version of the program, the product serial number, and the name of the person or company the product is licensed to (unless you need to give your serial number or the program Version number to one our support representatives, or unless you need to check to see if you are licensed to use all the features of the program, you probably will not need to come to this screen).

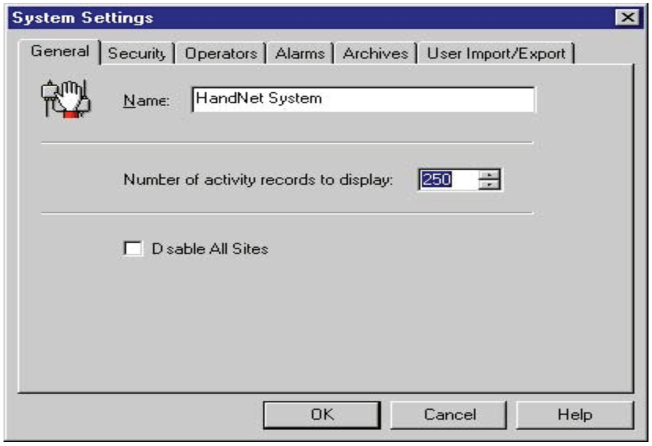
* * * * *

System Wide Settings

Settings on the *View* menu lets you control setup issues that are not related to specific sites or readers. This includes the name of the system, what user changes should be allowed at readers, who can use Handnet, which messages trigger alarms, when old messages should be archived, and settings for importing and exporting users.

General System Settings

To get to the *General* tab, pick *Settings* from the *View* menu.



Name: HandNet System

Number of activity records to display: 250

☐ D sable All Sites

Name of System

Name: This shows the name that appears above the list of sites in the *Network* window.

Amount of Activity to Show

Number of Activity Records to Display: This shows how many of the most recent activities to list in the *Activity* window. HandNet stores activities even after they are no longer listed in the *Activity* window; those that are no longer shown are still stored and still included if you print a report.

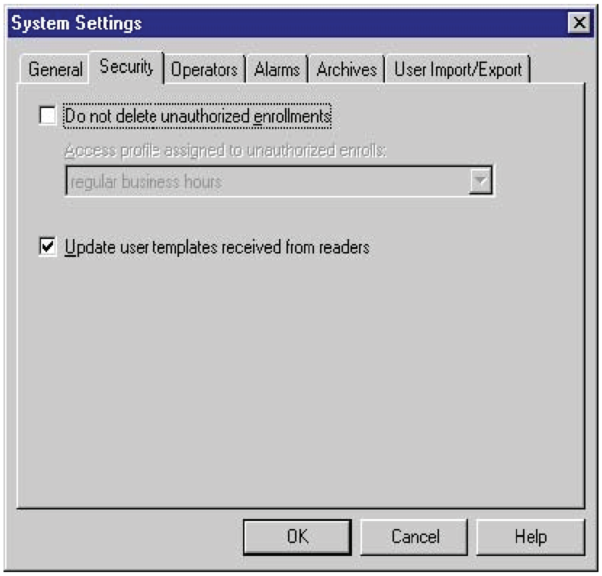
Disable All Sites

Disable All Sites: Check this box if you need to quickly prevent HandNet from trying to communicate with any site. You might check this if you were servicing a number of sites at once.

* * * * *

What User Changes Can Come from Readers

To get to the *Security* tab, pick *Settings* from the *View* menu, and then click the *Security* tab.



□ Do not delete unauthorized enrollments

Access profile assigned to unauthorized enrolls:

regular business hours

☑ Update user templates received from readers

Whether Users can be Added at the Reader

Do not delete unauthorized enrollments: When this is not checked (HandNet's initial setting) you can only add new users in HandNet; you cannot add a new user directly at the reader (you can add a user at a reader if the user is in HandNet so you can enroll the user, but if you add a user at the reader that has not been added in HandNet, HandNet will delete the new user). If you want to be able to add and enroll a new user at a reader without adding the user in HandNet first, check this box. If you allow this, and if you add a new user from the reader, the user will be given the access profile selected in the entry below (you can change the access profile on the *Security* tab in *User Properties*; see page 92).

Access profile assigned to unauthorized enrolls: Indicate what access profile should be given to a user who is added at a reader (if you do not want the user to be able to access any readers until you change them in HandNet, choose *Never*).

Whether to Revise the Stored Images of Users' Hands

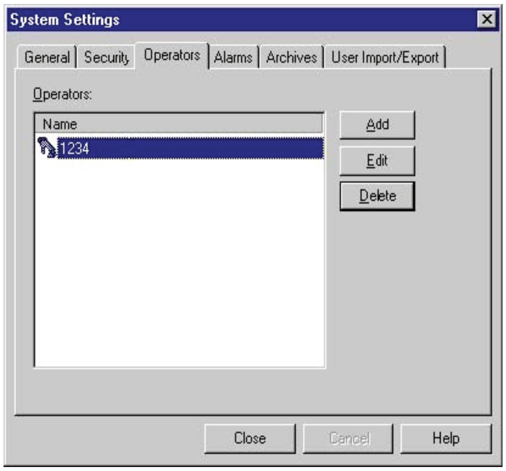
Update user templates received from readers: When you enroll a user, HandNet stores a template that contains information about the shape of the user's hand. If this box is checked, then each time a user gains access, HandNet updates this template. This means that if the user's hand changes gradually (for example, if the user gains or loses a significant amount of weight over time), the image of the user's hand in HandNet will automatically be gradually adjusted as well. If there are gradual changes, checking this prevents users from having access problems as their hands become increasingly different from the original image. If you do not check this, then readers will always compare the user's hand to the original image created when you enrolled the user. We recommend having this checked.

* * * * *

Who Can Use HandNet

The *Operators* tab lists those people who are authorized to use the HandNet program. When you click *Add* or *Edit*, the program brings up the *Operator Definition* box where you control which tasks the operator is allowed to do in HandNet.

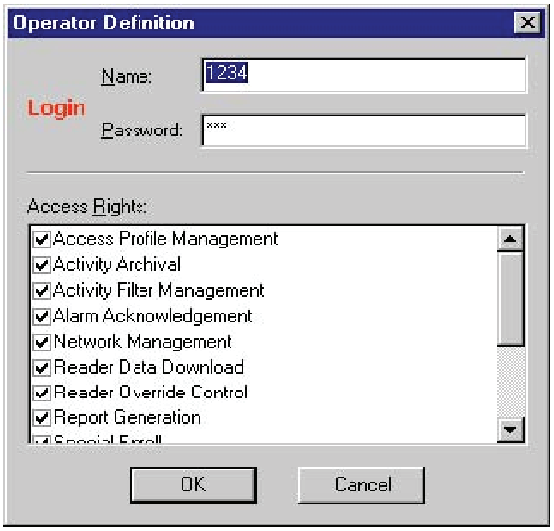
To get to this screen, pick *Settings* from the *View* menu, and then click the *Operators* tab.



1234

Adding or Changing an Operator

You see this box when you add or edit an operator. It has the name and password the operator must use to log into HandNet. The boxes that are checked control which types of activities the operator can do.



Name: 1234

Password: ***

Access Rights:

- ☑ Access Profile Management
- ☑ Activity Archival
- ☑ Activity Filter Management
- ☑ Alarm Acknowledgement
- ☑ Network Management
- ☑ Reader Data Download
- ☑ Reader Override Control
- ☑ Report Generation
- ☑ Special Enroll

Name: Enter the name that the operator will enter on the *Login* screen; see page 4. If the operator is also a user in HandNet (so s/he can gain access through readers), the name you enter here does NOT have be the same as the name in *User Properties*.

Password: Enter the password that the operator will enter on the *Login* screen. Passwords are NOT case sensitive. For example, if the password is *narnia, Narnia* and *NARNIA* would work identically.

Which Options the Operator Can Use

Access Rights: Check the corresponding boxes to determine which tasks the operator can do in HandNet. When you add a new operator, all of the boxes are unchecked; unless you check them, the operator will be able to do little more than look at information on the screen.

Click OK to save your changes and return to the list of operators.

Deleting an Operator

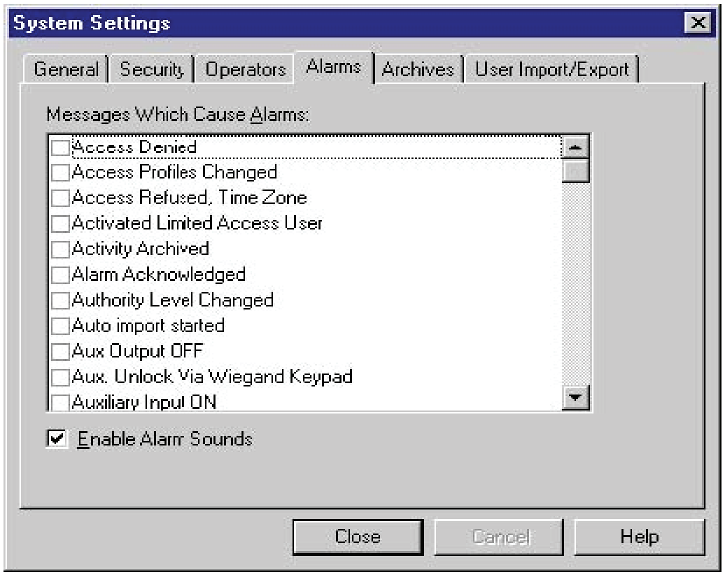
To delete an operator so that person will no longer have access to HandNet, click the operator in the list and click *Delete*. HandNet does NOT ask you to confirm this deletion, so make sure you have highlighted the right operator before you click delete.

If the operator is also a user and if you do not want the user to have access to readers anymore, you must also delete the person from the user list.

* * * * *

Which Messages Trigger Alarms

The *Alarms* tab controls which activities generate alarms in HandNet. To get to this screen, pick *Settings* from the *View* menu, and then click the *Alarms* tab.



Messages Which Cause Alarms:

□ Access Denied
□ Access Profiles Changed
□ Access Refused, Time Zone
□ Activated Limited Access User
□ Activity Archived
□ Alarm Acknowledged
□ Authority Level Changed
□ Auto import started
□ Aux Output OFF
□ Aux. Unlock Via Wiegand Keypad
□ Auxiliary Input ON

☑ Enable Alarm Sounds

Messages That Cause Alarms

Messages Which Cause Alarms: Check each message that should generate an alarm. What you check here only determines what triggers an alarm in the HandNet program; if you are connected to an auxiliary or external alarm system, actions that trigger external alarms are controlled by the *Auxiliary (AUX) Settings* (see page 48) and *Extended Setup* (see page 51) tabs in *Reader Properties*.

Alarms Sounds

Enable Alarm Sounds: If this is checked, then when an alarm situation occurs, a loud, siren-like alarm sound will begin and continue until you acknowledge the alarm. If this is not checked, when an alarm situation occurs, you will see a red flashing message at the bottom of the screen but will not hear any sound.

* * * * *

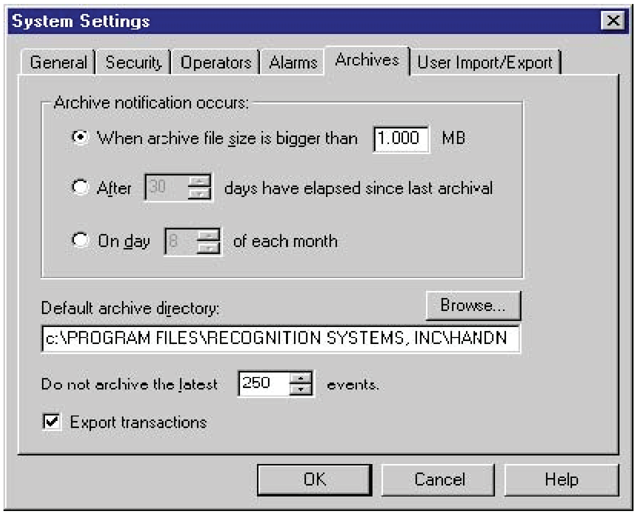
When Past Activity Gets Archived

What Archiving Is

Archiving is moving past activity from the current activity file to a separate file. This keeps the activity file smaller and faster while still keeping the information available for reports if needed. The *Archive* tab controls when HandNet reminds you to archive past activity, where it will make the archive file if you do not choose another location, and the minimum amount of activity to keep available in the current activity file.

You can make an archive at any time use *Archive* on the *File* menu; see page 113.

To get to the *Archives* tab, pick *Settings* from the *View* menu, and then click the *Archives* tab.



Archive notification occurs:

● When archive file size is bigger than 1.000 MB

○ After 30 days have elapsed since last archival

○ On day 8 of each month

Default archive directory: c:\PROGRAM FILES\RECOGNITION SYSTEMS, INC\HANDN

Do not archive the latest 250 events.

☑ Export transactions

When HandNet Reminds You to Make and Archive

Archive Notification Occurs: This controls when HandNet reminds you to make an archive.

When archive file size is bigger than... reminds you only when there is enough activity for the archive file to reach the size you enter. How long it will take depends on the amount of activity.

After ___ days... reminds you make an archive on a regular basis regardless of the amount of activity during that period. For example, if you wanted to make an archive once a year, you could select this option and enter 365 for the number of days.

On day ___of each month reminds you make an archive once a month. If you want to include all activity from a particular month in the archive, and you also want to keep a number of days worth of recent activity available in the activity window, then you might want to do this later than the first of the month and change the *To* date to the last day of the previous month when you make the archive. For example, if you wanted to keep activity from the past week in the current activity, then you might not make your monthly archive until the 8th of the month. That way, when you have made your archive through the end of the previous month, the past week would still be in the current activity.

Default Archive Directory: This shows the drive and directory (folder) that is automatically filled in for the file location when you make the archive. This is initially set to the same folder that the HandNet program is in, but you can change this if you wish.

What NOT to Archive

Do Not Archive the Latest __ Events: This indicates how many events or activities to keep in the current activity file. You can choose from 1-500. When you make an archive, HandNet this number of the most recent events in the activity file. If you want to keep more events than this in the current activity file, you can do this when you make the archive by changing the *To* date. For example, if you always wanted to keep at least the activity for the past week, when you make the archive, you could set the *To* date a week in the past.

Exporting Activity When Archiving

Export Transactions: If you check this, then whenever you make an archive, HandNet exports all the transactions being archived to an access database file called *expactvt.mdb* (you can also export transactions with *Export Activity* on the *File* menu; see page 115). While the main HandNet database files are password protected for security reasons, this file is not. This lets you create custom activity reports using the activity from HandNet using external report generating tools. If you are only going to generate reports with *Activity Reports* on the *File* menu, you do not need to check this box; doing so would only create a file that you do not need.

* * * * *

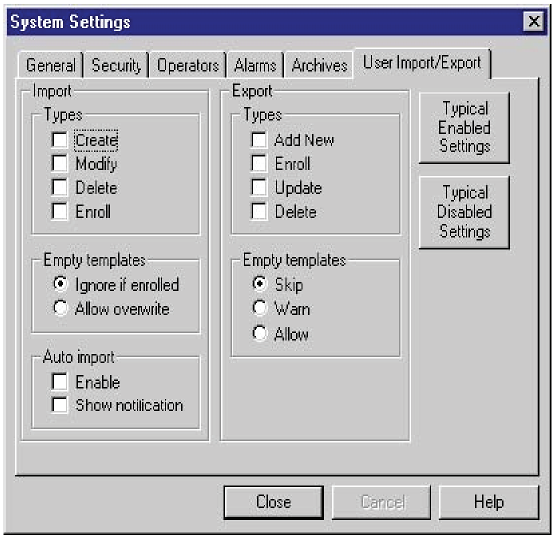
When Users Get Imported and Exported

User Import/ Export Tab

The *User Import/Export* tab is only available if you have purchased the upgrade to the full feature set of Version 2.0.

This tab controls what user information is imported and exported, and whether imports are automatic or manual. You only need this tab if you have readers connected to several different computers (each with its own copy of HandNet) and if users added to one system to be available on the others. If all of your readers are connected to a single copy of HandNet, you do not need this feature.

To get to this screen, pick *Settings* from the *View* menu, and then click the *User Import/Export* tab.



System Settings

General | Security | Operators | Alarms | Archives | User Import/Export

Import

Types
- □ Create
- □ Modify
- □ Delete
- □ Enroll

Empty templates
- ● Ignore if enrolled
- ○ Allow overwrite

Auto import
- □ Enable
- □ Show notification

Export

Types
- □ Add New
- □ Enroll
- □ Update
- □ Delete

Empty templates
- ● Skip
- ○ Warn
- ○ Allow

Setting Up for Common Situations

If all of your readers are connected to a single copy of HandNet: You do not need this feature. Click the *Typically Disabled Settings* button to make sure that the import and export features are both turned off.

If you have HandNet running on several computers and you want to be able to add, change or delete users from any of those computers: Click the *Typically Enabled Settings* button to turn both the import and export features on.

If you have multiple computers with HandNet but you only want users added, changed, deleted, or enrolled on this computer: Check the *Enroll, Update*, and *Delete* boxes in the *Export* column, and uncheck all of the boxes in the *Import* side of the screen. This causes HandNet to export users but prevents changes from elsewhere from being imported.

If you have multiple computers with HandNet but you only want users added, changed, deleted, or enrolled on another computer: Check the *Create, Modify, Delete* and *Enroll* boxes in the *Import* column, and uncheck all of the boxes in the *Export* side of the screen (you can also enable *Auto Import* if you wish). This keeps HandNet from creating an export file that you do not need, and enables it to import changes from another computer.

Import Settings

Types: This controls what user information HandNet will import. Make sure that you select the correct choices here before you try to import. When HandNet imports, it empties the *Import* file, discarding those user records that do not meet the conditions you have checked here.

Create: If this box is checked and HandNet finds a new user in the *Import* file, HandNet adds that user to your database. If this box is not checked, HandNet will not import any new users.

Modify: If this box is checked and HandNet finds a user in the *Import* file with the same ID number as a user that you already have, HandNet replaces the information for the user you have with the user in the *Import* file. If this box is not checked and HandNet finds a user in the *Import* file with the same ID number as a user that you already have, HandNet will not change the user that you have. If you do not have this checked, you could end up with different information for a user on different computers.

Delete: If this box is checked and HandNet finds a user marked for deletion in the *Import* file, HandNet deletes that user from your computer as well. If you do not have this checked, you could end up users that are still on your computer that are not in the copies of HandNet running on the other computers.

Enroll: If this box is checked and HandNet finds a newly enrolled user in the *Import* file, HandNet imports the user and the template (image of the user's hand). If you do not check this, you will have to enroll new users on each computer where they are imported.

Empty Templates: If HandNet finds a user that is not enrolled in the *Import* file, and it finds a user with the same ID number that is enrolled, this entry controls what HandNet will do. *Ignore if enrolled* keeps the enrolled Version of the user that you already have rather than replacing the user with the unenrolled user. *Allow overwrite* replaces the enrolled user with the unenrolled one; this means that the user will have to be enrolled again (to avoid this, on the computer that is exporting the users, do not check *Add New* on the *Export* side and make sure *Empty Templates* on the *Export* side is set to *Skip*. This way, users will not be exported until they are enrolled).

Auto Import:

Enable: If you check the *Enable* box, HandNet automatically import users whenever it finds an *import.mdb* file in the HandNet directory. If this box is not checked, then HandNet only import users when you pick *Import Users* from the *File* menu; see page 99.

Show Notification: If you check this box and the *Enable* box above is also checked, then when HandNet automatically imports users, it shows a message on the screen that lets you know that users are being imported. If you do not check this box, then HandNet just imports the users without popping a message up (either way, HandNet also records the activity in the *Activity* window). If the *Enable* box is not checked above, this entry does not apply.

Export Settings

Types: This controls what user information HandNet exports.

Add New: If this box is checked and you add a user, HandNet exports the user. Normally you do not want this box checked; you usually want HandNet to wait until the user is enrolled before exporting the user. If you have this checked, HandNet exports the unenrolled user.

Enroll: If this box is checked, then HandNet exports a new user after the user is enrolled.

Update: If this box is checked and change information for a user, HandNet exports the changed information. This can help keep user information the same on all of the computers.

Delete: If this box is checked and you delete a user, HandNet exports the fact that the user was deleted. If the other copies of HandNet are set up to import deletions, then the user will be removed from those computers as well.

Empty Templates: If you add or change a user that has not been enrolled yet, this controls whether or not HandNet will export it. Normally you only want HandNet to export users after they are enrolled, so you would leave this set to *Skip*.

“Typical” Settings

These buttons automatically check the appropriate options for two situations:

Typically Enabled Settings: This checks the appropriate boxes for a computer to be able to automatically import and export users.

Typically Disabled Settings: This unchecks all of the boxes; this is appropriate for any user who is not running HandNet on more than one computer.

See *Setting Up for Common Situations* on page 28 for more on common setups.

Getting Exported Users to Another Computer

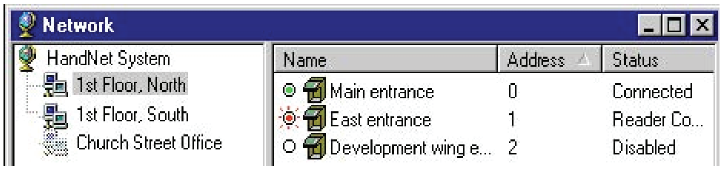
See *Importing Users from Another Copy of HandNet* on page 99 for more on how to get the exported user information to the other computer so you can import them there.

* * * * *

Setting Up Sites and Readers

Seeing Sites and Readers in the Network Window

The *Network* window lists every site and reader that you have added in HandNet. To open this window, pick *Network* from the *View* menu or press *CTRL-N*.



Name	Address	Status
🟢 Main entrance	0	Connected
🔴 East entrance	1	Reader Co...
○ Development wing e...	2	Disabled

The left pane lists all of your sites (that is groups of connected readers). The right pane lists all of the readers in the currently selected site (to list all readers for all sites, click *HandNet System* at the top of the left pane).

Understanding the Icons to the Left of the Name

You see one of these icons to the left of each reader's name:

🟢	The green light indicates that this reader is currently connected and communicating with HandNet.
◉	The black dot indicates that HandNet communicates with this reader by modem, and HandNet is not currently connected with the reader (when HandNet connects with the readers in that site depends on what you have on the *Schedule* tab in *Site Properties*).
○	The empty circle indicates that you have not enabled this reader. This is the case when you are setting a new reader up (you enable a reader on the *General* tab in *Reader Properties*. You must also enable the site on the *General* tab in the *Site Properties*).
🔴	The red light indicates that there is a communication problem between HandNet and the reader. The reader may not be configured correctly, or there may be a problem with the way the reader is connected.

Changing How the Readers are Sorted

You can sort the list of readers using the information in any column by clicking on the column heading. For example, to sort the list alphabetically by name, click on the name heading. If you click on the same heading again, it will sort the list in reverse order; for example, using the name, it would sort from Z to A. You can also sort by address (this might be useful if you wanted to find the next available number for a new reader), by status (this could be useful to group all of the readers that are not enabled or that are having communication problems), or by site if you clicked *HandNet System* at the top of the site list to list all readers from all sites at once.

Rearranging or Resizing the Columns

To move any column, click the column heading and hold the mouse down. With the mouse held down, drag the column heading to the left or right (see the *User's window* in the online help for an example of this).

You can also change the width of a column by pointing to the edge of the column heading, holding the mouse down, and then dragging the edge of the column to the desired position. This lets you fit more columns in the window.

F5 restores all columns to the width they had when you started HandNet. If you want HandNet to save the new column widths, exit the HandNet program and come back in. HandNet then uses your changed column widths as the new standard or default.

* * * * *

Setting Up Sites, Overview

What a Site Is

In HandNet, a site refers to a group of up to thirty-two connected readers. Put another way, one reader is physically connected to the computer (by network, serial cable, or modem), and up to thirty-one additional readers can be daisy chained to that first reader; that is, a cable runs from the first reader to the second, another cable runs from the second to the third, and so on. We call this chain of readers a site. A site does not have any connection to a particular building or location; these readers could be in one building or in more than one building (if the buildings are close enough to run a cable from one to the other), and one building could have one or many sites.

You control access to each reader separately, so having readers with unrelated purposes in one site is fine; the site designation merely indicates that the readers are physically connected to each other.

There are two parts to setting up a site and readers: you must physically set the readers up and connect them to each other and to the computer, and you must add the site and readers in HandNet. This help only explains adding the site in HandNet. For help setting up and connecting the readers, see the manual that came with the readers.

Before You Enable a Site

If you have been using readers without HandNet and you want to get the users from the reader(s), follow these steps BEFORE enabling the site and reader:

1. Pick *Settings* from the *View* menu.
2. Click the *Security* tab.
3. Check the box by *Do not delete unauthorized enrollments* (see page 23 for more about what this option does; after you have gotten your users from the reader, you may want to check this box again).

If you enable both the site and the reader without changing this setting, HandNet regards all of the users in the reader as unauthorized (because they are not in HandNet yet) and deletes them from the reader. Once it deletes them, there is no way to get them back without adding and enrolling the users again.

* * * * *

Adding or Changing a Site

QUICK STEPS

Adding a Site in HandNet

1. Click *Site* on the main menu bar at the top of the screen, and then pick *Add Site*. This starts the *New Site Wizard*.
2. Complete each screen and then click the *Next* button at the bottom of the screen. The screens that you see in this process vary depending on whether the site is connected to the computer by a serial cable, through a network, or by a modem.
3. On the final screen, indicate whether to enable site
   If the site is physically set up and connected: Enable the site now. Check the *Enable Site* box and then click *Finish*.
   If the site is not physically set up yet: Enable the site later. To do this, you will open the *Network* window, double-click the site in the left pane of the window to open up the site properties, check the *Enabled* box, and then click *OK*.

Adding a Site

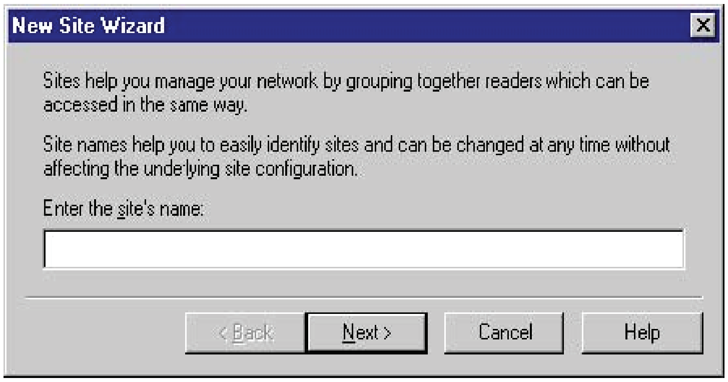
Click *Site* on the main menu bar at the top of the screen, and then pick *Add Site*. This starts the *New Site Wizard*.

Changing a Site

Click a site in the left pane of the *Network* window, pick *Properties* from the *Site* menu, and then click the tab with the information you need to change.

Name

This is the first screen in the process of adding a new site. Enter a name that identifies the site, and then click the *Next* button.



New Site Wizard

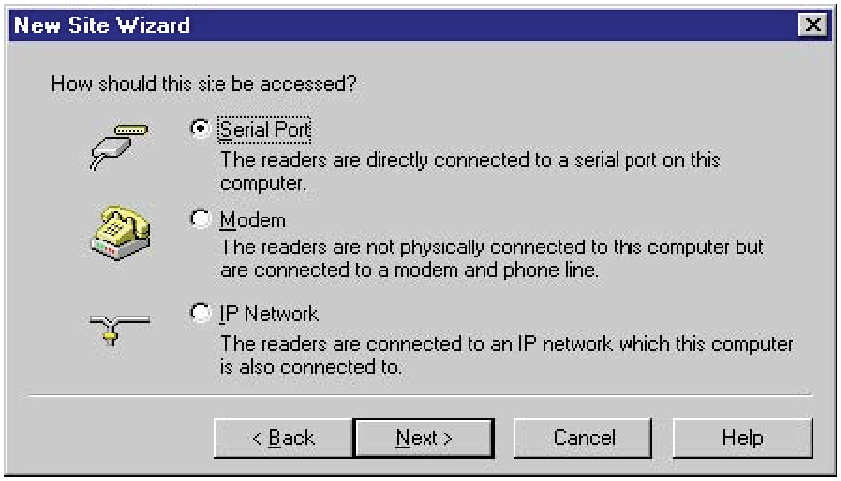
Sites help you manage your network by grouping together readers which can be accessed in the same way.

Site names help you to easily identify sites and can be changed at any time without affecting the underlying site configuration.

Enter the site's name:

Type of Connection

When adding a new site, this screen lets you indicate how HandNet will communicate with the site.



New Site Wizard

How should this site be accessed?

● Serial Port
The readers are directly connected to a serial port on this computer.

○ Modem
The readers are not physically connected to this computer but are connected to a modem and phone line.

○ IP Network
The readers are connected to an IP network which this computer is also connected to.

Serial Port: To connect to a site by running a cable from your computer to the reader, you must have a free serial port on your computer. See the HandKey manual for more on the requirements for the cable. This first reader must have an address of zero (and no other reader in the site can have an address of zero).

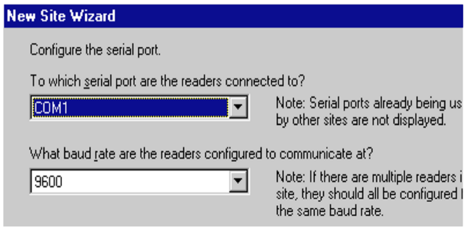
Modem: To connect to a site by modem, the first reader in the site must have a modem installed in it (contact your dealer for more information). This first reader must have an address of zero (and no other reader in the site can have an address of zero).

IP Network: To connect to a site through your network, you must have a TCP/IP network with static IP addresses. Your computer must have a network card and be connected to the network. If the network is faster than 10baseT, you must have a switching hub. The first reader in the site must have an ethernet card (contact your dealer for more information). This first reader will automatically have an address of zero (no other reader in the site can have an address of zero), and you must enter a unique IP address in the reader; see *Configuring the Physical Reader* on page 54 for more detail on this.

Serial Port Connection

To connect to a site by running a cable from your computer to the reader, you must have a free serial port on your computer; see the HandKey manual for more on the requirements for the cable. This first reader must have an address of zero (and no other reader in the site can have an address of zero).

when adding a new site



New Site Wizard

Configure the serial port.

To which serial port are the readers connected to?

COM1

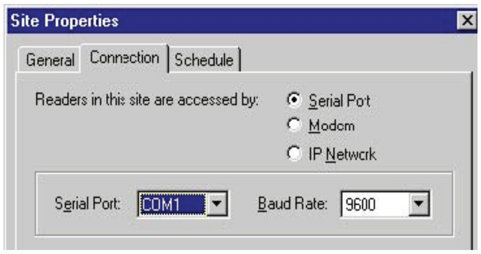
Note: Serial ports already being us
by other sites are not displayed.

What baud rate are the readers configured to communicate at?

9600

Note: If there are multiple readers i
site, they should all be configured t
the same baud rate.

when changing a site



Site Properties

Readers in this site are accessed by: ● Serial Pot ○ Modem ○ IP Network

Serial Port: COM1 Baud Rate: 9600

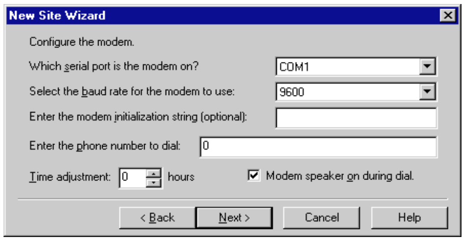
Serial Port: Click this and pick the serial port that the cable from the reader is connected to. If you pick the wrong port here, HandNet will not be able to communicate with the reader. If you have several sites, each must be connected to a different serial port. HandNet only lists ports set up on your computer that are not already used for communicating with another site. If you click this and get a blank list, all of the serial ports are already used. Contact the person who services your computer hardware if you need to add additional serial ports.

Baud Rate: Click this and pick the baud rate, we recommend 9600. While 19200 should theoretically be faster, because of the way the reader sends information, this does not result in any real gain. The speed here must match the speed set in the reader; see *Configuring the Physical Reader* on page 54 for more detail on how to change the baud rate in the reader.

Modem Connection

To connect to a site by modem, the first reader in the site must have a modem installed in it (contact your dealer for more information). This first reader must have an address of zero (and no other reader in the site can have an address of zero).

when adding a new site



New Site Wizard

Configure the modem.

Which serial port is the modem on? COM1

Select the baud rate for the modem to use: 9600

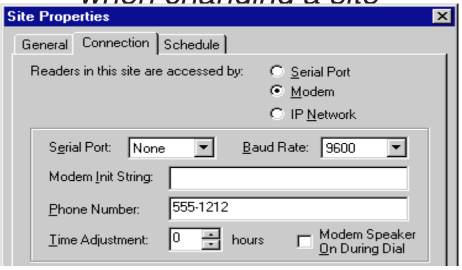
Enter the modem initialization string (optional):

Enter the phone number to dial: 0

Time adjustment: 0 hours

☑ Modem speaker on during dial.

when changing a site



Site Properties

Readers in this site are accessed by: ○ Serial Port ● Modem ○ IP Network

Serial Port: None

Baud Rate: 9600

Modem Init String:

Phone Number: 555-1212

Time Adjustment: 0 hours

□ Modem Speaker On During Dial

Serial Port: If you have an external modem, click this and pick the serial port your modem is connected to; this is usually (but not always) *COM1* or *COM2*. If you have an internal modem, it is usually connected to *COM3* or *COM4*. HandNet only lists ports that are set up on your computer and that are not already used for communicating with another site.

Baud Rate: Choose 9600 if you are connecting to a HandKey II or HandKey CR; choose 2400 if connecting to a HandKey.

Modem Init String: If you need HandNet to send any commands to the modem before dialing, enter the appropriate codes here. The modem must be set up for no data compression, no error correction, an appropriate baud rate, and auto answer. The manual that came with your modem explains the various commands that work with your modem. An inappropriate init string can prevent the modem from connecting. Try connecting without any init string to see if you can communicate; you modem may be automatically set up correctly. If you have problems getting your modem to connect and communicate with the site, here are init strings that have worked for some modems:

Typical Modem Strings		AT&F&C1&D2X1V1E0 AT&C1&D2X1V1E0 AT&C1X1VE0
Rockwell Chip Set Modems		AT&D2E0&Q0N0S37=5
US Robotics Sportster 14.4 F/M		AT&F0 AT&FX0&C1&D2&H0&N6&K0S0=0
Everex 2400E		AT&F
Hayes Accura 14,400	1200 Baud	AT&F&C1&D2&K0S0=0S37=5
	2400 Baud	AT&F&C1&D2&K0S0=0S37=6
Hayes Optima 14,400	1200 Baud	AT&F&C1&D2&K0S0=0S37=5
	2400 Baud	AT&F&C1&D2&K0S0=0S37=6
Practical Peripherals PM144MTII	1200 Baud	AT&F&C1&D2&K0S0=0S37=5
	2400 Baud	AT&F&C1&D2&K0S0=0S37=6
Practical Peripherals 14.4 FXSA	1200 Baud	AT&D2E0&Q0N0S37=5
	2400 Baud	AT&D2E0&Q0N0S37=6

Cardinal 33.6 V.34/V.FC	1200 Baud	ATE0S37=5&C1&D2&K0
	2400 Baud	ATE0S37=6&C1&D2&K0
Multitech Model MT1932ZPX		AT&F&C1&D2X1V1E0&E0&E3&E7&E8 &E10&E12&E14$MB1200$SB1200
Zoom Model cc4336	2400 Baud	AT&Q0&K0+MS=2

Phone Number: If you have to dial some digit to get an outside line, enter this digit followed by a comma before the phone number. If the number is a long distance number, enter the one and the area code as appropriate. For example, if you had to dial a nine for an outside line, and the number was long distance and required one and an area code, you would enter the number like this:

9, 1-802-555-1212

You do not have to enter the dashes; they do not make a difference. You could equally well enter the number above like this:

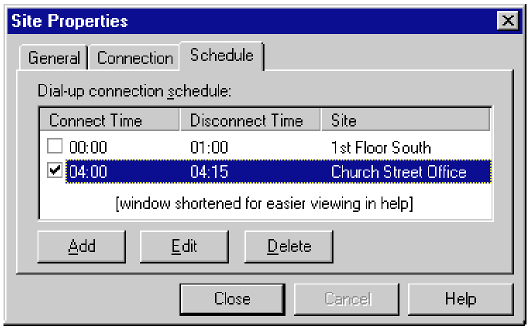
9,18025551212

Time Adjustment: If this site is in a different time zone, enter the number of hours the time difference is. For example, if you are in New York and were setting up a connection with a site in California, you would enter *-3* since in California it is three hours earlier than in New York. If you are in California and setting up a connection with a site in New York, you would enter *3* since it is three hours later in New York. Only do this if you want all times reflecting the time zone you are currently in.

Modem Speaker On During Dial: If you check this box, when HandNet connects to this site, it turns the modem speaker on so you can hear it dialing and connecting. If there is a problem connecting, turning the modem speaker on can help identify where the problem is. Unless you are having a problem connecting, we do not recommend checking this box.

Scheduling a Connection Time

If you are connecting to sites by modem, this screen shows when HandNet is scheduled to connect with each site. You can only change the connection time for the current site (this screen does not apply if you are not communicating by modem; if you connect by serial port or through a network, HandNet stays connected to the site continuously and does not need a scheduled connection time).



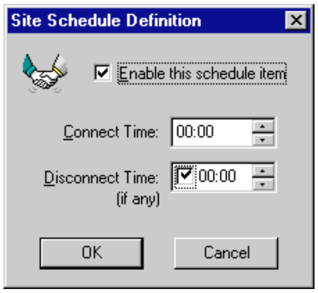
Dial-up connection schedule:

Connect Time	Disconnect Time	Site
☐ 00:00	01:00	1st Floor South
☑ 04:00	04:15	Church Street Office

[window shortened for easier viewing in help]

Adding a New Scheduled Connection Time

When you choose to add a new schedule time, you see this screen:



☑ Enable this schedule item

Connect Time: 00:00

Disconnect Time: (if any) ☑ 00:00

Enable this schedule item: This box must be checked for HandNet to make the connection. Only uncheck this box if the modem is not set up yet at the site and you do not want HandNet to try to communicate with the site.

Connect Time: Enter the time that you want HandNet to try to connect. This must be at least one minute later than the disconnect time for the previous connection. For example, if another connection is scheduled to end at 5:00, the new connection can be scheduled for 5:01, but not for 5:00. If the phone lines are busy when HandNet tries to connect, it will keep trying until it makes a connection (or reaches the *Disconnect Time*).

Disconnect Time: If you uncheck this box, HandNet will stay connected to this site continuously. Since the modem will be continuously connected to that site, you will not be able to schedule a connection to any other site; if you need more than one connection, this must be checked. When you enter a disconnect time, it must be after the start time. For example, you cannot schedule a connection to both begin and end at 5:00; if the connection begins at 5:00, the disconnect time must be 5:01 or later.

When you enter the disconnect time, allow enough time for HandNet to download all of the potential activity in the reader. The reader can send about 100 events a minute. This means that if the reader were full (with 5000 events), it could take up to an hour to get all of the activity. The amount of activity you have each day and the number of times you connect to reader during the day determine how long your connection must be.

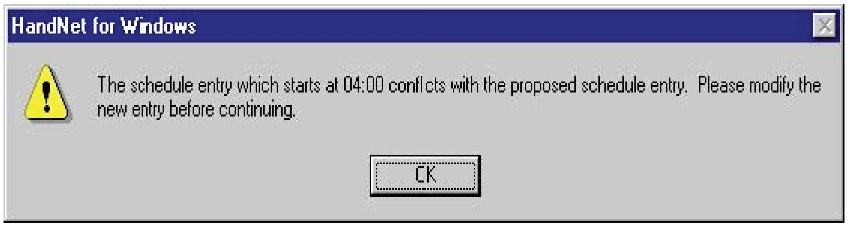
When HandNet reaches the disconnect time, it disconnects even if there is still activity that the reader needs to send. When HandNet disconnects, if the reader is not done sending activity, a few activities would be lost. If there is regularly more activity at the reader than the connection time allows for, the reader's memory would eventually fill up, at which point additional activity would also cause activity to be lost. To avoid this, make sure the time between the *Connect Time* and the *Disconnect Time* is long enough to get all of the activity.

Changing or Deleting a Scheduled Communication Time

Even though HandNet lets you see the scheduled connection times for all sites, HandNet only lets you change a scheduled time for the site with which you are currently working. To change a scheduled time for a different site, you must go to the properties for that site, select the scheduled time there, and then click the *Edit* button.

If You Get a Message that the Time Conflicts

If the time that you enter conflicts with the time that HandNet is already scheduled to communicate with a different site, you see a message like this:



The schedule entry which starts at 04:00 conflcts with the proposed schedule entry. Please modify the new entry before continuing.

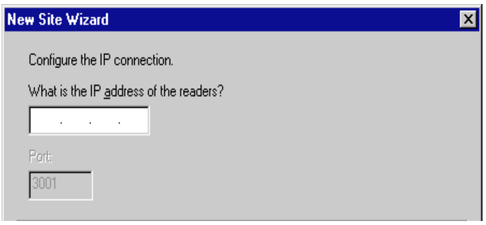
Make sure that each other scheduled connection has a disconnect time. If you schedule a connection with no end time, HandNet would never disconnect from that site, so it would not be possible to schedule another connection. If you want to have more than one scheduled connection, each connection must have a disconnect time.

Also make sure the connect time is at least one minute later than the disconnect time for the previous connection. For example, if another connection is scheduled to end at 5:00, the new connection can be scheduled for 5:01, but not for 5:00.

IP Address

You see this screen if you indicate that HandNet will communicate with this site through a network.

when adding a new site

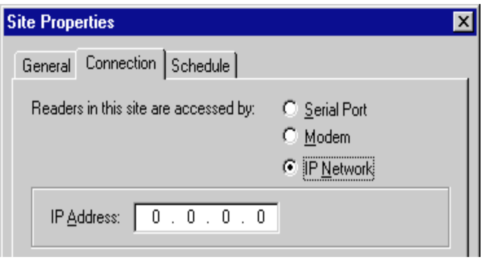


Configure the IP connection.

What is the IP address of the readers? . . .

Port: 3001

when changing a site



Readers in this site are accessed by: ○ Serial Port ○ Modem ● IP Network

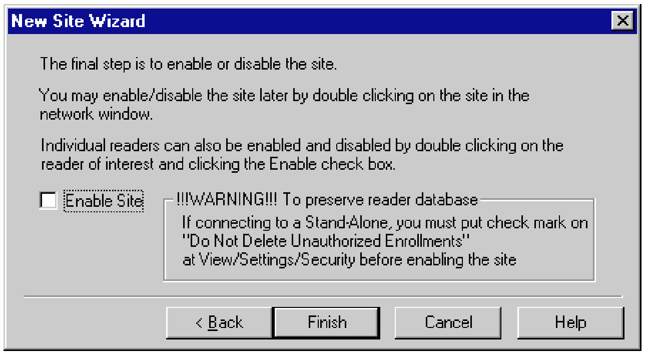
IP Address: 0 . 0 . 0 . 0

IP address: Each site must have a unique IP address. Ask your network administrator for an appropriate address. The address you enter here must match the address you enter in the reader; see *Configuring the Physical Reader* on page 54 for more on how to change the address in the reader.

Port: This entry no longer applies; it is always grayed out.

Enabling the Site

This is the final screen that you see in the *New Site Wizard* (when you go back to *Site Properties* to change this site, this is on the *General* tab).



New Site Wizard

The final step is to enable or disable the site.

You may enable/disable the site later by double clicking on the site in the network window.

Individual readers can also be enabled and disabled by double clicking on the reader of interest and clicking the Enable check box.

□ Enable Site

!!!WARNING!!! To preserve reader database

If connecting to a Stand-Alone, you must put check mark on "Do Not Delete Unauthorized Enrollments" at View/Settings/Security before enabling the site

Enable Site: You must enable the site before HandNet can communicate with the readers in it, but you might not want to enable it yet. Please read the sections below if you are not sure.

If the site is not physically set up yet

If the site is not physically set up yet, do not enable it; you do not want HandNet to repeatedly try to communicate with something that is not there. This would slow the system down.

If you have been using readers independently of HandNet and you need to get users from the readers

If you have been using readers independently of HandNet and if you want to get the users from the readers into HandNet, **you also do NOT want to enable the site until you have set HandNet to accept users from the reader that are not in HandNet.** To do this:

1. Click *Finish* without checking the *Enable Site* box.
2. Pick *Settings* from the *View* menu.
3. Click the *Security* tab.
4. Check the box by *Do not delete unauthorized enrollments* (see page 23 for more about what this option does; after you have gotten users from the reader, you may want to check this box again).

If you enable both the site and the reader without changing this setting, HandNet will regard all of the users in the reader as unauthorized (because they are not in HandNet yet) and it will delete them from the reader. Once it deletes them, there is no way to get them back without adding and enrolling the users again.

If you are ready to connect

If the site is physically set up and you do not need to get users from the readers (or if you have already changed the setting above), then you can enable the site now. Check the *Enable Site* box and then click *Finish*.

To Enable the Site Later

After you leave this screen, you can enable the site by doing this:

1. Open the *Network* window.
2. Double-click the site in the left pane of the window to open up the site properties (or click once and pick *Properties* from the *Site* menu).
3. Check the *Enabled* box and then click *OK*.

* * * * *

Setting Up Readers, Overview

There are two parts to setting up readers: 1) physically setting the readers up and connecting them to each other and to the computer; and 2) adding the site and readers in HandNet. This manual only explains adding the site and readers in HandNet. For help setting up and wiring readers, see the manual that came with the readers.

Before You Enable the Reader

Before you add readers, you must set up the site they are connected to; see page 34.

If you have been using readers without HandNet and you want to get users from the reader(s), follow these steps BEFORE enabling the site and reader:

1. Pick *Settings* from the *View* menu.
2. Click the *Security* tab.
3. Check the box by *Do not delete unauthorized enrollments* (see page 23 for more about what this option does; after you have gotten your users from the reader, you may want to check this box again).

If you enable the site and the reader without changing this setting, HandNet regards all users in the reader as unauthorized (because they are not in HandNet yet) and deletes them. Once it deletes them, there is no way to get them back without adding and enrolling the users again.

Selecting Readers

Most options on the *Reader* menu are disabled until you select a reader.

To select a single reader: Click that reader in the list.

To select multiple readers that are together on the list: Click the first reader in the group, hold the *SHIFT* key down, and click the last reader that you want to select.

To select multiple readers that are not together on the list: Click the first reader to select, hold the *CTRL* key down, and click each other reader that you want to select.

Renaming a Reader

You might rename a reader if you discovered that the original name was not clear or if you changed the purpose of the areas the reader gave access to. Renaming the reader does not change any of its properties and does not require you to set anything up again; it only changes the name that appears in the lists on the screen and in reports that you generate.

To rename a reader:

1. If the *Network* window is not open, pick *Network* from the *View* menu (or press *CTRL-N*).
2. Click the reader in the right pane of the *Network* window.
3. Pick *Rename* from the *Reader* menu (you could also right click and pick *Rename*, or you could double-click the reader and change the name in the *Reader Properties*).

* * * * *

Setting Up a New Reader

QUICK STEPS

Adding a New Reader

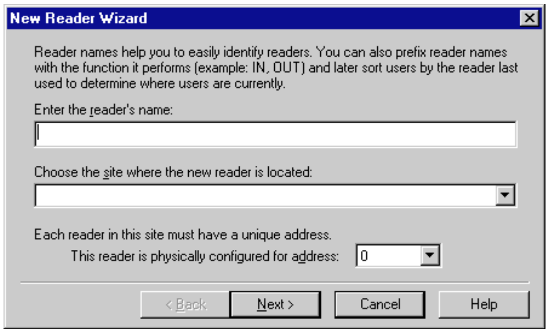
1. Click *Reader* in the main menu bar at the top of the screen, and then pick *Add New*. This starts the *New Reader Wizard*.
2. On the second screen of the *New Reader Wizard*, indicate whether you want to set the reader up by going through each configuration screen, or whether you want to copy the settings from another reader. Copy the settings from another if the settings are identical or even similar to the other reader (if you copy settings, you can use *Properties* on the *Reader* menu to make changes).
3. If you are setting up the reader by going through each configuration screen, see the different tabs in the *Reader Properties* for help with particular entries. Click the *Next* button at the bottom of the screen to continue with the next screen.
4. Make sure that the address in the reader matches the address you entered on the first reader properties screen; see *Configuring the Reader* for more details.
5. Once the reader is physically connected and set up correctly, enable the reader. To do this, open the *Network* window, double-click the site in the right pane of the window to open the *Reader Properties*, check the *Enabled* box, and then click *OK*.

Getting Started

When you pick *Add New...* from the Reader menu, HandNet starts the *New Reader Wizard*. This takes you through the process of adding the reader.

Name and Address Screen

This is the first screen that you see when adding a new reader:



Reader names help you to easily identify readers. You can also prefix reader names with the function it performs (example: IN, OUT) and later sort users by the reader last used to determine where users are currently.

Enter the reader's name:

Choose the site where the new reader is located:

Each reader in this site must have a unique address.

This reader is physically configured for address: 0

Enter the reader’s name: Enter any name that clearly describes the reader’s function and location. This name is used in the *Activity* window and in activity reports to identify where activity took place.

Choose the site where the new reader is located: Click this to pick the site (group of readers) that this reader is connected to. You must set the site up before you can add the reader.

This reader is physically configured for address: HandNet automatically fills in the first available address that has not been used yet in this site. For example, if you already have readers 0, 1, and 2 in this site, HandNet automatically fills in an address of 3. You can change this if you wish. The first reader in each site my be reader 0; other readers in the site can use any number up to 254. Readers do not need to be numbered sequentially. For example, your readers could be numbered 0, 1, 2, 3... or they could be numbered 0, 100, 110, 137... Within a site, each reader must have a

unique number. For example, you cannot have two readers in the same site that both use the address of 1. However, you can reuse numbers in different sites. For example, if you have twenty sites, you could have a reader with an address of 1 in each of them.

Make sure the address matches the address in the reader

The number here must match the address entered in the reader; see *Configuring the Physical Reader* on page 54 for more on how to set the address up in the reader.

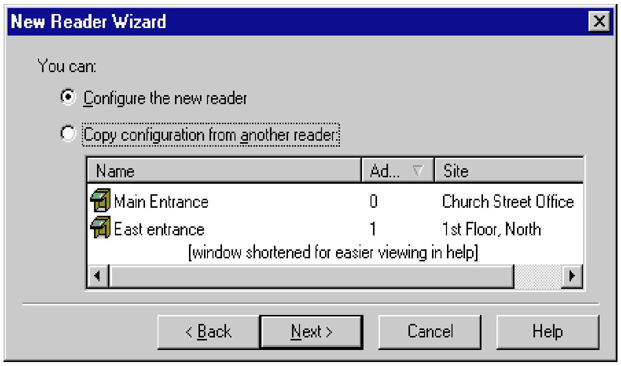
Never put more than 32 readers in a site

Even though HandNet allows numbers from 0 to 254, you should never have more than thirty-two readers in a site. While it is sometimes technically possible to connect more than thirty-two readers, not all readers support this, and even for readers that do, connecting more than this causes unacceptably slow response times from readers. The software was not designed to handle more than this, and we cannot guarantee results with more than thirty-two readers. If you feel that more than thirty-two readers in a single site is essential for you, please contact us to discuss your situation first; in nearly all cases, the preferable (and sometimes only) solution is to set up additional site(s).

Click *Next* to go on to the next screen. This button is disabled until you have filled in all of the entries on this screen.

Configuration

This is the second screen that you see in the process of adding a new reader. This screen lets you choose whether you want to set the reader up by going through each configuration screen in the reader properties, or whether you want to copy the settings from another reader. Copy the settings from another reader if the settings are identical or even similar to the other reader. If you copy the settings from another reader, and you want to make the settings slightly different, you can use *Properties* on the *Reader* menu to make changes; see page 45.



New Reader Wizard

You can:

● Configure the new reader

○ Copy configuration from another reader:

Name	Ad...	Site
Main Entrance	0	Church Street Office
East entrance	1	1st Floor, North

[window shortened for easier viewing in help]

Configure the new reader: This lets you go through each of the *Reader Properties* screens so you can choose the appropriate settings on each. The *Reader Properties* screens are explained starting on page 45. You would choose this for the first reader you add. You would also choose this if you wanted very different settings from the other readers. For example, if other readers are set to trigger an auxiliary alarm after certain events and you do not want this reader to trigger an alarm, or if other readers have an automatic unlock time and you do not want that for this reader, then you might want to use this option.

Copy the configuration from another reader: If another reader has the same or nearly the same settings as you want for this reader, copying settings from the other reader is faster. It also protects you from accidentally

making the settings slightly different if you want readers configured exactly the same way.

If you choose this option, click the reader in the list to copy the settings from and then click the *Finish* button (the *Next* button changes to a *Finish* button when you choose this option).

When you copy the configuration from another reader, HandNet does NOT enable the reader. You must go to the *General* tab in the *Reader Properties* to enable the reader before HandNet will communicate with it; see page 45.

If you copy the settings from another reader, and you want to make the settings slightly different, you can use *Properties* on the *Reader* menu to make changes; see page 45.

* * * * *

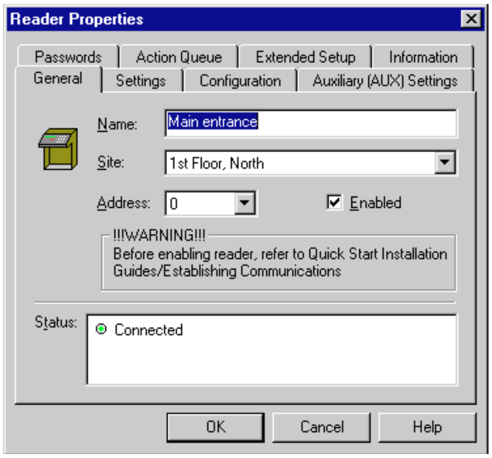
Changing Reader Settings with Reader Properties

Getting to the Reader Settings

Click a reader in the right pane of the *Network* window, and pick *Properties* from the *Reader* menu (or just double-click the reader in the *Network* window). You are initially on the *General* tab; click any other tab to jump to the corresponding screen.

General

This screen contains the reader's name and address, the site the reader is a part of, and whether or not the reader is currently enabled and connected.



Name: Main entrance

Site: 1st Floor, North

Address: 0

☑ Enabled

!!!WARNING!!!
Before enabling reader, refer to Quick Start Installation Guides/Establishing Communications

Status: ● Connected

Name: The name is to help you identify the reader. Changing the name does not affect any of the reader's other settings or connection. If you change the name of the reader, the new name is used in activity reports for activity at that reader, even if the activity occurred before the name change.

Site: This is the site (that is, the group of up to thirty-two readers) that this reader is associated with.

Address: The number here can be from 0 to 254. If the site is connected by IP Network, the first reader in the site (the one with the ethernet card) must be reader 0. Other readers can use any number and do not need to be numbered sequentially. For example, your readers could be numbered 0, 1, 2, 3... or they could be numbered 0, 100, 110, 137.... You can use the same reader number in more than one site. For example, if you have twenty sites, you could have a *Reader One* in each of them.

The number here must match the address entered in the reader; see *Configuring the Physical Reader* on page 54 for more on how to set the address up in the reader.

Even though HandNet allows numbers from 0 to 254, you should never have more than thirty-two readers in a site. While it is sometimes technically possible to connect more than thirty-two readers, not all readers support this, and even for readers that do, connecting more than this causes unacceptably slow response times from readers. The software was not designed to handle more than this, and we cannot guarantee results with more than thirty-two readers. If you feel that more than thirty-two readers in a single site is essential for you, please contact us to discuss your situation first; in nearly all cases, the preferable (and sometimes only) solution is to set up additional site(s).

Enabled: This should be checked once reader setup is done and users should have access through the reader. Leave this unchecked if you do not want HandNet to try to communicate with the reader at this point.

If you have been using readers without HandNet and you want to get the users from the reader, follow these steps BEFORE enabling the site and reader:

1. Pick *Settings* from the *View* menu.

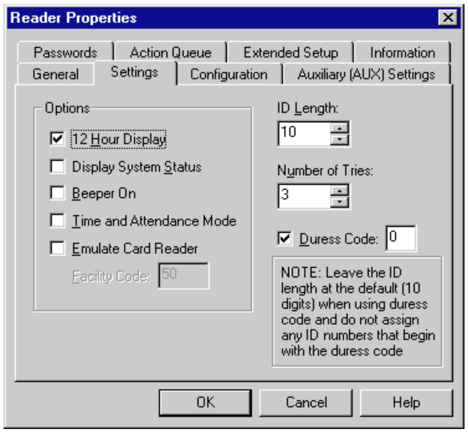
2. Click the *Security* tab.

3. Check the box by *Do not delete unauthorized enrollments* (see page 23 for more about what this option does. After you have gotten your users from the reader, you may want to check this box again).

If you enable both the site and the reader without changing this setting, HandNet will regard all of the users in the reader as unauthorized (because they are not in HandNet yet) and it will delete them from the reader. Once it deletes them, there is no way to get them back without adding and enrolling the users again.

Status: This indicates whether the reader is connected.

Settings



Options

☑ 12 Hour Display
☐ Display System Status
☐ Beeper On
☐ Time and Attendance Mode
☐ Emulate Card Reader

Facility Code: 50

ID Length: 10

Number of Tries: 3

☑ Duress Code: 0

NOTE: Leave the ID length at the default (10 digits) when using duress code and do not assign any ID numbers that begin with the duress code

This screen controls the reader's display and other factors that affect what happens when the user enter an ID number at the reader.

12 Hour Display: If you check this, the reader displays times after noon using the numbers one through twelve; if it is not checked, it uses twenty-four hour time. For example, if this is checked 5:00 PM displays on the reader as 5:00; if this is not checked, 5:00 PM displays as 17:00.

Display System Status: Do not check this option unless asked to by one of our support staff. This displays technical information on the reader display about the status of different aspects of the reader. It is not relevant to normal use of the reader.

Beeper On: If this is checked, the reader beeps each time you press a button on it; if this is not checked, the reader does not beep. In a high security setting, you might want the beeps off to make it harder for a casual observer to figure out how many digits are in the ID number. In other contexts, your choice here depends only on your preference; some people like the beeps since it lets them know that they have not missed the button; others prefer not to hear them.

Time and Attendance Mode: Do not check this option. If you check this, the reader asks users for additional information related to time and attendance tracking (whether one is coming in or out or leaving for a job, the job number you are working on, etc.). However, HandNet is currently NOT able to store or track this information.

Emulate Card Reader: If you want the readers to send output directly to a lock and unlock it, leave this unchecked. If you have an access control panel and want the reader to send information formatted like card output to that control panel, check this box.

Facility Code: This only applies if you are emulating a card reader.

ID Length: If all of your user IDs are the same length, you can enter the number of digits here so that users do not have to press *ENTER* or *YES* after typing the ID at the reader. For example, if all of your IDs are four digits long, then you could enter *4* here. Then, at the reader, once the user had entered four digits, the reader would ask the user to place the hand (assuming the ID was valid). Without this, the user would have to type the four digits and then press the *ENTER* or *YES* button on the reader. However, if you use a duress code (see below), do not enter a number here. This is because the duress code adds a digit; if your IDs are four digits, the user will have to be able to enter five digits if they ever need the duress code. If you are using a duress code, leave this set to ten.

Number of Tries: If a user enters a valid ID number but the users hand does not match the image stored, the reader does not give access. This entry controls how many times the user can try to get access before the reader will block the user's ID and not allow further tries. This prevents someone from making repeated tries to gain access with someone else's ID number. Normally three is a good setting here; it allows for two retries if the user did not place the hand correctly, but limits the number of attempts someone can make.

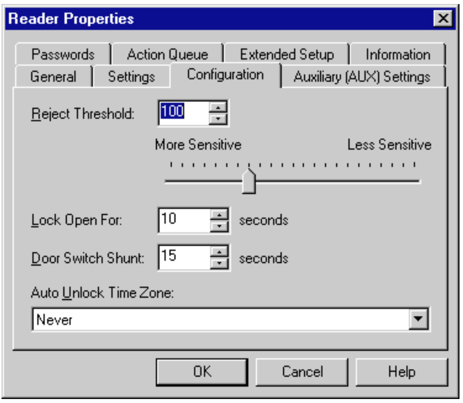
If the user does not gain access after the number of tries here, the reader no longer accepts that user's ID until another user successfully gains access through that reader.

Duress Code: A duress code is single digit that users can enter before the ID number to indicate that they are in danger or that someone else is forcing them to open the door. For example, suppose that you set zero up as a duress code. If a user is being forced to let someone into the building, instead of entering the regular ID of *1234*, the user would enter *01234*. The system would still grant access as it would for the normal ID, but it would also trigger an alarm. This could be merely the alarm in the HandNet program, or, it could also trigger an external alarm through the *Auxiliary Settings*; see page 49.

Zero (0) is often a good digit for the duress code because you cannot begin a user ID with zero if you enroll users from the command menus on the reader (while HandNet distinguishes between *5* and *0005*, the process of adding a user from the reader command menu does not. This means that if you create a user with an ID of *0005* in HandNet and try to enroll that user with the command menus on the reader, when you type *0005*, the reader would think you were enrolling User Five. This would not correspond with *0005* in HandNet).

Configuration

This screen controls how closely the typical user's hand must match the image that is stored, how long the door can stay open, and when (if ever) the door should be automatically unlocked.



Reject Threshold: 100

Lock Open For: 10 seconds

Door Switch Shunt: 15 seconds

Auto Unlock Time Zone:

Never

Reject threshold: The lower this number is, the more closely the user's hand must match the image or template of the hand stored in HandNet. Thirty

(the lowest possible number) requires the hand shape and position to match very closely; two hundred fifty (the highest possible number) will grant access if the hand match is close but not exactly the same. One hundred is good for most contexts; enter a lower number if you have an especially high security situation. You can either enter a number or drag the pointer.

If particular users have trouble placing their hands consistently because of arthritis or some other hand condition, you can override the reader's setting for an individual user on the *Security* tab in the *User Properties*; see page 93.

Lock Open For: This is the number of seconds the door stays unlocked once a user's hand is recognized.

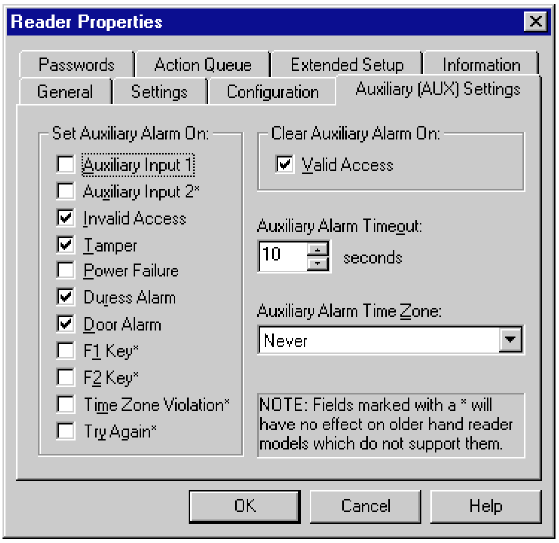
Door Switch Shunt: This is the number of seconds the door can be open before potentially triggering an alarm. The *Alarms* tab in *System Properties* (see page 25) and the *Door Alarm* on the *Auxiliary (AUX) Settings* (see below) and *Extended Settings* (see page 51) tabs control whether this causes an alarm.

Auto Unlock Time Zone: This controls when (if ever) the door is automatically unlocked. For example, you might want a door unlocked during normal business hours, and you might want the door to require hand recognition for access during other hours. You would set up a time zone that reflected the hours you wanted the door open and then pick that time zone here (see page 61 for more on setting up time zones). When you reached the start time, HandNet would unlock the door, and when you reached the end of the time zone, HandNet would lock it again. Leave this set to *Never* if you always want the door locked.

Auxiliary (AUX) Settings

Readers can communicate with auxiliary devices like alarms, lights, or security cameras. HandKey readers can communicate with one auxiliary device; this screen controls when and under what conditions output is sent to that device. HandKey II and HandKey CR readers can communicate with up to three auxiliary devices; this screen controls the output to the first; the *Extended Setup* tab (see page 51) controls output to the second and third.

To get to this screen, click a reader in the right pane of the *Network* window, pick *Properties* from the *Reader* menu, and then click the *Auxiliary (AUX) Settings* tab.



Set Auxiliary Alarm On:
- ☐ Auxiliary Input 1
- ☐ Auxiliary Input 2*
- ☑ Invalid Access
- ☑ Tamper
- ☐ Power Failure
- ☑ Duress Alarm
- ☑ Door Alarm
- ☐ F1 Key*
- ☐ F2 Key*
- ☐ Time Zone Violation*
- ☐ Try Again*

Clear Auxiliary Alarm On:
- ☑ Valid Access

Auxiliary Alarm Timeout: 10 seconds

Auxiliary Alarm Time Zone: Never

NOTE: Fields marked with a * will have no effect on older hand reader models which do not support them.

Set Auxiliary Alarm On: Even though this says *Set Auxiliary Alarm On*, the device does not have to be an alarm; this can trigger any type of auxiliary device. If a condition occurs and the corresponding box is checked, HandNet turns auxiliary output on if it is during the time zone selected at the bottom of the column on the right.

Auxiliary Input 1: This occurs if the reader receives input from an auxiliary input device. This is irrelevant if you do not have an auxiliary input device connected to the reader.

Auxiliary Input 2: This occurs if the reader receives input from the second auxiliary input device (HandKey II and HandKey CR support two auxiliary input devices; HandKey readers support just one). This is irrelevant if you do not have a second auxiliary input device connected to the reader.

Invalid Access: This occurs if someone repeatedly entered a valid ID at a reader, and each time the reader does NOT recognize the user's hand (at the reader, the user would see the message *ID Refused*, and the *Activity* window would show the message *Access Denied*). The number of times that a user can try before this occurs depends on the *Number of Tries* entry on the *Settings* tab in the *Reader Properties*; see page 47. If this occurs, someone might be trying to gain access with someone else's ID.

Tamper: This occurs if someone has shaken the reader roughly or opened the reader. Unless someone was servicing the reader, this message generally warrants further investigation.

Power Failure: This occurs if the reader loses power from an external source. While this could just be due to an ordinary power failure, sometimes someone trying to gain invalid access will cut power in an attempt to disable alarm systems.

Duress Alarm: This occurs if a user entered the duress code. This code indicates that the user is in trouble or that someone is forcing the user to give him/her access; see page 47 for more on setting up a duress code.

Door Alarm: This occurs if the door connected to the reader is forced open, or if the door is kept open for longer than allowed based on the *Door Switch Shunt Time* on the *Configuration* tab in the *Reader Properties*; see page 48.

F1 / F2 Key: This occurs if the corresponding key was pressed on the reader keypad (HandKey II and HandKey CR have F1 and F2 keys to the right of the number keys. The HandKey reader does not have these buttons, what you check here does not make any difference for that type of reader).

Time Zone Violation: This occurs if a user enters a valid ID at a reader, but the user is not authorized to have access during the hours or days of the week based on the time zone associated with the reader in the access profile.

Try Again: This occurs if a user enters a valid ID at a reader, but the reader does not recognize the user's hand (this situation causes the *Identity Unknown* message in the *Activity* window). This could be just the result of incorrect hand placement (if this happens repeatedly, HandNet generates the *Invalid Access* condition above.)

Clear Auxiliary Alarm On: If the auxiliary device is turned on, this controls whether it will be shut off when someone gains valid access (that is, enters a valid ID number and has his/her hand recognized). If this is checked, the alarm (or other auxiliary output) is turned off when a valid user gains access through that reader; if this is not checked, the output continues until the time entered in the following entry ends or until you go to the *Reader* menu, highlight *Auxiliary Output*, and pick *Off*; see page 129.

Auxiliary Alarm Timeout: This indicates the number of seconds that the auxiliary device should be on for.

Auxiliary Alarm Time Zone: This controls when HandNet should turn output to an auxiliary device on. For example, if the auxiliary device is a set of floodlights, it would only help to turn the lights on if the condition occurred at night. To do this, you would create a time zone for night hours, and then assign that time zone here (see page 61 for more on setting up time zones). If this says *Always*, HandNet turns output on for the auxiliary device whenever the checked condition(s) occur.

Passwords

This screen controls the passwords needed to access the menus available through entered command mode on the reader. Generally the passwords below are adequate since a user must be set up with the appropriate authority level on the *Security* tab in *User Properties* (see page 92), and the user must know how to get to these menus in the reader before the passwords below would do any good.

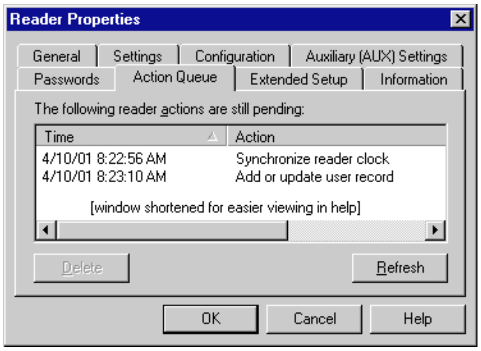
What is available on the different reader menus

1. **Service:** This lets you recalibrate the reader and change the reader's status display.
2. **Setup:** This lets you control reader setup issues including how the reader is connected to your computer network, what language the reader displays in, the date/time, etc.
3. **Management:** This lets you list users.
4. **Enrollment:** This lets you add or remove users.
5. **Security:** This lets you control the passwords for the reader menus, change time zones, enroll users who do not need hand access, etc.

For more detail, see the reader manual.

Action Queue

If the reader is not connected to HandNet continuously (typically only the case if HandNet communicates with the reader by modem), this screen lists changes that have not been sent to the reader yet. These actions will be sent to the reader the next time the modem connects.



The following reader actions are still pending:

Time	Action
4/10/01 8:22:56 AM	Synchronize reader clock
4/10/01 8:23:10 AM	Add or update user record

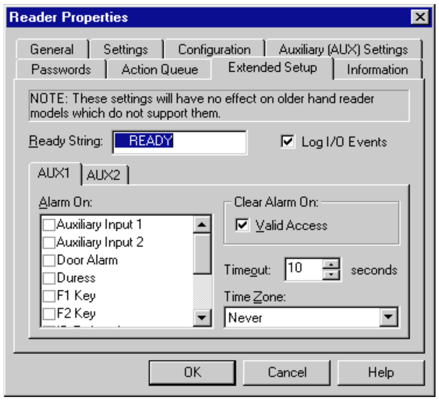
[window shortened for easier viewing in help]

To get to this screen, click a reader in the right pane of the *Network* window, pick *Properties* from the *Reader* menu, and click the *Action Queue* tab.

If there is been a change that requires that certain actions NOT be sent to the reader, you can select those actions in the list and click *Delete*.

Extended Setup

Readers can turn auxiliary devices like alarms, lights, or security cameras on or off. HandKey II and HandKey CR readers can communicate with up to three auxiliary devices; this screen controls the output to the second and third auxiliary devices; the *Auxiliary (AUX) Settings* tab controls output to the first; see page 48. If you have a HandKey (instead of a HandKey II or HandKey CR), this screen does not apply since the HandKey only supports one auxiliary device.



NOTE: These settings will have no effect on older hand reader models which do not support them.

Ready String: READY

☑ Log I/O Events

Alarm On:
- □ Auxiliary Input 1
- □ Auxiliary Input 2
- □ Door Alarm
- □ Duress
- □ F1 Key
- □ F2 Key

Clear Alarm On:
☑ Valid Access

Timeout: 10 seconds

Time Zone: Never

Ready String: This is the text that appears in the reader display when the reader is ready and waiting for the user to enter an ID. For example, if you want the readers to read *Enter ID* instead of *Ready* you could change the text here. You can enter up to fourteen characters. If you want this text centered in the reader's display, add spaces before the text if needed.

Log I/O Events: This entry only applies to the HandPunch. We do not recommend connecting a HandPunch to HandNet. The HandPunch is used for tracking time and attendance, which is not what HandNet is for. If you do connect a HandPunch and this box is checked, the reader records all activity (including invalid access attempts, door alarms, accessing command mode on the reader, etc.); if you do not have this checked, the HandPunch only records successful accesses. If you have an ID3D HandKey, HandKey II, or HandKey CR, the reader records all activity regardless of whether this is checked or not.

AUX1/AUX2

Aux1 contains the settings for the second auxiliary device that can be connected to a HandKey II or HandKey CR reader; *Aux2* contains the settings for the third (the settings for the first are on the *Auxiliary (AUX) Settings* tab; see page 48).

Alarm On: Even though this says *Alarm On*, the device does not have to be an alarm; this could trigger any type of auxiliary device. If a condition occurs and the corresponding box is checked, HandNet turns auxiliary output on if it is during the time zone selected at the bottom of the column on the right.

Auxiliary Input 1: This occurs if the reader receives input from an auxiliary input device. This is irrelevant if you do not have an auxiliary input device connected to the reader.

Auxiliary Input 2: This occurs if the reader receives input from the second auxiliary input device (HandKey II and HandKey CR support two auxiliary input devices; HandKey readers support just one). This is irrelevant if you do not have a second auxiliary input device connected to the reader.

Door Alarm: This occurs if the door connected to the reader is forced open, or if the door is kept open for longer than allowed based on the *Door Switch Shunt Time* on the *Configuration* tab in the *Reader Properties*; see page 48.

Duress Alarm: This occurs if a user entered the duress code. This code indicates that the user is in trouble or that someone is forcing the user to give him/her access; see page 47 for more on setting up a duress code.

F1 / F2 Key: This occurs if the corresponding key was pressed on the reader keypad (HandKey II and HandKey CR have F1 and F2 keys to the right of the number keys. The HandKey reader does not have these buttons, what you check here does not make any difference for that type of reader).

Invalid Access: This occurs if someone repeatedly entered a valid ID at a reader, and each time the reader does NOT recognize the user's hand (at the reader, the user would see the message *ID Refused*, and the *Activity* window would show the message *Access Denied*). The number of times that a user can try before this occurs depends on the *Number of Tries* entry on the *Settings* tab in the *Reader Properties*. If this occurs, someone might be trying to gain access with someone else's ID.

Power Failure: This occurs if the reader loses power from an external source. While this could just be due to an ordinary power failure, sometimes someone trying to gain invalid access will cut power in an attempt to disable alarm systems.

Tamper: This occurs if someone has shaken the reader roughly or opened the reader. Unless someone was servicing the reader, this message generally warrants further investigation.

Time Zone Violation: This occurs if a user enters a valid ID at a reader, but the user is not authorized to have access during the hours or days of the week based on the time zone associated with the reader in the access profile.

Try Again: This occurs if a user enters a valid ID at a reader, but the reader does not recognize the user's hand. This could be just the result of incorrect hand placement (if someone repeatedly entered a valid ID at a reader, and each time the reader does NOT recognize the user's hand, this would generate the *Invalid Access* condition above).

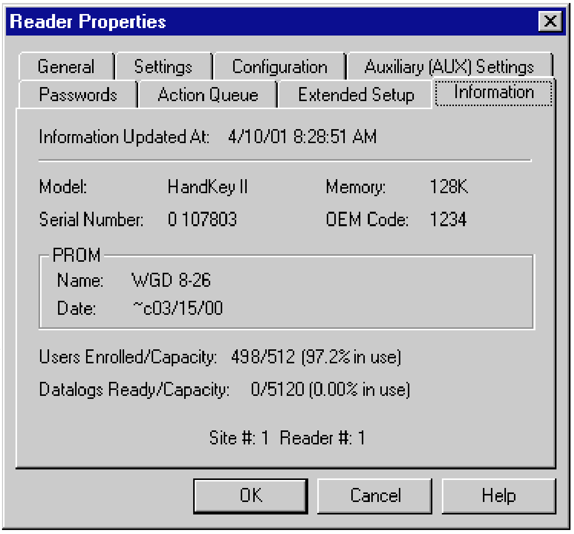
Clear Auxiliary Alarm On: If the auxiliary device is turned on, this controls whether it will be shut off when someone gains valid access (that is, enters a valid ID number and has his/her hand recognized). If this is checked, the alarm (or other auxiliary output) is turned off when a valid user gains access through that reader; if this is not checked, the output continues until the time entered in the following entry ends or until you go to the *Reader* menu, highlight *Auxiliary Output*, and pick *Off*; see page 129.

Timeout: This indicates the number of seconds that the auxiliary device should be on for.

Time Zone: This controls when HandNet should turn output to an auxiliary device on. For example, if the auxiliary device are a set of floodlights, it would only help to turn the lights on if the condition occurred at night. To do this, you would create a time zone for night hours, and then assign that time zone here (see page 61 for more on setting up time zones). If this says *Always*, HandNet turns output on for the auxiliary device whenever the checked condition(s) occur.

Information

This screen contains information about the reader. A key piece of information on this screen is the *Users Enrolled/Capacity:* this reflects the amount of available space in the reader. For example, the screen below reflects a reader with 498 users and space for up to 512 users. You could only add fourteen more users before this reader reached its limit. If you were approaching this limit, you would want to consider a memory upgrade for the reader so it would have space for additional users.



Information Updated At: 4/10/01 8:28:51 AM

Model: HandKey II
Memory: 128K
Serial Number: 0 107803
OEM Code: 1234

PROM
Name: WGD 8-26
Date: ~c03/15/00

Users Enrolled/Capacity: 498/512 (97.2% in use)
Datalogs Ready/Capacity: 0/5120 (0.00% in use)

Site #: 1 Reader #: 1

Most of the other information on this screen is helpful if your reader needs service, but not relevant to the ongoing use of the reader.

To get to this screen, click a reader in the right pane of the *Network* window, pick *Properties* from the *Reader* menu, and then click the *Information* tab.

* * * * *

Configuring the Physical Reader

While most of the information in the reader is controlled through HandNet, you must initially set up certain settings in the reader so it can communicate with HandNet. You do this through the command menus on the reader.

For readers with a network (ethernet) card: The IP address in this reader must match the *IP address on the Connection* tab in *Site Properties*; see page 39.

For a reader connected by serial port or connected as part of a chain of readers: The address in the reader must match the address on the *General* tab in *Reader Properties*; see page 45. The serial settings must also be correct, and the baud rate must match the baud rate on the *Connection* tab in *Site Properties*; see page 35.

We do not recommend changing any other settings through the reader command menus. All other settings can be controlled through *Reader Properties* in HandNet; see page 45 (if you were to make other changes directly in the reader, these would be overridden by the settings in HandNet when you enabled the reader).

Getting to the Setup Menu in the Reader

1. Enter command mode on the reader:

If you have a HandKey II or HandKey CR reader: Press *CLEAR*, and then press *ENTER*.

If you have an ID3D HandKey reader: Press *#* AND *** (you can press them at the same time, or one after the other).

If you have not used the reader with HandNet before, or if you have used it with HandNet and cleared its memory, the display looks like this.

```
ENTER PASSWORD
```

Type the password for the setup menu and press *ENTER* or *#.* If you have not changed it, the password is two (2).

If you have previously used the reader with HandNet and are reconfiguring it for another site or location, you may see:

```
READY:
*:
```

If the display looks like this, type your user ID and press *ENTER* or *#*. The reader will ask you to place your hand. Once you place it, you should then see the *Enter Password* display shown above. Type the password for the *Setup* menu and press *ENTER* or *#*. If you have not changed it, the password is two (2).

Changing the Reader Address

You must set the address in readers that are connected to the computer by a serial cable, and in readers that are connected to another reader (that is, readers that are not the first reader in the site). You cannot change the address in a reader that has an ethernet card; these readers automatically have an address of zero (0).

The following steps are specific to the HandKey II and CR; the menus are slightly different in other readers. Please see the manual that came with the reader if you are not sure how to find the correspond settings in your reader.

1. If you have not already done so, follow the steps on page 54 for getting to the reader setup menu.
2. Press the ** / NO* button until the display looks like this:

   ```
   SET ADDRESS
   *  NO     YES #
   ```

3. Press the *# / YES* button. The display will look like this:

   ```
   RDR ADD ID 1
   NEW?:
   ```

4. Type the new address. The address you enter must match the address on the *General* tab in *Reader Properties*; see page 45. Press *YES* or *ENTER*. The display returns to:

   ```
   SET ADDRESS
   *  NO     YES #
   ```

5. If you are done changing settings, press *CLEAR* to leave the *Reader Command* menu. If you need to change others settings, press *NO* until you get to the next setting you need to change.

Changing the Serial Settings and Baud Rate

You must have appropriate serial settings and baud rate in readers that are connected to the computer by a serial cable, and in readers that are connected to another reader (that is, readers that are not the first reader in the site). These settings do not apply to a reader with an ethernet card.

The following steps are specific to the HandKey II and CR; the menus are slightly different in other readers. Please see the manual that came with the reader if you are not sure how to find the correspond settings in your reader.

1. If you have not already done so, follow the steps on page 54 for getting to the reader setup menu.

2. Press the *NO* button until the display looks like this:

```
SET SERIAL
*  NO     YES #
```

3. Press the *YES* button. The display will look like this:

```
SET RS-485/422?
*  NO     YES #
```

4. Typically you will answer *YES* here. The display now asks for the baud rate. The baud rate here must match the rate on the *Connection* tab in *Site Properties*. Generally 9600 is appropriate.

   If you have a HandKey II or HandKey CR:

   The display will show the baud rate:

```
SET RS-485/422?
*  NO     YES #
```

   To accept the rate shown and continue, press *YES*. To change the rate, press *NO* to cycle through the choices until you find the one you want.

   If you have an ID3D HandKey: The baud rate is represented by a code:

baud rate	code	baud rate	code
38.4K	0	2400	4
19.2	1	1200	5
9600	2	600	6
4800	3	300	7

   For example, for 9600, you would enter the code of two (2).

5. The reader will display:

```
SET RS-232?
*  NO     YES #
```

Unless you have a printer connected directly to the reader, you would typically answer *NO* here. If you have a printer directly connected to this reader, answer *YES* (most users working with HandNet print from HandNet rather than connecting a printer directly to the reader). The only other time you might say *YES* here was if you had a single reader connected directly to HandNet with a serial port; there is a way to wire the connection to use RS-232 (if this were the case, you would say *YES*, pick the appropriate baud rate, and then indicate that RS-232 was connected to 1-Host (that is, HandNet)).

6. Once you are done, you see the *Set Serial* display again:

```
   SET SERIAL
*  NO     YES #
```

7. Press *CLEAR* to leave the command menu.

Changing the IP Address in a Reader with an Ethernet Card

You must set the IP address in a reader with an ethernet card. Before you do this, get the appropriate IP address and gateway (if needed) from your network administrator. If you have a WAN (wide area network), you also need the subnet mask; only certain subnet masks are supported; see the table below.

1. If you have not already done so, follow the steps on page 54 for getting to the reader setup menu.

2. Press the *NO* button until the display looks like this:

```
   SET SERIAL
*  NO     YES #
```

3. Press the *YES* button. The display will look like this:

```
   IP ADDRESS
000.000.000.000
```

   If the display says *Set RS-485/422?* at this point, the reader does NOT have a network card. Contact your dealer if you need to get one.

4. Quickly type the correct address; if you pause for more than about four seconds while entering the IP address, the reader advances to the next display without saving your change. The address will have four parts separated by periods. Enter each part as three digits; if one part has less that four digits, add zeros before that part of the number to make it three digits. You do not have to enter the periods. For example, if your administrator gave you the address 192.9.210.10, you would enter:

   192 009 210 010

   This address must match the IP address on the *Connection* tab in *Site Properties*; see page 39. Press *YES* or *ENTER*. The display will now look like this:

```
    GATEWAY
000.000.000.000
```

5. If your network administrator has told you to enter a gateway, do so; otherwise press *YES* or *ENTER*. As with the IP address, if you change this, you must type fairly quickly; if you pause for more than about four seconds while entering the gateway, the reader advances to the next display without saving your change. Once press *ENTER*, you see:

```
HOST BITS: 0
NEW?
```

6. If you are communicating over a LAN (local area network), type zero (0) for the Host Bits and press *YES* or *ENTER*. If you have a WAN, enter the number from the table below that corresponds to your subnet mask (only the subnet masks listed are currently supported). If you are not sure, check with your network administrator.

For this subnet mask:	Enter this for the host bits:	For this subnet mask:	Enter this for the host bits:
255.255.255.255	0	255.255.224.0	13
255.255.255.254	1	255.255.192.0	14
255.255.255.252	2	255.255.128.0	15
255.255.255.248	3	255.255.0.0	16
255.255.255.240	4	255.254.0.0	17
255.255.255.224	5	255.252.0.0	18
255.255.255.192	6	255.248.0.0	19
255.255.255.128	7	255.240.0.0	20
255.255.255.0	8	255.224.0.0	21
255.255.254.0	9	255.192.0.0	22
255.255.252.0	10	255.128.0.0	23
255.255.248.0	11	255.0.0.0	24
255.255.240.0	12		

7. The reader will display:

```
  9600 BAUD
* NO     YES #
```

The speed you choose should match the baud rate you are setting in the rest of the readers in this site. Generally 9600 is appropriate. To accept the rate shown and continue, press *YES*. To change the rate, press *NO* to cycle through the choices until you find the one you want.

Once you press *YES*, the reader display returns to:

```
  SET SERIAL
*  NO     YES #
```

8. If you missed one of the settings because the reader display changed too quickly for you, press *YES* to go through the settings again. If you are done changing settings, press *CLEAR* to leave the command menus.

9. If you need the changes to take effect immediately, disconnect the power from the reader, wait a few seconds, and then connect the power again. This resets the reader. If you do not do this, it may take up to six minutes for the changes to take effect.

* * * * *

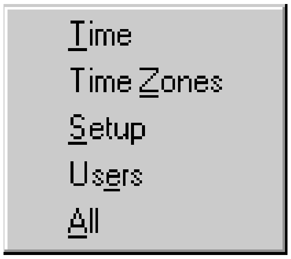
Resending Information to a Reader

Why You Might Need to Resend Information

While HandNet automatically sends the appropriate information to readers, occasionally you will need to use this when correcting a problem with a reader. You can do this with *Download* on the *Reader* menu.

Getting to the Download Option

To do this, select one or more readers, and go to the *Reader* menu, click *Download*, and then click the type of information to send.



Time: This sends the current time from the computer to the selected reader(s). You typically only need to use this option if the time changed (for example, for Daylight Savings Time). You can select all of your readers and send the time to all of them at once, or you can select specific readers.

Time Zones: This sends time zone and holiday information to the selected reader(s). You need to download this information if you change *Time Zones* (page 61) or *Holidays* (see page 65).

Setup: This sends configuration information to the selected readers. In most cases this is done automatically.

Users: After adding users, you need to download them to the hand readers so the readers will recognize the new users. This sends all current users to the selected readers.

All: This sends *Time, Time Zones, Setup*, and *User* information to the selected reader(s). You would use this when you set up a new reader so the reader had all the needed information.

Confirming That You Want to Send Information to the Reader

Whenever you choose to download information to readers, HandNet asks you to confirm that you want to download to the selected reader. Click *YES* to continue.

* * * * *

Settings That Control User Access

Setting Up Time Zones

What Time Zones Are

Time zones are periods of time on different days of the week when users can have access. There is no connection between what we call time zones in HandNet and the time zones we usually think of that have to do with different times around the world. This does not have anything to do with Eastern, Central, Mountain, or Pacific time; it only has to do with controlling which hours of the day access is available through readers.

When You Need to Set Up Time Zones

If you want some users to be able to use certain readers only during certain hours or on certain days of the week, time zones let you identify when access is available. For example, suppose some users should only be able to gain access through certain readers between 8:00 AM and 5:00 PM, Monday through Friday. You would create a time zone that identified these times and days, associate that time zone with appropriate readers using an access profile, and then assign that access profile to the users. After you did this, users with that access profile would only have access during the times you identified in the time zone.

You can also use time zones to determine when certain doors should be automatically unlocked; see *Automatically Unlocking a Door on a Scheduled Basis* on page 128.

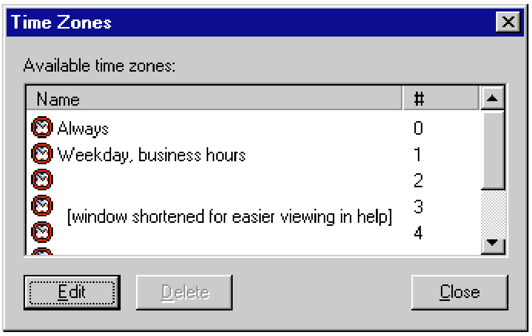
If users should have different access on holidays than on other days, you can set different hours for holidays in the time zone. You will have to also set up holidays; see page 65.

When You Do not Need to Set Up Time Zones

If you do not need to limit access by day or time (that is, if users could use the readers twenty-four hours a day, seven days a week if they wanted), and if you do not want doors to unlock automatically, you do not need to set up time zones.

Getting to the List of Time Zones

1. Click the *View* menu.
2. Click *Time Zones*. You see a screen like the one below (though the time zones listed will be different). From here you can add, change, or delete time zones.



Name	#
Always	0
Weekday, business hours	1
	2
[window shortened for easier viewing in help]	3
	4

Adding or Changing Time Zones

The first time zone is *Always* and the last (#61) is *Never*; you cannot change either of these.

To add a time zone, click one of the blank lines in the time zone list and click *Edit*. To change a time zone, click the time zone to change and click *Edit*. Change the *Time Zone Definition* screen (see below) as needed and then click OK to return to this list. You can then add or change another or click *Close* when done.

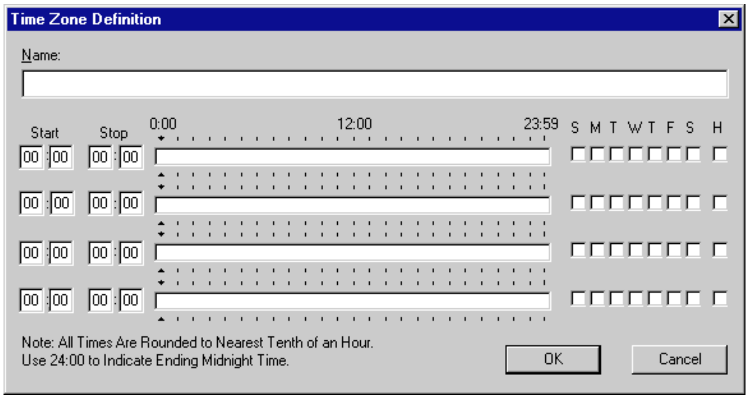
Deleting Time Zones

Click the time zone and click *Delete*. The program asks if you are sure you want to delete the time zone. Click *Yes*.

If you try to delete a time zone and get a message that the time zone is used in an access profile, you must close the time zone window, go to access profiles and select a different time zone for each reader that had this time zone selected if you still want to delete it.

Time Zone Definition Screen

This screen determines what hours access is available on different days of the week. A time zone is active if the time is equal to or after the start time and before the stop time, and if the day of the week matches one of those checked.



Start	Stop	S	M	T	W	T	F	S	H
00 : 00	00 : 00	□	□	□	□	□	□	□	□
00 : 00	00 : 00	□	□	□	□	□	□	□	□
00 : 00	00 : 00	□	□	□	□	□	□	□	□
00 : 00	00 : 00	□	□	□	□	□	□	□	□

Note: All Times Are Rounded to Nearest Tenth of an Hour.
Use 24:00 to Indicate Ending Midnight Time.

Name: Enter a name that will be clear to you so that when you associate the time zone with a reader in an access profile, you will be sure to pick the right one.

You can assign four different periods in each time zone if you need them; for example, if you want to give access during different hours on different days. Be sure to leave lines that you do not need blank.

Start/Stop Times: Enter hours after noon using military time. Use the chart below or see the examples if you need help. Times are divided into tenths of an hour, so HandNet rounds minutes to the nearest six minute interval. For example, if you enter 8:02, the program rounds this to 8:00; if you enter 8:03, the program rounds it to 8:06.

	Enter on the Time Zone screen		Enter on the Time Zone screen
noon	12:00	**7:00 PM**	19:00
1:00 PM	13:00	**8:00 PM**	20:00
2:00 PM	14:00	**9:00 PM**	21:00
3:00 PM	15:00	**10:00 PM**	22:00
4:00 PM	16:00	**11:00 PM**	23:00
5:00 PM	17:00	**midnight**	00:00 if a start time; 24:00 if a stop time
6:00 PM	18:00		

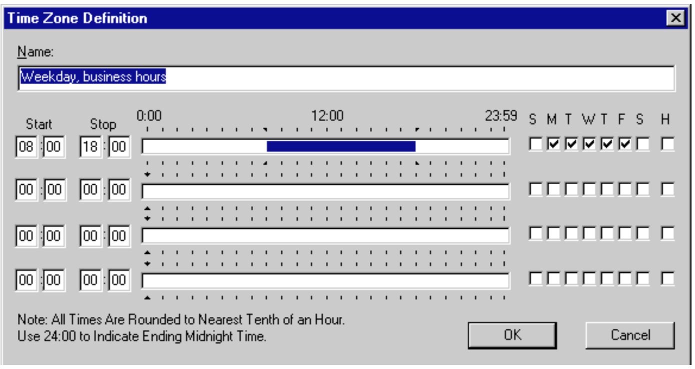
If a time zone must cross midnight (for example, if you want to give access between 8:00 PM and 4:00 AM), you must use two lines to create that access time. The first line would give access from 20:00 to 24:00 (that is, 8:00 PM to midnight), and the next line would give access on the same days of the week from 0:00 to 4:00 (that is, midnight to 4:00 AM). See the third example on the following page.

Days of the Week: Check the boxes for each of the day of the week that access should be available. The letters over the boxes correspond to the days of the week (Sunday through Saturday); H stands for holiday. If access is different on holidays than on other days, you must also set up holidays; see page 65. See the examples on the following page.

Click *OK* when done.

Examples of Time Zone Settings

These settings give access between 8:00 AM and 6:00 PM, Monday through Friday. They do not give any access on Saturday, Sunday, or Holidays. The blue bar in the center section of the screen shows when access is available.

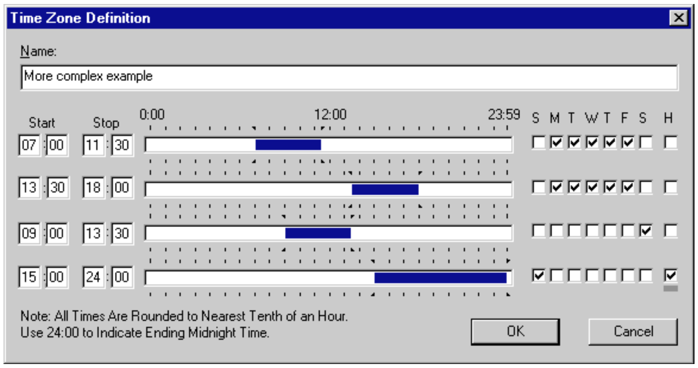


Name: Weekday, business hours

Start	Stop	S	M	T	W	T	F	S	H
08 : 00	18 : 00	□	☑	☑	☑	☑	☑	□	□
00 : 00	00 : 00	□	□	□	□	□	□	□	□
00 : 00	00 : 00	□	□	□	□	□	□	□	□
00 : 00	00 : 00	□	□	□	□	□	□	□	□

Note: All Times Are Rounded to Nearest Tenth of an Hour.
Use 24:00 to Indicate Ending Midnight Time.

The following settings give access from 7:00 to 11:30 in the morning on weekdays, from 1:30 in the afternoon to 6:00 PM also on weekdays, from 9:00 in the morning to 1:30 in the afternoon on Saturdays, and from 5:00 PM to midnight on Sundays and holidays.

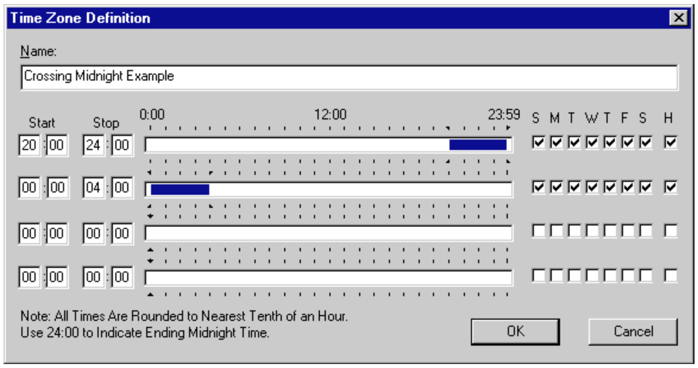


Name: More complex example

Start	Stop	S	M	T	W	T	F	S	H
07 : 00	11 : 30	□	☑	☑	☑	☑	☑	□	□
13 : 30	18 : 00	□	☑	☑	☑	☑	☑	□	□
09 : 00	13 : 30	□	□	□	□	□	□	☑	□
15 : 00	24 : 00	☑	□	□	□	□	□	□	☑

Note: All Times Are Rounded to Nearest Tenth of an Hour.
Use 24:00 to Indicate Ending Midnight Time.

The following settings show how to cross midnight. This gives access from 8:00 PM through 4:00 AM any day of the week. Notice that this requires two lines to set up: the first going from 8:00 PM to midnight, and the next going from midnight to 4:00 AM.



Name: Crossing Midnight Example

Start	Stop	S	M	T	W	T	F	S	H
20 : 00	24 : 00	☑	☑	☑	☑	☑	☑	☑	☑
00 : 00	04 : 00	☑	☑	☑	☑	☑	☑	☑	☑
00 : 00	00 : 00	□	□	□	□	□	□	□	□
00 : 00	00 : 00	□	□	□	□	□	□	□	□

Note: All Times Are Rounded to Nearest Tenth of an Hour.
Use 24:00 to Indicate Ending Midnight Time.

* * * * *

Setting Up Holidays

When You Need to Set Up Holidays

If you want to prevent access on holidays or to give different access on holidays than on other days, the holidays list identifies when those holidays are. When you reach a holiday in the list, HandNet applies the holiday access times instead of the regular access times (if you set holidays up, you will also have to set up time zones to indicate what access users should have on different days; see page 61 for more on setting up time zones).

When You Do not Need to Set Up Holidays

If you do not give different access on holidays than on other days, you do not need to set up any holidays.

Adjusting Holidays Each Year

If you set holidays up, remember to return to the holidays setup at the beginning of each year to adjust each holiday that is celebrated on a different date than the previous year. For example, Thanksgiving, Memorial Day, and Labor Day are on different dates each year. Also, while holidays like Christmas and New Year's are always on the same date, when these holidays fall on a weekend, the day they are taken off is sometimes on a different date.

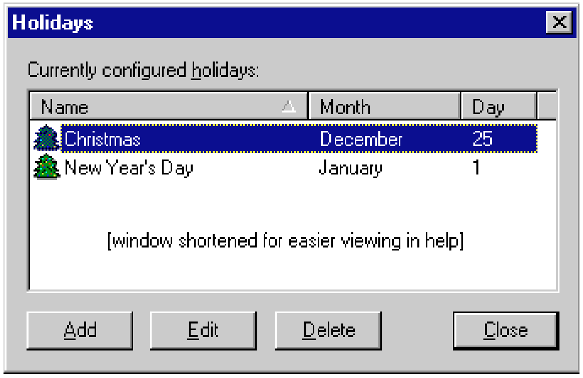
Getting to the Holidays List

1. Click *View* from the *Main Menu* bar.

2. Click *Holidays*. You see a list like this one below. From here you can add, change, or delete holidays.

Adding or Changing Holidays

To add a holiday, click *Add*; to change a holiday, click the holiday in the list and then click *Edit*. When you add or edit, you see this screen:



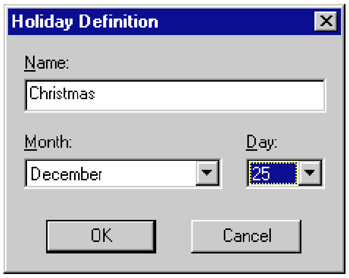
Currently configured holidays:

Name	Month	Day
Christmas	December	25
New Year's Day	January	1

[window shortened for easier viewing in help]

Name: Enter a name to help you identify the holiday.

Month: Click this entry and pick the month from the list (you could also press *TAB* from the *Name* entry and then type the first letter of the month. If more than one month begins with the same letter, typing that letter cycles through those months).



Name: Christmas

Month: December

Day: 25

Day: Click this entry and pick the day from the list (you could also press *TAB* from the *Month* entry and then type the first digit. For example, if you want to get to twenty-five, you would type two (2) several times. The first time you type two (2), the date would show *2*; when you type two (2) a second time, you would see *20*; typing two again would switch to *21*; you would repeat this until you got to the number you need).

Click *OK* when each entry is correct.

Deleting Holidays

To delete a holiday: Click the holiday in the list and click *Delete*.

* * * * *

Setting Up Access Profiles

When You Need to Set Up Access Profiles

If some users can only use certain hand readers and/or only use them at certain times or on certain days, access profiles define when each type of user can use each reader. For example, suppose your maintenance staff should have access to the maintenance rooms seven days a week, your office staff should have access to the office but only during business hours, and your supervisors should have access to everything at any time. You would create three access profiles: one for supervisors, one for office staff, and one for maintenance personnel. These profiles would identify which readers each group could use. In these profiles you would also identify which time periods each group could use each reader (you would set up these time periods first using *Time Zones*). After creating these different profiles, whenever you added a user, you would just identify which group the user was a part of, and the access profile for that group would automatically give the appropriate access.

To limit access to certain days or times, you must set up time zones before creating access profiles; see page 61 for more on setting up time zones.

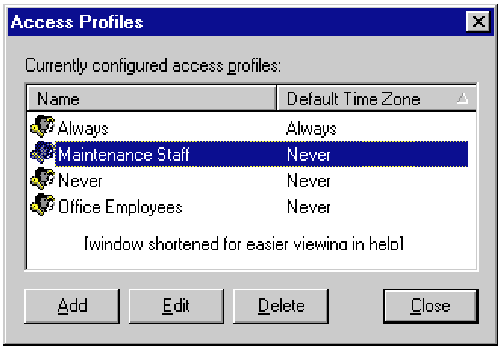
When You Do Not Need to Set Up Access Profiles

If you want all users to be able to use every reader any time, you do not need to set up access profiles. HandNet comes set up with an *Always* profile that lets users use any reader in the system twenty-four hours per day, seven days per week (it also has a *Never* profile that does not let the user verify at any reader at any time).

Getting to the List of Access Profiles

1. Click the *View* menu from the main menu bar.

2. Click *Access Profiles*. You see a screen like the one below (though the profiles listed will be different). From here you can add, change, or delete access profiles.



Access Profiles

Currently configured access profiles:

Name	Default Time Zone
Always	Always
Maintenance Staff	Never
Never	Never
Office Employees	Never

[window shortened for easier viewing in help]

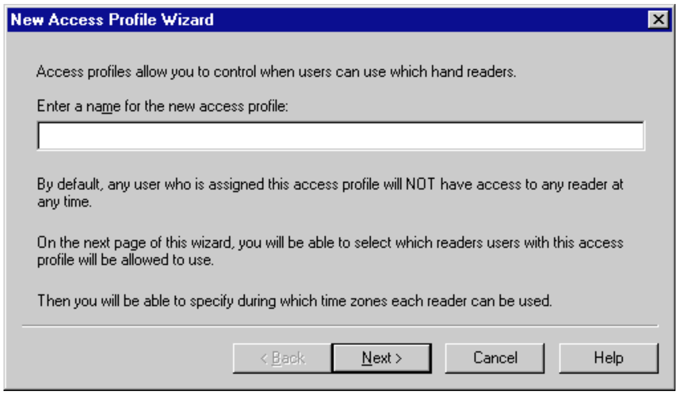
The *Default Time Zone* shown on this list does NOT reflect the time zones associated with the readers in this profile; it only reflects the time zone that HandNet initially picks if you associate another reader with this profile. Except for the *Always* profile, this column always says *Never*.

Adding an Access Profile

Click the *Add* button to add an access profile. This starts the *New Access Profile Wizard*.

New Access Profile Wizard, Screen 1

You see the *New Access Profile Wizard* when you add a new access profile to the list of access profiles.



New Access Profile Wizard

Access profiles allow you to control when users can use which hand readers.

Enter a name for the new access profile:

By default, any user who is assigned this access profile will NOT have access to any reader at any time.

On the next page of this wizard, you will be able to select which readers users with this access profile will be allowed to use.

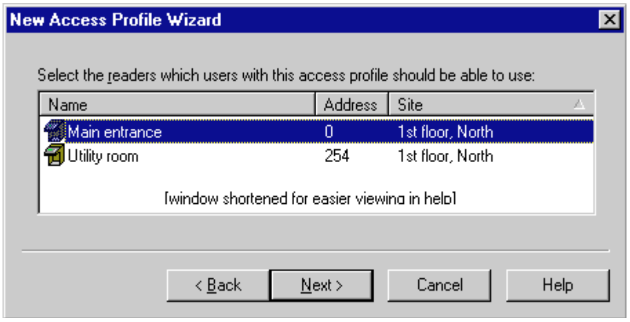
Then you will be able to specify during which time zones each reader can be used.

Name: Enter a name that describes the group of users that this access profile will be used for. For example, if this profile gives access that is appropriate for all of your maintenance staff, you could use that for the name. The important thing is for the name to be clear so that you do not give inappropriate access to users.

Click the *Next* button to go to the next screen.

New Access Profile Wizard, Screen 2

The second screen in the *New Access Profile Wizard* lists all of your readers (typically you will have many more than the two shown in the example below). Select each reader that you want to give access to with this profile, and then click *Next*.



New Access Profile Wizard

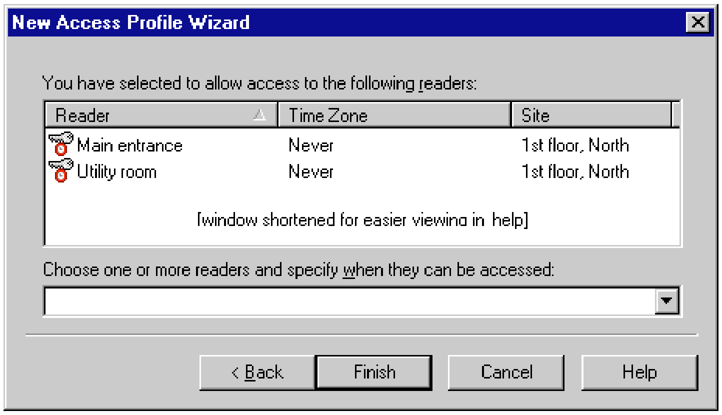
Select the readers which users with this access profile should be able to use:

Name	Address	Site
Main entrance	0	1st floor, North
Utility room	254	1st floor, North

[window shortened for easier viewing in help]

New Access Profile Wizard, Screen 3

The third and final *New Access Profile Wizard* screen shows all of the readers that you selected on the previous screen (if you discover that you missed a reader on the previous screen, click the *Back* button to return to the list of all readers and select it there).



New Access Profile Wizard

You have selected to allow access to the following readers:

Reader	Time Zone	Site
Main entrance	Never	1st floor, North
Utility room	Never	1st floor, North

[window shortened for easier viewing in help]

Choose one or more readers and specify when they can be accessed:

When you come to this screen, each reader has a time zone of *Never*; you must change the time zone for each reader to give access to that reader through this profile.

To associate time zones with the readers:

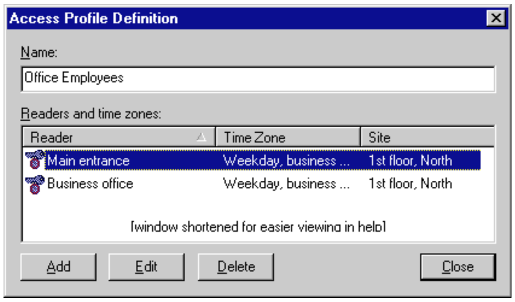
1. Select one or more readers on the list. If you forget to select readers, HandNet still lets you do the following step but it will not have any effect.

2. Click on the entry under *Choose one or more readers...* and select a time zone there. HandNet uses that time zone for each selected reader.

If you need to associate a different time zone with some readers, repeat these steps until you have specified a time zone for each reader. For example, suppose you were creating an access profile for maintenance workers, and suppose these workers had access to building entrances and maintenance facilities twenty-four hours a day, but they only had access to the business offices during normal business hours. You would select the entrance and maintenance readers and associate a time zone of *Always* with them. You would then select the business office readers and associate your normal business hours time zone with those readers.

Changing an Access Profile

To change an access profile, click it on the list and then click the *Edit* button. That brings up a list of readers that have been associated with the profile. The list looks like this:



Name: Office Employees

Readers and time zones:

Reader	Time Zone	Site
Main entrance	Weekday, business ...	1st floor, North
Business office	Weekday, business ...	1st floor, North

[window shortened for easier viewing in help]

To add another reader to those associated with this profile: Click the *Add* button to bring up the *Access Profile Override* box (shown on the following page). Complete the entries there and click *OK*.

To change the time zone a reader is accessible with this profile: Click the reader in the list and click *Edit* to bring up the *Access Profile Override* box. Click the *Time Zone* entry, select the appropriate time zone, and then click *OK*.

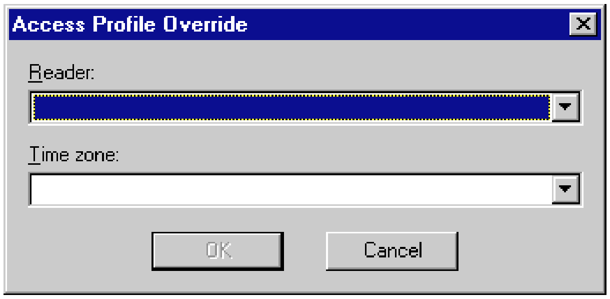
To change the time zone for several readers at once: Hold the *CTRL* key down and click each reader that you want to change the time zone. When all the appropriate readers are selected, click *Edit*. This brings up the *Access Profile Override* box but you can only change the *Time Zone* entry. Click the *Time Zone* entry, select the appropriate time zone, and then click *OK*.

To remove one or more readers from this access profile: Select the reader(s) in the list and click *Delete*.

Click *Close* to return to the list of profiles.

Access Profile Override Box

You see this same screen whether you are adding a reader to a profile or editing a reader that you have added previously (when adding the entries are initially blank; when editing, the entries are filled in with your previous choices).



Reader: Click this to choose a reader that should be associated with this profile. This only lists readers that have not already been added to this profile. If you click this and an empty pick box comes up, then you have already added all readers to this profile. This entry is disabled if you are changing several readers at once.

Time Zone: Click this and pick the time zone that the users with this profile should have access to the selected reader(s). If you have selected several readers, this changes all of them at once.

Click *OK* to return to the list of readers in this profile.

Deleting an Access Profile

To delete an access profile, click the profile on the list and click the *Delete* button. HandNet does not ask you to confirm the deletion, so make sure you pick the right one.

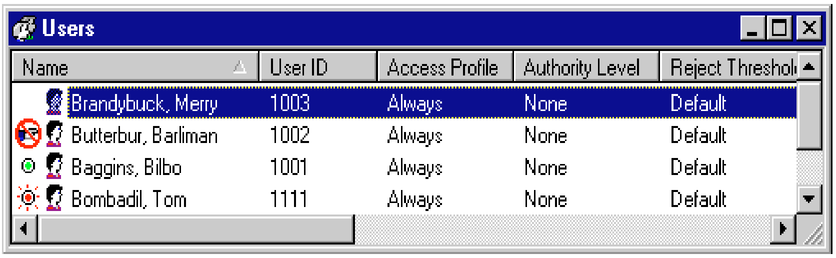
If you get a message that the access profile you are trying to delete is still assigned to a user, go to the list of users, double-click the user to go to the *User Properties*, click the *Security* tab, and select a different access profile for the user there. The message only lists the last user that the profile was assigned to, so there may be other users that also use the profile. Check the list of users to see if any other users use that profile (click the heading of the profile column in the user list to sort by profile; that will put all users with each profile together). If you find any other users using the profile you want to delete, select a different profile for each of them as well. Once no users are using the profile, you can return to this option and delete the profile.

* * * * *

Adding and Maintaining Users

Users Window

The users window lists every user that is in HandNet. To open this window, pick *Users* from the *View* menu or press *CTRL-U*.



Name	User ID	Access Profile	Authority Level	Reject Threshol
Brandybuck, Merry	1003	Always	None	Default
🚫 Butterbur, Barliman	1002	Always	None	Default
🟢 Baggins, Bilbo	1001	Always	None	Default
🔴 Bombadil, Tom	1111	Always	None	Default

Understanding the Icons to the Left of the Name

	No icon indicates that the user is enrolled able to use any readers permitted by the access profile.
🚫	The no access icon indicates that the user is not enrolled yet and hence will not have access to any readers. You must enroll the user to give access; see page 87.
🟢	The green light indicates that the user currently has access, and that the limited access feature was used to so this access will automatically expire at some point; see page 93 for more about limited access.
●	The black dot indicates that the limited access feature was used to set a begin and end date/time for this user’s access, and the user does NOT have access because the access period has not started yet; see page 93 for more about limited access.
🔴	The red light indicates that the limited access feature was used to set a begin and end date/time for this user’s access, and the user does NOT have access because the access period has ended; see page 93 for more about limited access.

Changing How the User List is Sorted

You can sort the list of users using the information in any column by clicking on the column heading. For example, to sort the user list alphabetically by name, click on the name heading. If you click on the same heading again, it will sort the list in reverse order (for example, using the name, it would sort from Z to A). Usually sorting by name or ID is most useful, but occasionally you might sort by another column to put all similar users together. For example, if you were preparing to change or delete a particular access profile, you might sort by the access profile column so that all users with that profile would be together on the list.

Rearranging Columns in the User Window

To move any column, click the column heading and hold the mouse down. With the mouse held down, drag the column heading to the left or right; see the online help for an example of this.

You might want to move columns to keep important information like user IDs out of view, or, if you have created custom user entries, you might want to move them to where you can see them, since they are initially out of view.

F5 restores all columns to the positions they had when you started HandNet. If you want HandNet to save the new column positions, exit the HandNet program and come back in. HandNet then uses your changed column positions as the new standard or default.

Changing Column Width

You can also change the width of a column by pointing to the edge of the column heading, holding the mouse down, and then dragging the edge of the column to the desired position. This lets you fit more columns in the window (or, if you wanted to hide information from the casual observer, you could make columns wider to push other columns out of view); see the online help for an example of this.

F5 restores all columns to the widths they had when you started HandNet. If you want HandNet to save the new column widths, exit the HandNet program and come back in. HandNet then uses your changed column widths as the new standard or default.

Columns of Information in the User Window

User ID: The ID number the user must enter at the reader to gain access.

Access Profile: The profile determines which readers the user can access and when. You set up access profiles using *Access Profiles* on the *View* menu. You can change a user's access profile on the *Security* tab in *User Properties*; see page 92.

Authority Level: This indicates whether the user is allowed to access the command menus on the readers. For most users, this should say *None*. You can change a user's authority level on the *Security* tab in *User Properties*; see page 92.

Reject Threshold: The reject threshold controls how closely a user's hand must match the stored hand profile for the user to gain access. If this says *Default*, then HandNet uses the *Reject Threshold* on the *Configuration* tab in the *Reader Properties* (see page 47). If this says *Default** (with an asterisk), this means the user does not need hand recognition to gain access because the user was set up with a special enrollment; see page 76. If this shows a number, someone chose to override the standard reject threshold on the *Security* tab in *User Properties*; see page 93. A lower number requires a very precise match to gain access; a high number requires the hand to match less exactly. Thirty is the lowest number possible; 250 is the highest. One might use a lower number for users with access to the highest security areas; one might need a higher number if a user had arthritis or other hand condition that made it impossible to consistently place the hand on the reader in exactly the same position.

Last Site: This lists the last site where the user gained access. This is blank for a new user who has not accessed a reader yet.

Last Reader: This lists the last reader the user gained access through. This is blank for a new user who has not accessed a reader yet.

Last Time Used: This shows the date and time of the user's last access.

Limited State: This says *Unlimited* for users who are not set up to only have access for a limited period of time, that is, for users whose access will continue indefinitely. For users who are set up to only have access for a limited period of time, this says *Waiting* if the access period has not started yet, *Limiting* if the user currently has access, and *Expired* if the user's access period has ended; see page 93 for more about limited access.

Limited Start Time: If this user has been set up to have access for a limited period of time, this shows the date and time that the user's access begins. HandNet will not give the user access before this date/time. This is blank for other users; see page 93 for more about limited access.

Limited End Time: If this user has been set up to have access for a limited period of time, this shows the date and time that the user's access ends. HandNet will not give the user access after this date/time. This is blank for other users; see page 93 for more about limited access.

Additional Custom Columns: If you created any custom user entries, those columns would be listed as well; see page 97 for more about adding custom entries.

* * * * *

Adding Users Overview

Before You Add Users

If you are going to limit access to specific time periods or specific readers, set up *Time Zones* (see page 61) and *Access Profiles* (see page 67) before you set your users up.

Choosing How to Add the Users

If you have already set up users in a stand alone reader: You do not need to add users; you can upload user information from the reader; see *Getting User Information from a Reader* on page 99.

If you have been using one of our MS-DOS HandNet products (HandNet or HandNet Plus): You do not need to add users; you can import them from HandNet(+); see page 98.

If you only have one user to add, if you do not assign ID numbers sequentially, if you are adding users with different access profiles, if you want to fill in custom entries when adding the users, or if users choose their own ID numbers: Add a single new user; see page 76.

If a user needs access without hand recognition: Add a single new user and choose the *Special Enrollment* option. Before you do this, read *Adding a User Who Has Access Without Hand Recognition* below.

If you have many new users with the same access profile and you want automatically assigned ID numbers: Add multiple new users; see page 81.

Adding a User Who Has Access Without Hand Recognition

If a user has severe arthritis, missing fingers, or other hand deformities that keep the user's hand from being recognized, you can give the user access without hand recognition (if you choose this, the reader still asks the user to place a hand on the reader so it will not be apparent to others that hand recognition is not required, but the reader does not check the image of the hand; it gives access regardless of whose hand is placed there). **Since bypassing hand recognition gives you reduced security, only use this as a last resort.** Try these options first:

> **If the user only has a problem with the right hand:** Enroll the user using the left hand (the user will place the hand palm up on the reader).
>
> **If the user has all of his/her fingers and is just having trouble with placing the hand consistently:** On the *Security* screen in *User Properties*, check *Override the reader's reject threshold*, and drag the pointer to the far right (the *Less Sensitive* side). This causes the reader to be more tolerant of what it considers a match for that user's hand.

If these options are not possible, or if you try them and they do not work, then you will have to set the user up so that hand recognition is not required. To do this, follow the steps below.

1. If you have already added this user, open the *User* window, click the user once, press the *DEL* key (or pick *Delete* from the *User* menu), and confirm that you want to delete the user.

2. Click the *User* menu and then click *Add New….* This takes you to the first screen of the *New User Wizard*.

3. Check the *Special Enrollment* box. Since this option does give lower

security, HandNet asks you to confirm that you want to do this; click *Yes*.

4. Click the *Next* button.

5. Complete the rest of the process just as you would for any other new user.

6. Since the reader does not have to recognize this user's hand, you do not need to enroll this user; once you click *Finish*, the process is done for this user.

Allowing Users to be Added at the Reader

HandNet is initially set up to only allow new users to be added in the program; you can enroll a user at a reader, but you cannot add a new user there. If you want to be able to add and enroll a new user at a reader without adding the user to HandNet first, do this:

1. Click the *View* menu.

2. Click *Settings*.

3. Click the *Security* tab.

4. Check the box by *Do not delete unauthorized enrollments*.

5. Underneath this, indicate what access profile should be given to a user who is added at a reader (if you do not want the user to be able to access any readers until you change them in HandNet, choose *Never*).

6. Click the *OK* button at the bottom of the box.

Preventing Users from Being Added at Readers

Follow the steps above to get to the *Security* tab and make sure that *Do not delete unauthorized enrollments* is NOT checked.

* * * * *

Adding a Single New User

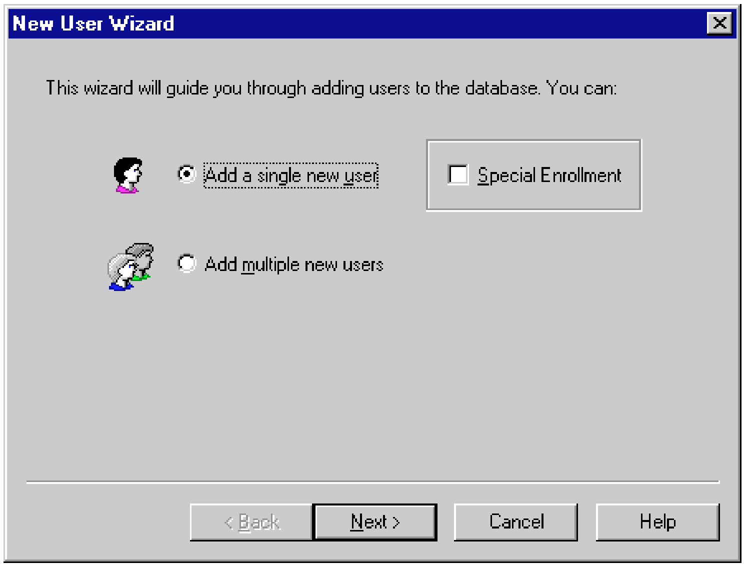
QUICK STEPS

Adding a Single User

1. Click the *User* menu and then click *Add New....* This takes you to the first screen of the *New User Wizard*.
2. *Add a single new user* is automatically selected, so click *Next* to continue.
3. On the *Name/ID* screen, enter the name and the ID number you are assigning to that user, and then click *Next* to continue.
4. On the *Security* screen, choose the access profile, authority level, and other security options. If you have set up custom user entries, click *Next*; otherwise click *Finish*.
5. If you see the *Custom* entries screen, fill in the column on the right and then click *Finish*.
6. Once you are done adding the user, you must enroll the user before the user will have access; see page 87.

Beginning the Process

To begin adding a new user, pick *Add New...* from the *User* menu.



New User Wizard

This wizard will guide you through adding users to the database. You can:

● Add a single new user

□ Special Enrollment

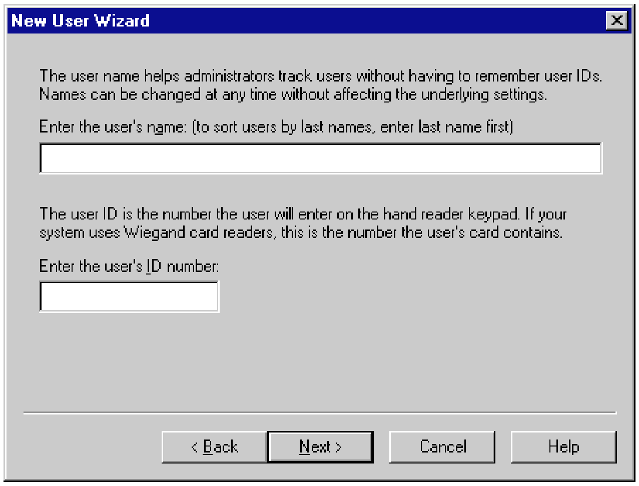
○ Add multiple new users

Special Enrollment: Check this box only if the user has severe hand deformities that require you to give the user access without hand recognition. This box is disabled if you are adding multiple users; if you are enrolling a user without hand access, you must add a single user.

Click *Next* to continue.

Name/ID Screen

This is the second screen in the process of adding a single new user:



The user name helps administrators track users without having to remember user IDs. Names can be changed at any time without affecting the underlying settings.

Enter the user's name: (to sort users by last names, enter last name first)

The user ID is the number the user will enter on the hand reader keypad. If your system uses Wiegand card readers, this is the number the user's card contains.

Enter the user's ID number:

Name: Enter the user’s name.

If you want to sort the list of users by last name: Enter the last name first. For example, if the user’s name is Sam Gamgee, you would enter *Gamgee, Sam*.

If you have two users with the same name: You must enter a unique name for each user. If two users have the same name, you might add a middle initial, or you might add a job description after each. For example, if you have two users named John Jones, you might enter something like *Jones, John (engineer)* and *Jones, John (maintenance).*

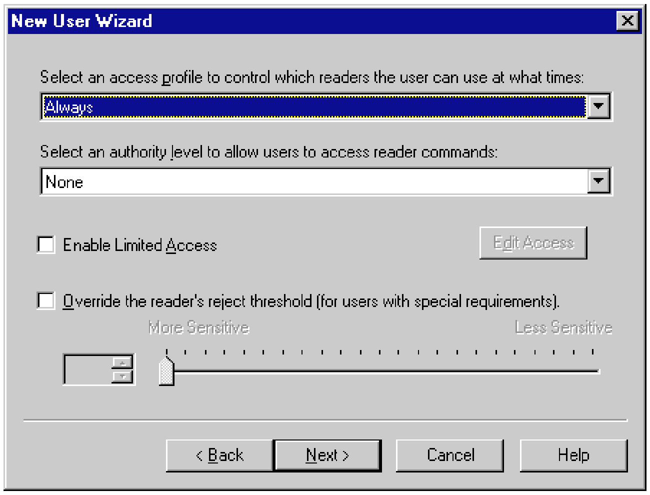
ID Number: Each number must be unique (if you could give the same number to two users, the reader would not know which was trying to gain access). Longer numbers are slightly more secure, but four or five digits are generally adequate in context where user’s must enter the number. You may enter up to ten digits if you do not use a duress code, or up to nine digits if you do use a duress code. If you use a duress code, make sure that you do not create an ID that begins with that digit (see page 47 for more about duress codes). If you have set up an ID length on the *Settings* tab in the *Reader Properties* (see page 46), make sure that you do not create an ID that is longer than this.

If you use Wiegand card readers: Enter the ID number that is stored on the card.

Do not begin an ID with 0 (zero) if you are going to enroll the user with the command menus on the reader: HandNet lets you enroll a user by either picking *Enroll* from the *Reader* menu, or by using the *Command* menus on the reader (see page 88 for more about these options). If you are going to use the command menus on the reader, the *ID Number* should not begin with zero (0). While HandNet distinguishes between *5* and *0005*, the process of adding a user from the reader command menu does not. This means that if you create a user with an ID of 0005 in HandNet and try to enroll that user with the command menus on the reader, when you type 0005, the reader thinks you are enrolling user 5. This will not correspond with 0005 in HandNet. If you are going to use *Enroll* on the *Reader* menu, you can begin an ID with zero (0) (if you are never going to begin an ID with zero, this might be a good choice for a duress code if you use one).

Security Screen

This screen controls what this user has access to and when.



New User Wizard

Select an access profile to control which readers the user can use at what times: Always

Select an authority level to allow users to access reader commands: None

□ Enable Limited Access

□ Override the reader's reject threshold (for users with special requirements).

Select an access profile to control which readers the user can use at what times: Click this entry for a list of available access profiles. If this user can use all readers at all times, choose *Always*. If you do not want the user to be able to use any readers, choose *Never*. For other access, select the appropriate profile. You must set access profiles up before they are available here; see page 67 for more on setting up access profiles.

Select an authority level to allow users to access reader commands: This determines what the user can do at the reader. Each higher level gives access to the lower levels as well. For example, a user with an authority level of four can also use the *Level 1, 2* and *3* menus. Except for recalibrating the reader (part of *Level 1*), and enrolling a user if you have not purchased the upgrade to the full feature set, HandNet can control every setting in the reader, so there is generally no need to control settings through the reader menus.

None: This lets the reader gain access through the reader, but not use the command menus in the reader to change the reader's settings. This choice is appropriate for most users.

(1) Service: This lets you recalibrate the reader and change the reader's status display.

(2) Setup: This lets you control reader setup issues including how the reader is connected to your computer network, what language the reader displays in, the date/time, etc.

(3) Management: This lets you list users.

(4) Enrollment: This lets you add or remove users.

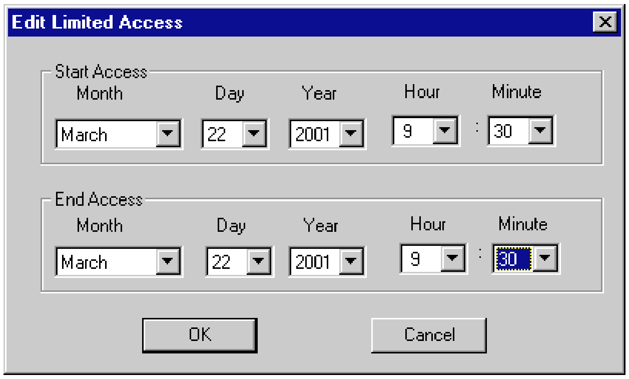
(5) Security: This lets you control the passwords for the reader menus, change time zones, enroll users who do not need hand access, etc.

See the HandKey manual for more on directly changing settings through the reader.

Limited Access

Enable limited access: This gives a user access for a specific date range. For example, suppose a contractor or temporary employee was going to be working in your building for a month. Or suppose an employee gave notice that s/he was leaving for a new job in two weeks. Once this period was over, you would not want these users to have access. Rather than having to remember to disable the user on the appropriate date, this option lets you set a start and end date/time so the user is automatically enabled and disabled at the appropriate points.

To set up start and end date/times, check the box by this button and then click the *Edit Access* button (this button only works if you have checked the box). This takes you to the *Edit Limited Access* screen:



Edit Limited Access

Start Access

Month	Day	Year	Hour		Minute
March	22	2001	9	:	30

End Access

Month	Day	Year	Hour		Minute
March	22	2001	9	:	30

To change either start or end date or time, click the corresponding entry and pick from the list that comes up.

This option is disabled if you have not purchased the license upgrade to the full feature set of Version 2.0.

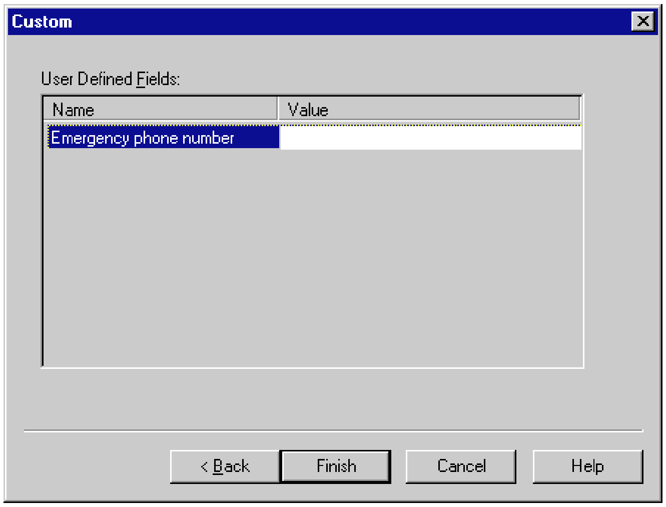
This option is NOT for limiting access to specific readers or for specific times of the day; to control that, use the *Access Profiles* entry.

Override the reader's reject threshold (for users with special requirements): For users with a physical condition like arthritis that prevents them from placing their hands on the reader in exactly the same way each time, this option lets you control how exact the hand match must be for the reader to grant access.

Normally you would not change this when adding the user. Instead, add and enroll the user, and then see if the user is having trouble gaining access. If a user is having trouble getting access consistently, go to the *Security* tab in the *User Properties* and change this entry there. You would check this box and then slide the pointer further to the right (the *Less Sensitive* side). If a user has a really severe hand condition, it is possible to give access without hand recognition, but because this offers reduced security, that should only be a last resort.

Custom Entries Screen

You only see this screen if you have set up any custom user entries (see page 97). The entries on this screen vary depending on what you have set up. For each entry on this screen, type the information in the *Value* column.



Name	Value
Emergency phone number	

Click *Finish* when done.

What to Do Next

The next step is to enroll the user; see page 87.

* * * * *

Adding a Group of Users at Once

You would add a group of users at once if you have to add many new users with the same access profile and other security access options, and if you want HandNet to automatically assign sequential ID numbers (if each user needs a different access profile, if you need to assign non-sequential ID numbers, or if you want to fill in custom user entries while adding the users, add single users instead; see *Adding a Single New User* on page 76).

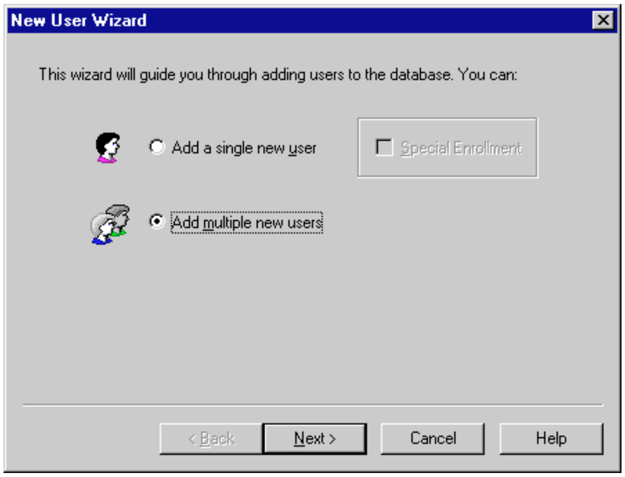
QUICK STEPS

Adding Multiple Users

1. Click the *User* menu and then click *Add New....* This takes you to the first screen of the *New User Wizard*.
2. Click *Add multiple new users*, and then click *Next*.
3. On the screen that asks for the number of users and starting ID, enter the number of users to create, and the ID number for the first new user. Click *Next* to continue.
4. On the *Security* screen, choose the access profile to assign to each of the new users. If needed, you can change the authority level and limited access. Do NOT change the user reject threshold. If you need to, you can later change this individually for a user who is having access problems. Click *Next* to continue.
5. The next screen shows the progress in adding the users. Once the process is done, click *Finish*.
6. You need to enroll the users before they have access. Typically, you will also rename the users since adding multiple users at once uses the ID number for the name.
7. If you have set up custom user entries, you will also want to edit the *Properties* for each user, click the *Custom* tab, and fill the appropriate information in there.

Beginning the Process

To begin adding a new user, pick *Add New...* from the *User* menu.



New User Wizard

This wizard will guide you through adding users to the database. You can:

○ Add a single new user

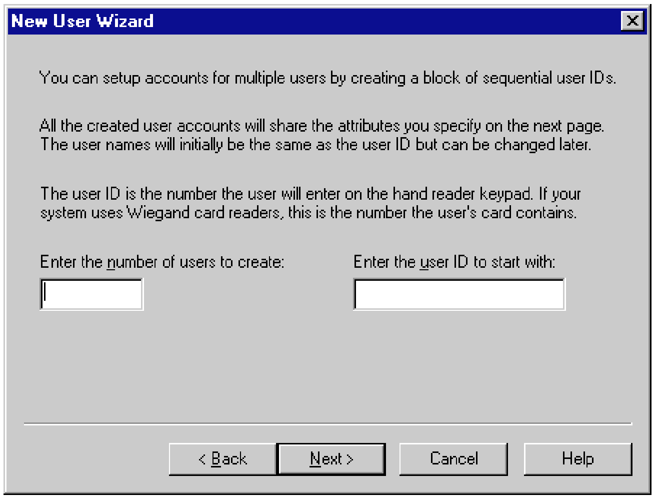
□ Special Enrollment

● Add multiple new users

Click the *Radio* button by *Add Multiple Users*, and then click the *Next* button.

Number of Users to Add and Starting ID

After you choose to add multiple users at once on the first screen of the *New User Wizard*, you see this screen.



New User Wizard

You can setup accounts for multiple users by creating a block of sequential user IDs.

All the created user accounts will share the attributes you specify on the next page. The user names will initially be the same as the user ID but can be changed later.

The user ID is the number the user will enter on the hand reader keypad. If your system uses Wiegand card readers, this is the number the user's card contains.

Enter the number of users to create:

Enter the user ID to start with:

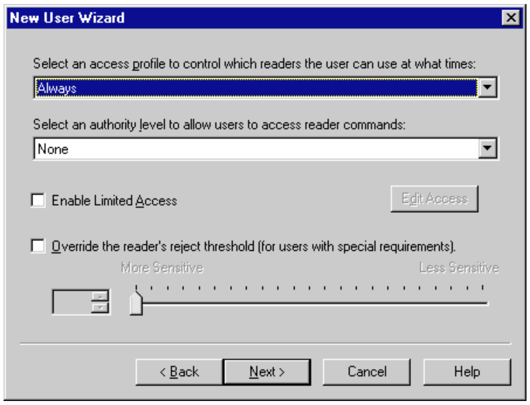
Number of users to create: Enter the number of users you want to add.

User ID to start with: Enter the starting user ID number. Use the number of digits that you would like for the final ID. For example, if you always want a five-digit ID number and you want to start with *1*, enter 00001 rather than just *1*. If you enter *00001*, HandNet will use *00002* next, then *00003*, and so on. If HandNet finds that a number is already used, if will skip that number and use the next available number. For example, if you enter *1000* as the starting number and *1000* through *1020* are all used, HandNet will automatically skip these numbers and start at *1021*. When the program adds the numbers at the end of the process, it lets you know if it had to skip any existing ID numbers.

However, do not begin an ID with zero (0) if you are going to enroll the user with the command menus on the reader. HandNet lets you enroll a user by either picking *Enroll* from the *Reader* menu, or by using the *Command* menus on the reader. If you are going to use the *Command* menus on the reader, the ID number should not begin with zero (0). While HandNet distinguishes between *5* and *0005*, the process of adding a user from the reader command menu does not. This means that if you create a user with an ID of *0005* in HandNet and try to enroll that user with the command menus on the reader, when you type *0005*, the reader thinks you are enrolling User Five, and this will not correspond with *0005* in HandNet. If you are going to use *Enroll* on the *Reader* menu, you can begin an ID with zero (if you are never going to begin an ID with zero, this might be a good choice for a duress code if you use one; see page 47 for more about duress codes).

Security Options

This screen controls what this user has access to and when.



New User Wizard

Select an access profile to control which readers the user can use at what times: Always

Select an authority level to allow users to access reader commands: None

☐ Enable Limited Access

☐ Override the reader's reject threshold (for users with special requirements).

After you click *Next* on this screen, HandNet adds the new users.

Select an access profile to control which readers the user can use at what times: Click this entry for a list of available access profiles. If these users can use all readers at all times, choose *Always*. If you do not want these users to be able to use any readers at this point, choose *Never*. For other access, select the appropriate profile. You must set access profiles up before they are available here; see page 67 for more about setting up access profiles.

Select an authority level to allow users to access reader commands: This determines what the users can do at the reader. For most users, *None* is the appropriate choice.

Each higher level gives access to the lower levels as well. For example, users with an authority level of four can also use the *Level 1, 2* and *3* menus. Except for recalibrating the reader (part of *Level 1*), and enrolling a user if you have not purchased the upgrade to the full feature set, HandNet can control every setting in the reader, so there is generally no need to control settings through the control menus in the reader.

None: This lets the reader gain access through the reader, but not use the command menus in the reader to change the reader's settings. This choice is appropriate for most users.

(1) Service: This lets you recalibrate the reader and change the reader's status display.

(2) Setup: This lets you control reader setup issues including how the reader is connected to your computer network, what language the reader displays in, the date/time, etc.

(3) Management: This lets you list users.

(4) Enrollment: This lets you add or remove users.

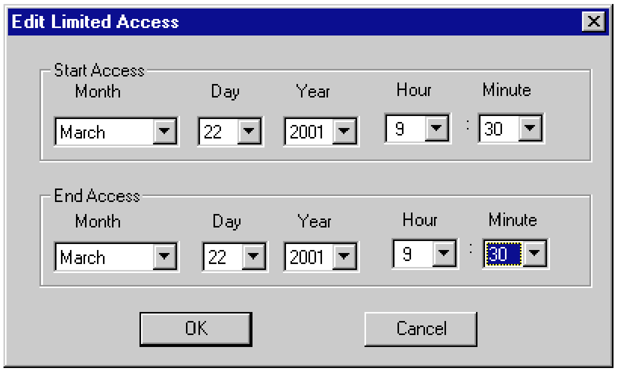
(5) Security: This lets you control the passwords for the reader menus, change time zones, enroll users who do not need hand access, etc.

See the HandKey manual for more on directly changing settings through the reader.

Limited Access

Enable limited access: This gives a user access for a specific date range. For example, suppose a contractor or temporary employee was going to be working in your building for a month. Or suppose an employee gave notice that s/he was leaving for a new job in two weeks. Once this period was over, you would not want these users to have access. Rather than having to remember to disable the user on the appropriate date, this option lets you set a start and end date/time so the user is automatically enabled and disabled at the appropriate points.

To set up start and end date/times, check the box by this button and then click the *Edit Access* button (this button only works if you have checked the box). This takes you to the *Edit Limited Access* screen:



Edit Limited Access

Start Access

Month	Day	Year	Hour		Minute
March	22	2001	9	:	30

End Access

Month	Day	Year	Hour		Minute
March	22	2001	9	:	30

To change either start or end date or time, click the corresponding entry and pick from the list that comes up.

This option is disabled if you have not purchased the license upgrade to the full feature set of Version 2.0.

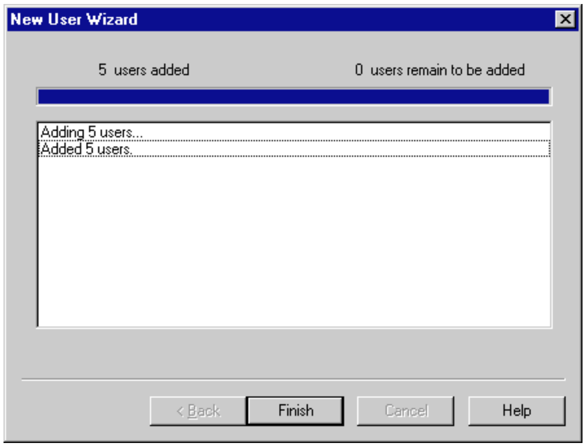
This option is NOT for limiting access to specific readers or for specific times of the day; to control that, use the *Access Profiles* entry.

Override the reader's reject threshold (for users with special requirements): Never change this option when adding multiple users at once. For users with a physical condition like arthritis that prevents them from placing their hands on the reader in exactly the same way each time, this option lets you control how exact the hand match must be for the reader to grant access. Only change this for individual users who are having trouble gaining access, never for a whole group of users at once.

If you later discover that a user is having trouble getting access consistently, go to the *Security* tab in the *User Properties* and change this entry there; see page 92. You would check this box and then slide the pointer further to the right (the *Less Sensitive* side). If a user has a really severe hand condition, it is possible to give access without hand recognition, but because this offers reduced security, that should only be a last resort; see *Adding a User Who Has Access Without Hand Recognition* on page 74 for more on this.

Progress Bar

This is the final screen in the process of adding new users. If you are adding a large number of users, it gives you an idea of how much longer the process will take.



Adding 5 users...
Added 5 users.

If HandNet tries to add ID numbers that are already used, you see messages about those numbers being skipped (this will not changed the number of new users that are added).

What to Do Next

After you click *Finish* to leave the screen above, you need to enroll the users before they have access; see page 87. You will typically also want to rename the users since this process uses the ID number for the name; page 90. And if you created custom user entries, you will want to go to the *Custom* tab in *User Properties* to fill these entries in for each user; see page 94.

* * * * *

Teaching Users How to Place Their Hands on Readers

Correct Hand Placement

Because the reader is looking at the shape of the hand, it is important that you place your hand on the reader the same way every time. When you put your hand on the reader, do this:

- If you are wearing a ring, make sure the stone is up in its normal position.
- Slide your hand forward onto the platen (moving forward like a plane would land at the airport; not straight down like a helicopter would land). Place your hand gently and comfortably; there is no need to apply pressure.
- Keep your hand flat. You should feel the platen with your palm and with the bottom of your fingers.
- Once you hand is flat on the platen, gently close your fingers so they touch against the finger pins. Again, there is no need to apply pressure or press hard. Watch the lights on the hand diagram on the top of the reader; if a light stays on, that finger is not making proper contact with the pin.

Left Hand Placement

If you have been enrolled with your left hand, follow the instructions above, but put your left hand palm up on the reader. The back of your hand should be as flat as possible against the platen.

* * * * *

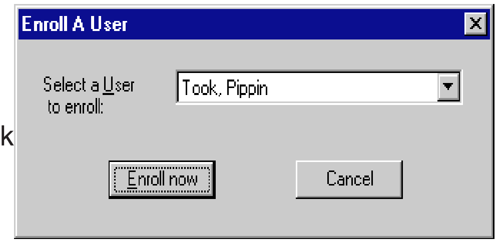
Enrolling Users

Before a user can have access, you must take the user to a reader and have the reader create an image or template of the user's hand. If you have purchased the upgrade to the full feature set, you can start this process using *Enroll* on the *Reader* menu. If you have not purchased this upgrade, you must use the reader command menus to start the enrollment process.

Using the Enroll Option on the Reader Menu

Before you enroll a user, add the user in HandNet; see page 76. You should also teach the user about correct hand placement; see page 86.

1. If the *Network* window is not open, press *CTRL-N* to open it.
2. In the *Network* window, click the reader to enroll the user at.
3. Click the *Reader* menu, and click *Enroll*. You see a screen like this:
4. If the user to enroll is not shown, click the entry and pick the user's name. Then click *Enroll now*.



Select a User to enroll: Took, Pippin

5. The reader asks the user to place and remove his/her hand three times (if it asks for the hand more than three times, the user is not placing his/her hand consistently; go over the instructions for correct hand placement).

Unless you get a message indicating that there was a problem, the user is now enrolled.

Manually Enrolling Users Using the Reader Command Menus

Before you enroll a user, add the user in HandNet; see page 76. You should also teach the user about correct hand placement on page 86.

1. Check the list of users to make sure you have an authority level of four or higher. If you have an authority level of none, one, two, or three, you cannot do this (to change your authority level, double-click your name on the list of users, click the *Security* tab, click the *Authority Level* entry, and select the appropriate level).
2. Go to the reader to be recalibrated, and enter command mode on the reader:

   If you have a HandKey II or HandKey CR reader: Press *CLEAR*, and then press *ENTER*.

   If you have an ID3D HandKey reader: Press # AND * (you can press them at the same time, or one after the other).

   The display on the reader should look like this:

```
    READY
  * :
```

3. Type your user ID number (the same one you enter to get access through the reader), and press *ENTER* or *#.* The reader asks you to place your hand. Once it recognizes your hand, this display looks like this:

```
ENTER PASSWORD
```

4. Type *4* and press *ENTER* or *#* (this is the standard password for the *Enrollment* menu in the reader; if you have changed this on the *Passwords* screen in the *Reader Properties*, enter the password you have set up).

   If you have a HandKey II or HandKey CR reader: The display should now look like this:

```
     ADD USER
  *  NO     YES #
```

   If you have an ID3D HandKey reader: The display should now look like this:

```
   ENROLL USER
  *  NO     YES #
```

   If the reader shows the *READY* screen again instead of this screen, then either you placed your hand improperly or you do not have the rights to do this; carefully check step one again.

5. Press the *YES / #* button. This display should now look like this:

```
  ID?
  :
```

6. Type the ID number of the user to enroll and press *ENTER* or *YES / #*. The display should now look like this:

```
** PLACE HAND **
     1/3
```

7. Have the user place his/her hand on the reader. The reader will ask the user to remove the hand and place it again. The reader should ask the user to place his/her hand three times; if it asks for the hand more than three times, the user is not placing his/her hand consistently; go over the instructions for correct hand placement.

   Once the user has correctly placed the hand three times, the reader asks for the time zone:

```
ENTER TIME ZONE
     (0)?:
```

8. When the user has access to this and other readers is controlled by the access profile you have assigned in the user's properties, so just press *ENTER* or *YES / #.*

9. The reader briefly flashes the message *User Enrolled* and then returns you to the *Add User* or *Enroll User* display. Enroll another user if needed, or press the *CLEAR* button to leave the *Enrollment* menu and return to the reader to its normal display.

* * * * *

Changing Users

Overview

QUICK STEPS

Changing Users

1. If the user window is not shown, press *CTRL-U* or pick *Users* from the *View* menu.
2. Double-click the user to change information. This takes you to the *General* tab in the *User Properties* (you can also click the user once and then pick *Properties* from the *User* menu).
3. Click the tab that has the information you want to change:
   To change the user's name or ID: this is on the *General* tab.
   To change the users access level, authority, limited access, or the reader's sensitivity: Click the *Security* tab.
   To change Custom entries: Click the *Custom* tab.
4. Change information as needed ant then click *OK*.

Renaming Users

1. If the user window is not shown, press *CTRL-U* or pick *Users* from the *View* menu.

2. Double-click the user to rename. This takes you to *User Properties*.

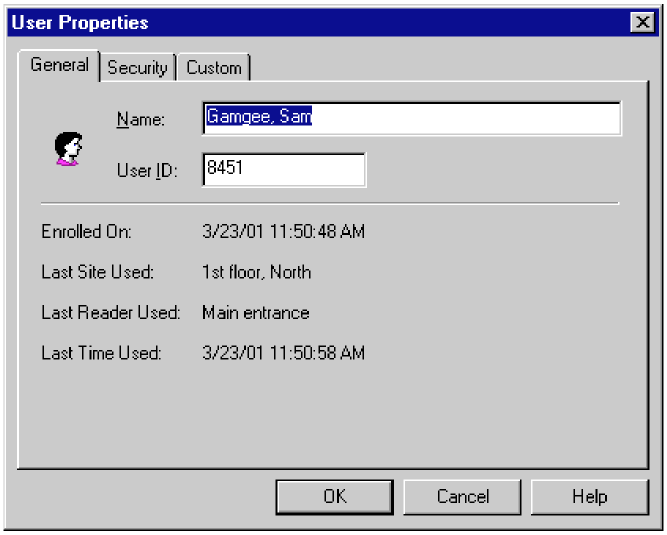
3. Type the new name, and then press *ENTER* or click *OK*.

Alternate Methods

Right-click the user's name and pick *Rename* from the menu that pops up; click the user once and pick *Rename* from the *View* menu; or click the user once, pause for long enough so the computer will not think you are double-clicking, and then click directly on the user's name.

User Properties, General

The *General* tab in *User Properties* lets you change the user's name or ID. It also shows when the user last accessed a reader.



User Properties

Name: Gamgee, Sam

User ID: 8451

Enrolled On: 3/23/01 11:50:48 AM

Last Site Used: 1st floor, North

Last Reader Used: Main entrance

Last Time Used: 3/23/01 11:50:58 AM

Name: Enter the user's name.

If you want to sort the list of users by last name: Enter the last name first. For example, if the user's name is Sam Gamgee, you would enter *Gamgee, Sam*.

If you have two users with the same name: You must enter a unique name for each user. If two users have the same name, you might add a middle initial, or you might add a job description after each. For example, if you have two users named John Jones, you might enter something like *Jones, John (engineer)* and *Jones, John (maintenance)*.

ID Number: If you change a user's ID, be sure to let the user know. The user will not be able to gain access through any reader without knowing the correct ID.

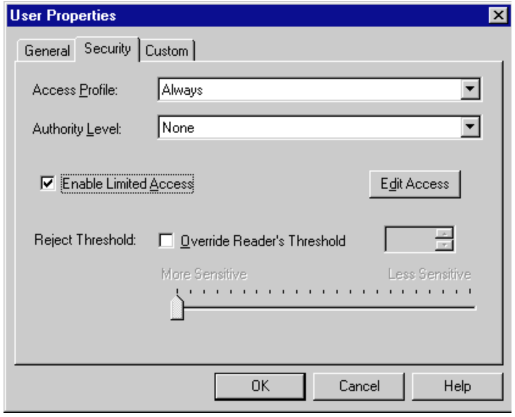
Each number must be unique (if you could give the same number to two users, the reader would not know which was trying to gain access). Longer numbers are slightly more secure, but four or five digits are generally adequate in context where user's must enter the number. You may enter up to ten digits if you do not use a duress code, or up to nine digits if you do use a duress code. If you use a duress code, make sure that you do not create an ID that begins with that digit; see page 47 for more about duress codes. If you have set up an *ID length* on the *Settings* tab in the *Reader Properties*, make sure that you do not create an ID that is longer than this; see page 47 for more about ID length.

If you use Wiegand card readers: Enter the ID number stored on the card.

Do not begin an ID with zero (0) if you are going to enroll the user with the command menus on the reader: HandNet lets you enroll a user by either picking *Enroll* from the *Reader* menu, or by using the command menus on the reader. If you are going to use the command menus on the reader, the ID number should not begin with zero (0). While HandNet distinguishes between 5 and 0005, the process of adding a user from the reader does not. This means that if you create a user with an ID of 0005 in HandNet and try to enroll that user with the command menus on the reader, when you type 0005, the reader thinks you are enrolling user 5; this will not correspond with 0005 in HandNet. If you are going to use *Enroll* on the *Reader* menu, you can begin an ID with zero (if you are never going to begin an ID with zero, this might be a good choice for a duress code if you use one).

User Properties, Security

The *Security* tab controls what this user has access to and when.



Access Profile: Always

Authority Level: None

☑ Enable Limited Access

Reject Threshold: □ Override Reader's Threshold

Select an access profile to control which readers the user can use at what times: Click this entry for a list of available access profiles. If this user can use all readers at all times, choose *Always*. If you do not want the user to be able to use any readers at this point, choose *Never*. For other access, select the appropriate profile. You must set access profiles up before they are available here.

Select an authority level to allow users to access reader commands: This determines what the user can do at the reader. For most users, *None* is the appropriate choice.

Each higher level gives access to the lower levels as well. For example, a user with an authority level of four can also use the *Level one, two* and *three* menus. Except for recalibrating the reader (part of level 1), and enrolling a user if you have not purchased the upgrade to the full feature set, HandNet can control every setting in the reader, so there is generally no need to control settings through the reader menus.

None: This lets the reader gain access through the reader, but not use the command menus in the reader to change the reader's settings. This choice is appropriate for most users.

(1) Service: This lets you recalibrate the reader and change the reader's status display.

(2) Setup: This lets you control reader setup issues including how the reader is connected to your computer network, what language the reader displays in, the date/time, etc.

(3) Management: This lets you list users.

(4) Enrollment: This lets you add or remove users.

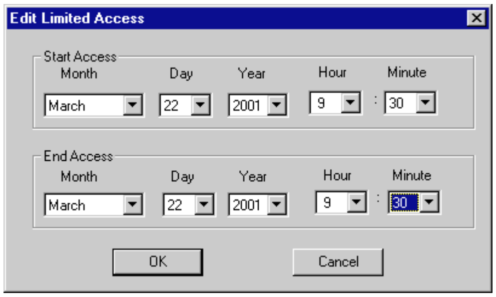
(5) Security: This lets you control the passwords for the reader menus, change time zones, enroll users who do not need hand access, etc.

See the HandKey manual for more on directly changing settings through the reader.

Limited Access

Enable limited access: This gives a user access for a specific date range. For example, suppose a contractor or temporary employee is going to be working in your building for a month. Or suppose an employee gives notice that s/he is leaving for a new job in two weeks. Once this period is over, you would not want these users to have access. Rather than having to remember to disable the user on the appropriate date, this option lets you set a start and end date/time so the user is automatically enabled and disabled at the appropriate points.

To set up start and end date/times, check the box by this button and then click the *Edit Access* button (this button only works if you have checked the box). This takes you to the *Edit Limited Access* screen:



Edit Limited Access

Start Access

Month	Day	Year	Hour	Minute
March	22	2001	9	30

End Access

Month	Day	Year	Hour	Minute
March	22	2001	9	30

To change either start or end date or time, click the corresponding entry and pick from the list that comes up.

This option is disabled if you have not purchased the license upgrade to the full feature set of Version 2.0.

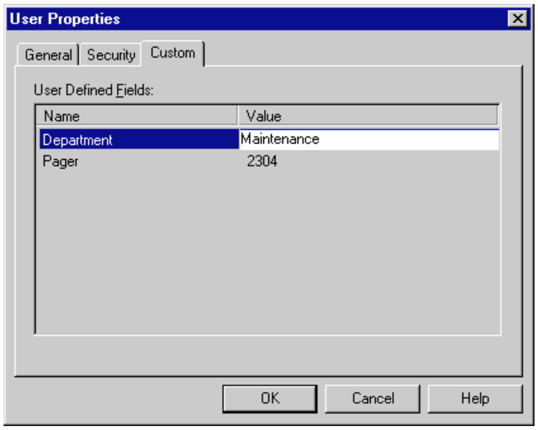
This option is NOT for limiting access to specific readers or for specific times of the day. To control that, use the *Access Profiles* entry.

Override the reader's reject threshold (for users with special requirements): For users with a physical condition like arthritis that prevents them from placing their hands on the reader in exactly the same way each time, this option lets you control how exact the hand match must be for the reader to grant access.

If a user is having trouble getting access consistently, check this box and then slide the pointer further to the right (the *Less Sensitive* side). If a user has a really severe hand condition, it is possible to give access without hand recognition, but because this offers reduced security, that should only be a last resort.

User Properties, Custom

You only see entries on the *Custom* tab if you have set up custom user entries (see page 97 for more on creating custom user entries). The entries on this screen vary depending on what you have set up; the entries on your screen will probably be completely different from the examples show below.



User Defined Fields:

Name	Value
Department	Maintenance
Pager	2304

To change a value, click the item in the *Value* column and then enter the correct value.

When You Are Done

When you are done changing *User Properties*, click the *OK* button at the bottom of the screen.

* * * * *

Changing Access for Many Users at Once

Import TZ Option

Import TZ on the *File* menu lets you change the access profile to *Always* or *Never* for many users based on information in a text file (this file would be created with some other program).

Caution

If you use this option, be aware that there are security risks involved: if you mistype a number in the file, you could easily give full access to a different user than you intended. And unlike most other changes in HandNet, the fact that this option is used and the fact that a user's access is changed is NOT reflected in the activity log, so you will not have any record of the change. In most contexts, it is more appropriate to change user access through the *Security* tab in *User Properties*; see page 92.

File Format

Each line of the file would list a user ID number followed by a comma, and then either 0 (zero) to set that user's access profile to *Always*, or sixty-one, to set that user's profile to *Never* (currently, you cannot use the file to switch to any other profile). For example, suppose your text file looked like this:

```
1001, 0
1002, 0
1003, 61
21345, 0
43567, 61
```

If you import this file, HandNet would set the access profile to *Always* for users with the IDs of 1001, 1002, and 21345, and it would set the profile to *Never* for users with IDs 1003 and 43567. It would not change the access profiles for any other users. If HandNet could not find a user with the corresponding ID number, or if you have something other than zero or sixty-one after the comma, HandNet would skip that line. It would not give you any message or tell you the line was skipped. If you have any lines that did not match the format above (for example, if you do not have the comma between the ID and the zero or sixty-one), HandNet would give a message at the end of the process that tells you how many bad records are ignored. If other lines are in the correct format, HandNet would still process them successfully.

You do not see any message or progress bar during the import process. If you are importing many records, you could have some delay where it looks like nothing is happening. For example, on a 166MHz processor, importing 1,000 records takes slightly over thirty seconds; you would not see any activity while this is happening.

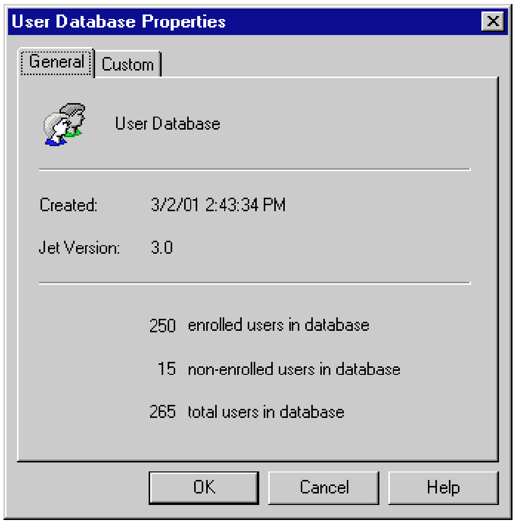
* * * * *

User Database Properties

What Information Is Shown

This screen shows general information about the whole user database, including the date it is created, the Version number, the number of enrolled users and number of non-enrolled users, and the total number of users in the database. You do not typically need this information during normal use of the program. However, if you want to add or change custom user entries, you would come to this screen and then click the *Custom* tab.

You get to this screen by picking *DB Properties* from the *User* menu.



Created: 3/2/01 2:43:34 PM

Jet Version: 3.0

250 enrolled users in database

15 non-enrolled users in database

265 total users in database

* * * * *

Adding Custom User Entries

To collect additional information about users in HandNet, you can add additional custom entries. HandNet then asks for this information on the *Custom* screen of *New User Wizard* (see page 80) and the *Custom* tab in the *User Properties* (page 94).

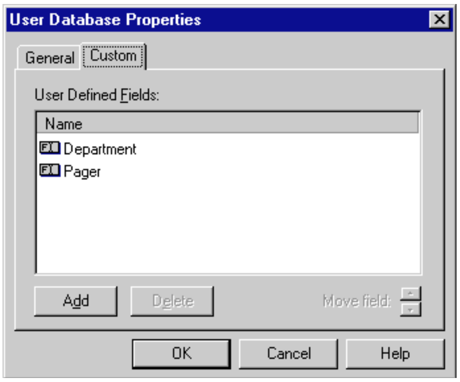
What you might want to collect could vary widely depending on how you are using HandNet: emergency phone numbers, employment start dates, department, pager number. You can add as many entries as you need.

The information that you add in custom entries is only available on the screen, either in *User Properties* or on the list of users (available by picking *Users* from the *View* menu). Currently, HandNet does not include custom user information on any reports.

Getting to the List of Custom Entries

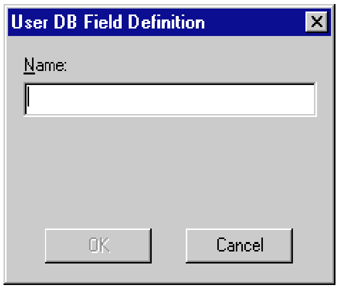
1. Click the *User* menu and then click *DB Properties*.

2. Click the *Custom* tab. You will see a screen like this, but with different entries.



Adding a New Entry

To add a new custom entry, click the *Add* button. You see this screen:



Type the name of the field or entry to add and press *ENTER* or click *OK*. Make sure that you enter the name of the entry correctly; once you continue, you cannot change the name.

Deleting a Custom Entry

Click the entry in the list and click *Delete*. Be sure that you are deleting the correct item; the program will not ask you to confirm the deletion, and once you delete a custom entry, all information that you have entered for users in that entry is gone. For example, suppose you create an *Emergency Phone Number* entry and entered phone numbers for all of your users. If you delete emergency phone numbers here, all of the phone numbers that you enter would be gone and there would be no way to get them back unless you make a backup of your HandNet information.

Changing the Order of the Entries

On the *Custom* screen in the *User Properties*, the entries in the same order as they are listed here. To change the order of the entries, click the entry to move and then click the up or down arrows next to the words *Move field*.

* * * * *

Converting Users from MS-DOS HandNet or HandNet+

If you have been using one of our MS-DOS programs (either HandNet or HandNet+), *Convert HandNet+...* on the *File* menu lets you import your users so you do not have to enter and enroll them again. This option brings in each user's name, ID number, authority level, and reject threshold.

If you have been using an older Version of HandNet for Windows, you do not need to do anything to convert that information.

To Convert HandNet Plus Users

1. If you have been using HandNet rather than HandNet Plus, follow the steps below to convert your user information from HandNet to HandNet Plus format.
2. Pick *Convert HandNet+* from the *File* menu.
3. If you have installed HandNet+ somewhere other than in C:\HNET, click the *Browse* button and go to the directory where HandNet+ is installed. Then click the *Open* button.
4. Click the *Convert* button. The HandNet+ database is converted to HandNet for Windows™ format.
5. This con Version does not bring in the access profiles for the users, so when this is done you must assign an access profile to each user on the *Security* tab in *User Properties*.

To Convert MS-DOS HandNet Users

If your DOS Version of HandNet is in the standard /HNETdirectory: Press *F1* while in HandNet to pop up the help. In the index, type *convert* and open the topic on converting HandNet+ information. In this topic there is a button that automatically does this process for you.

If your DOS Version of HandNet is NOT in the standard /HNET directory:

1. Copy the *convert.exe* file from the HandNet for Windows directory to the directory the MS-DOS Version of HandNet is located. The standard location for HandNet for Windows is *C:\Program Files\Schlage Biometrics, Inc.\HandNet for Windows.* For example, to copy the convert file from this directory to *c:\hnet*, you would type:

```
copy c:\progra~1\recogn~1\handne~1\convert.exe c:\hnet\
```

2. Switch to the directory the MS-DOS Version of HandNet is in. For example, to switch to the *\hnet* directory, you would type *cd\hnet* and press *ENTER*.
3. Make a backup copy of the file that contains your user information. This file is called *id_dbase.dat*. For example, you might type:

```
copy id_dbase.dat id_dabase.bak
```

4. Type *convert* and press *ENTER*. This should convert the information to HandNet Plus format. Once you have done this, you are ready to import the information into HandNet for Windows using the steps described above.

* * * * *

Importing and Exporting Users

Getting User Information from a Reader

If you have already set up users in a reader that you are connecting to HandNet, you do not need to recreate those users. You can get user information from the reader by doing this:

1. Pick *Network* from the *View* menu (or type *CTRL-N*).
2. On the list of readers in the right pane of the *Network* window, select the reader(s) to get user information from.
3. Click the *Reader* menu, click *Upload*, and click *Users*.
4. The program asks you to confirm that you want to upload users from the reader; click *Yes* to continue.

Importing Users from Another Copy of HandNet

You only need to import users if you have readers connected to several different computers (each with its own copy of HandNet) and if users added to one system need to be available on the others. If all of your readers are connected to a single copy of HandNet, you do not need this feature.

The export feature is only available if you have purchased the upgrade to the full feature set of Version 2.0.

Setting Up Import Settings First

Make sure that you select the correct choices for what to import on the *User Import/Export* tab in *System Settings* before you try to import; see page 28. When HandNet imports, it empties the *Import* file, discarding those user records that do not meet the conditions you have checked there.

Importing Users From Another Computer

1. On the computer where you exported users, go to the HandNet directory and copy the file *export.mdb* to a floppy disk (you could also copy this file to a network drive, attach it to an e-mail, etc.).
2. Rename the file on the disk (or in the new location) to *import.mdb*.
3. Put this *import.mdb* file into the HandNet directory on the computer where you want to import users.
4. If you do not have that copy of HandNet set up to import automatically, pick *Import Users* from the *File* menu (if you have the *Enable* box under *Auto Import* checked on the *User Import/Export* tab in *System Settings*, HandNet starts importing as soon as it finds the *import.mdb* file in the directory; see page 28).

The activity window lists each user that is added, deleted or changed.

Exporting Users to Another Copy of HandNet

You only need to export users if you have readers connected to several different computers (each with its own copy of HandNet) and if users added to one system need to be available on the others. If all of your readers are connected to a single copy of HandNet, you do not need this feature.

The export feature is only available if you have purchased the upgrade to the full feature set of Version 2.0.

Automatically Exporting Users

HandNet can automatically export users when you create, enroll, change or delete users. When HandNet exports users is controlled by the items in the *Export* column on the *User Import/Export* tab in *System Settings*; see page 28.

Manually Exporting Users

1. Go to the *Users* window.
2. Select the users to export. To select multiple users that are together on the list, click the first user, hold the *SHIFT* key down, and click the last user that you want to select. To select multiple users that are not together on the list, click the first user to select, hold the *CTRL* key down, and click each other user that you want to select.
3. Right-click (this brings up a menu).
4. On the menu, point to *Export*, and then pick *Selected* (or pick *All* to export every user in the list whether selected or not).

You will see a message with a progress bar that indicates that the users are being exported (if you only selected a few users, this may vanish almost instantly). Once this box disappears, the export process is done.

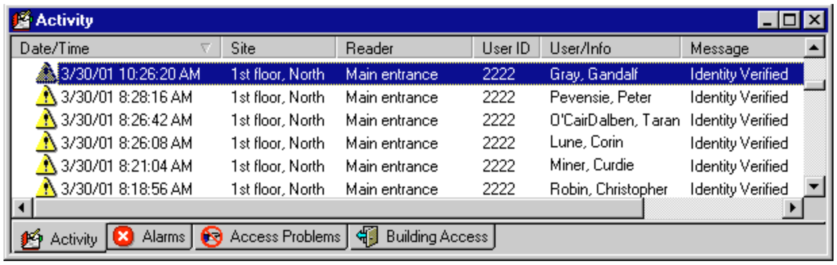
To import these users on the other computer, see the instructions for *Importing Users from Another Copy of HandNet* on page 99.

* * * * *

Monitoring Ongoing Activity

Activity Window

The *Activity* window lists everything that happens at any reader connected to HandNet, and any change made in the HandNet program. To open this window, pick *Activity* from the *View* menu, or press *CTRL-A*.



Date/Time	Site	Reader	User ID	User/Info	Message
3/30/01 10:26:20 AM	1st floor, North	Main entrance	2222	Gray, Gandalf	Identity Verified
3/30/01 8:28:16 AM	1st floor, North	Main entrance	2222	Pevensie, Peter	Identity Verified
3/30/01 8:26:42 AM	1st floor, North	Main entrance	2222	O'CairDalben, Taran	Identity Verified
3/30/01 8:26:08 AM	1st floor, North	Main entrance	2222	Lune, Corin	Identity Verified
3/30/01 8:21:04 AM	1st floor, North	Main entrance	2222	Miner, Curdie	Identity Verified
3/30/01 8:18:56 AM	1st floor, North	Main entrance	2222	Robin, Christopher	Identity Verified

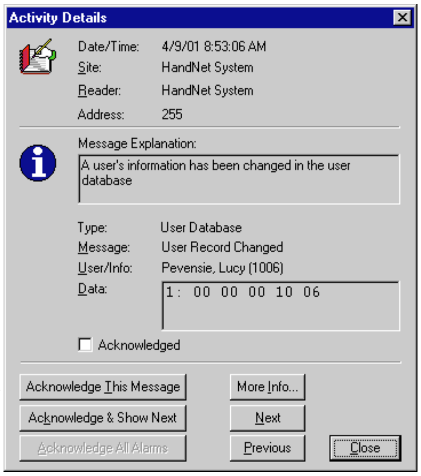
Only the first two tabs at the bottom of this screen (*Activity* and *Alarms*) are always there. The others are merely examples of custom activity views that you can create as needed; see *Creating Custom Activity Views* on page 104.

Rearranging or Resizing Columns in the Activity Window

To move any column, click on the column heading and hold the mouse down. With the mouse held down, drag the column heading to the left or right.

Getting More Detail about an Activity in the Activity Window

When you double-click on an activity in the *Activity* window, you get a screen like this that tells more about that activity.



Date/Time: 4/9/01 8:53:06 AM
Site: HandNet System
Reader: HandNet System
Address: 255

Message Explanation:
A user's information has been changed in the user database

Type: User Database
Message: User Record Changed
User/Info: Pevensie, Lucy (1006)
Data: 1: 00 00 00 10 06

□ Acknowledged

Date/Time: This shows the date and time when the activity occurred. The date is listed in month/day/ year order, and the time lists hours/minutes/seconds.

Site: If this activity happened at a reader, this shows the name of the site the reader is associated with.

Reader: If this activity happened at a reader, this shows the reader's name.

Address: If this activity happened at a reader, this shows the reader's address; this address should correspond with the name of the reader listed above. If this activity occurred in the HandNet program, this says *255*.

Message Explanation: This shows some additional explanation of the message. For more explanation, see the complete list of activity messages starting on *Activity Messages* on page 116.

Type: Each message falls into one of ten categories. When you are creating an activity filter or custom activity report, you can limit your report or activity view to specific types of messages; see *Message Types* on page 111 for more detail.

Message: This shows the same message that you saw on the list in the *Activity* window.

User/Info: If this message is associated with a particular user, this shows the user's name and ID number.

Data: This shows technical detail about the message that is not relevant to your use of the program. This is occasionally useful to support in debugging a problem.

Acknowledged [checkbox]: This shows whether this message has been acknowledged yet. You cannot uncheck this box once it is marked. You also can check the box directly; you must use one of the three *Acknowledge...* buttons below.

Buttons on the Activity Details Screen

Acknowledge This Message: This marks the message as acknowledged. After the message on the activity or alarm list, you will see *:ACK* followed by the name of the operator who acknowledged the message and the date/time when it was acknowledged. If this is an alarm, this also shuts the alarm off.

Acknowledge & Show Next: This acknowledges the current message and shows the next message. By next, we mean more recent in time; that is, the message above the current message on the activity list.

Acknowledge All Alarms: This button is disabled unless there is an alarm that has not been acknowledged yet. You might use this button if you see several related alarms on the list and you want to acknowledge them all at once.

More Info: This brings up the online help.

Next: This shows the message that occurred more recently in time, that is, the message directly before this on the activity list.

Previous: This shows the message that occurred before this message in time, that is, the message directly after it on the activity list.

* * * * *

Getting to and Acknowledging Alarms

Getting to the Alarms List

Alarms are listed with the rest of the activity in the *Activity* window, but we have also provided a separate view with just the alarms. To see this view, click the *Alarms* tab at the bottom of the *Activity* window.

Acknowledging an Alarm

If an alarm is triggered in HandNet, do this to acknowledge it and turn it off.

1. If the *Activity* window is not shown, press *CTRL-A* or pick *Activity* from the *View* menu.

2. Double-click the alarm message with the bell icon next to it (you can see it both in the regular activity view or by clicking the *Alarm* tab at the bottom of the window).

3. Click one of the *Acknowledge...* buttons at the bottom left of the window (you cannot just click the checkbox by the word acknowledged; you must click one of the buttons). After the message on the *Activity* or *Alarm* list, you will now see *:ACK* followed by the name of the operator who acknowledged the message and the date/time it was acknowledged.

4. Take whatever action is appropriate in response to the alarm.

What Situations Cause Alarms

Which situations trigger alarms depends on which items are checked on the *Alarms* tab in the *System Settings*; see page 25.

* * * * *

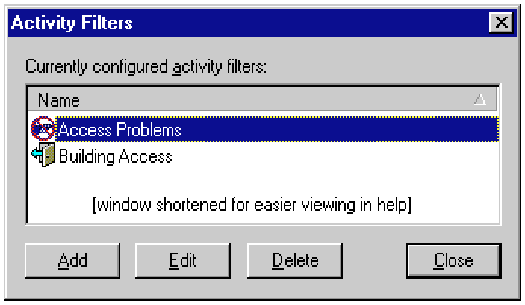
Creating and Printing Custom Activity Views

Creating a Custom Activity View

The main *Activity* window lists all activity that occurs: every access from every reader, every failed access, every user addition and enrollment, every alarm, and so on. Sometimes its useful to see less than this. For example, if you wanted to identify users who were having access problems, you might want to see only the *Identity Unknown* and *Access Denied* messages (the messages that can occur when someone enters a valid ID but then does not get a match on the hand). Or if you want to identify who has come in the building, you might want to see only *Identity Verified* messages and only for the readers that controlled entrances to the building.

You can create (and print reports on) custom views for these or any other subsets of activity, limiting the view to specific messages, dates, times, users, and/or readers. To create a custom activity view:

1. Click the *View* menu, and click *Activity Filter*. You see a list of any custom activity views if you have created any yet. This list looks like this, but the *filters* listed will be different.

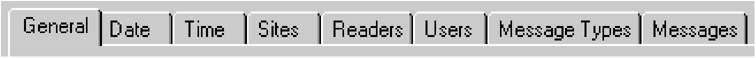


Access Problems
Building Access

[window shortened for easier viewing in help]

2. Click the *Add* button to create a new filter (that is, a set of conditions that will filter out only the information you want to see). This takes you to the first *Activity Filter* screen (to change a filter you have already created, click the filter and then click *Edit*).

3. Give the filter a name, associate an icon if you wish, and then go to each tab where you want to include something less than all of the activity.



   Each tab is initially set up to include all information; go to those where you want to limit or filter out particular information. For example, if you only want activity at certain readers, you would go to the *Readers* tab. If you only want certain messages, go to the *Messages* tab. The options on these tabs are explained, starting on page 107.

4. When you have entered all of the conditions needed, click the *OK* button at the bottom of the window.

To start this process, you could also right click on the bar at the bottom of the *Activity* window, and then pick *Add New Filter...*.

Removing a Custom Activity View

This does not remove any activity from HandNet; it only removes the custom view of the activity.

1. Click the *View* menu, and click *Activity Filter*. You will see a list of any custom activity views you have created.

2. Click the view or filter to remove and click *Delete*.

Printing an Activity Report Based on an Activity Window

1. Right-click on the bottom bar of the *Activity* window (where the *Activity* and *Alarms* tabs are).

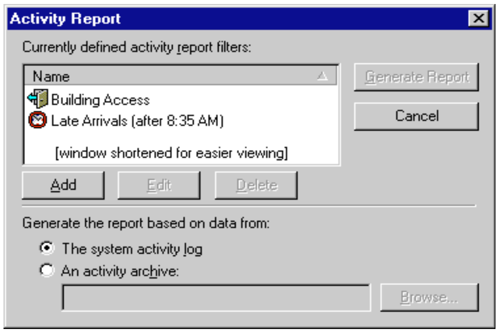
2. Pick *Generate Report*.

3. In the report window that comes up, click the printer icon in the header; see *Printing or Viewing Reports* on page 127 for more detail.

Creating a Custom Activity Report from the Reports Menu

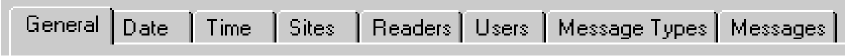
If you have not already created a custom activity view, or if you need to run the report on archived activity, then follow these steps to design the report.

1. From the *Main Menu* bar, click *File*, click *Reports*, and click *Activity....* You see a screen like this (if you created any custom reports they would be listed; your reports may be very different from the samples listed here).


Activity Report
Currently defined activity report filters:
Name
Building Access
Late Arrivals (after 8:35 AM)
[window shortened for easier viewing]
Generate Report
Cancel
Add
Edit
Delete
Generate the report based on data from:
● The system activity log
○ An activity archive:
Browse...

2. Click the *Add* button to create a report (that is, a set of conditions that will filter out only the information you want to see). This takes you to the first *Activity Report* screen (to change a report you have already created, click the filter and then click *Edit*). The screens that you see are identical to those that you see when creating a custom activity view.

3. Give the report a name, associate an icon if you wish, and then go to each tab where you want to include something less than all of the activity.

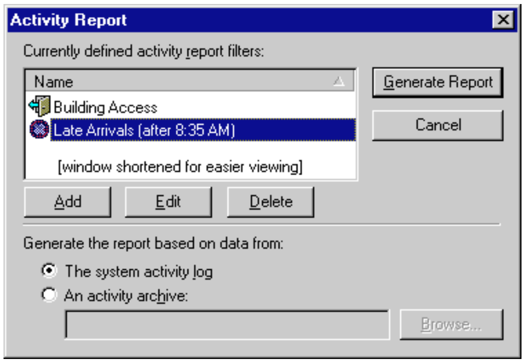


Each tab is initially set up to include all information; go to those where you want to limit or filter out particular information. For example, if you only wanted activity at certain readers, you would go to the *Readers* tab. If you only want certain messages, go to the *Messages* tab. The options on these tabs are explained starting on page 107.

4. When you have entered all of the conditions needed, click the *OK* button at the bottom of the window. This returns you to the list of reports.

Printing an Activity Report from the Reports Menu

1. From the main menu, click *File*, click *Reports*, and then click *Activity Reports*. You see a screen like this (if you have created any custom reports they would be listed; your reports may be very different from the samples listed here).


Activity Report
Currently defined activity report filters:
Name
Building Access
Late Arrivals (after 8:35 AM)
[window shortened for easier viewing]
Generate Report
Cancel
Add
Edit
Delete
Generate the report based on data from:
● The system activity log
○ An activity archive:
Browse...

2. If you have not already designed the report, see *Creating a Custom Activity Report* from the *Reports* Menu above for help designing it.

3. Click the report in the list of reports at the top of the window.

4. At the bottom of the window, indicate which activity to generate the report from:

   The system activity log: This includes all the activity that has occurred since the last time you archived activity (and that meets your report conditions).

   An activity archive: This includes all activity that meets your report conditions that is in the archive file that you pick. Click the *Radio* button by this choice, click the *Browse* button, and pick the file. HandNet lists files that have an *.hna* extension. Pick the *Archive* file and click *OK*.

   If the activity that you want is in several archive files, you will have to run the report several times, once for each archive file. If you need the information in a single report, you can export each report to a file and then use another program to combine the reports into a single file.

5. Click the *Generate Report* button. HandNet generates the report and shows it in a new window on the screen.

6. Click the *Printer* icon near the middle of the header to print the report, or click the icon with the envelope to export the content of the report to a file. You can export to a variety of formats including Word, Excel, Lotus 1-2-3, .rtf, text, and others; see *Printing or Viewing Reports* on page 127 for more detail.

   If the printer icon is disabled and grayed-out, you do not have a printer set up yet on this computer (to set up a printer, go to the Windows *Start* menu, highlight *Settings*, pick *Printers*, and click *Add Printer*).

7. To close the *Report* window when done, click the *X* in the upper-right corner of the window.

* * * * *

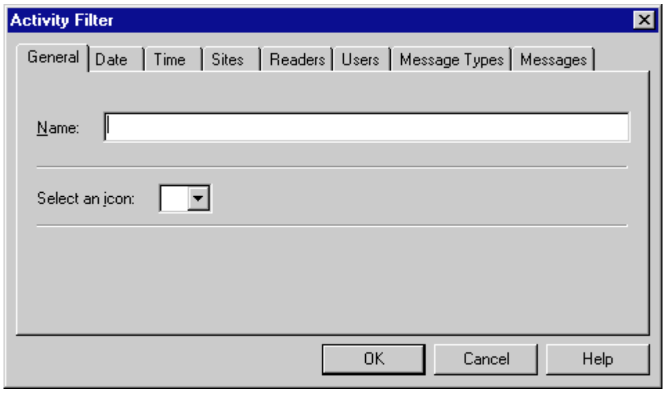
Condition Screens for Creating Custom Activity Views/Reports

When you create an activity filter (that is, a custom view of your activity; see page 104), or when you design a custom activity report (see page 105), you see the screen shown below.

Each tab is initially set up to include all information; you only need to go to those tabs where you want to limit or filter out particular information. For example, if you only want activity at certain readers, you would go to the *Readers* tab. If you only want certain messages, you would go to the *Messages* tab.

General

This screen contains the name and icon associated with activity filter or report.



Name:

Select an icon:

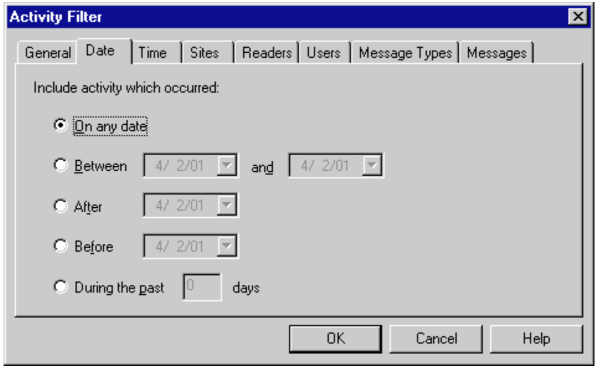
Name: Enter a name that describes the conditions that determine what activity will be included.

Icon: If you want an icon associated with the this activity view/report, click the this entry. You do not have to choose an icon if you do not want to. If you do not want an icon, do not pick an icon; once you pick one, you cannot go back to having no icon.

Do not click *OK* until you have gone to the other tabs and set up those conditions that limit the activity.

Date

This screen lets you limit the activity you see to certain dates.



Include activity which occurred:

● On any date

○ Between 4/ 2/01 and 4/ 2/01

○ After 4/ 2/01

○ Before 4/ 2/01

○ During the past 0 days

On any date: This includes activity from any date that is in the activity file. This is always the initial choice when you create a new report or activity filter.

Between: This includes any activity between the dates entered or on those dates. For example, if you chose *Between 05/01/01 and 05/31/01*, activity from both 05/01 and 05/31 would be included along with the activity in between.

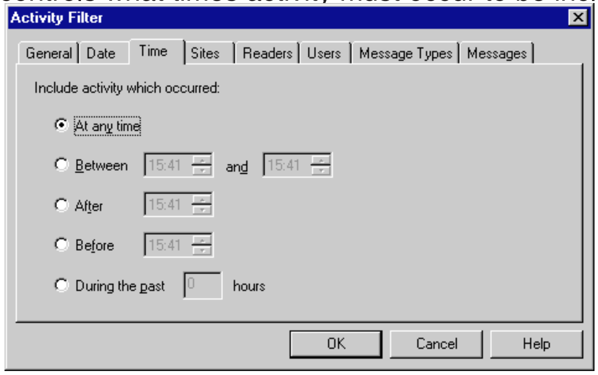
After: This includes activity that is after the date that you enter, but not activity that is on or before that date. For example, if you enter *05/01/01*, you would see activity from 05/02 on, but activity on 05/01 would not be included (if you want the activity from 05/01, you would have to enter *After 04/30*).

Before: This includes activity that is before the date that you enter, but not activity that is on or after that date. For example, if you enter *04/30/01*, you would see activity from 04/29 and before, but activity from 04/30 would not be included (if you want the activity from 04/30, you would have to enter *Before 05/01*).

During the past: This is useful for creating a view that lists only the most recent activity. For example, you might create a view that only listed activity during the past week. If you want to be more precise, this same option is on the *Time* screen so that you could, for example, limit a view to the last twenty-four hours.

Time

This screen controls what times activity must occur to be included.



Include activity which occurred:

● At any time

○ Between 15:41 and 15:41

○ After 15:41

○ Before 15:41

○ During the past 0 hours

On any time: This includes activity from any time. This is always the initial choice when you create a new report or activity filter.

Between: This includes any activity between the times entered or exactly at those times. For example, if you chose *Between 12:00 and 13:00*, activity that happened at exactly 12:00 or 1:00, PM along with the activity in between would be included. This goes from the earliest time to the latest time, regardless of which you enter first. For example, if you enter *Between 17:00 and 8:00* (hoping to get activity that was not during normal business hours), you would get the same activity as if you had entered *Between 8:00 and 17:00* (that is, activity that occurred during normal business hours). If you really want activity that is after 5:00 PM and before 8:00 AM, you would have to create two filters: one looking for activity after 17:00 and the other looking for activity before 8:00.

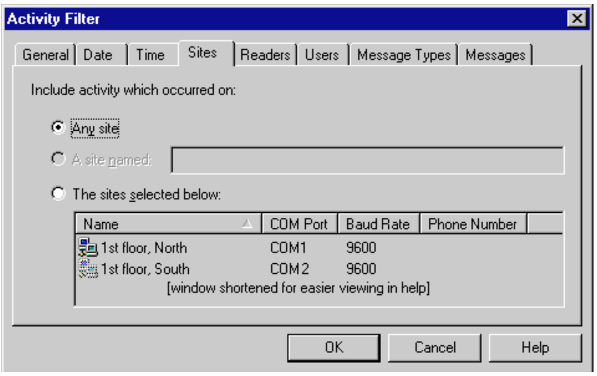
After: This includes activity that is after the time that you enter, but not activity that is exactly at that time. For example, if you enter 12:00, you would see activity from 12:00:01 (that is one second after 12) on, but activity at 12:00:00 or before would not be included.

Before: This includes activity that is before the time that you enter, but not activity that is exactly at that time. For example, if you enter 12:00, you would see activity from 11:59:59 (that is one second before 12:00) on, but activity at 12:00:00 or after would not be included.

During the past: This is useful for creating a view that lists only the most recent activity. For example, you might create a view that only listed activity during the past twenty-four or forty-eight hours (for longer periods, this same option is on the *Date* screen so that you could, for example, limit a view to the past thirty days).

Sites

This screen lets you limit the activity to certain sites.



Include activity which occurred on:

● Any site

○ A site named:

○ The sites selected below:

Name	COM Port	Baud Rate	Phone Number
1st floor, North	COM1	9600	
1st floor, South	COM2	9600	

[window shortened for easier viewing in help]

Any site: Leave this selected to not limit the activity based on site.

A site named: This option is permanently disabled. To get activity for a single site, use the following option and only click one site in the list.

The sites selected below: To limit the report/view to specific sites, click this and then select the sites to include activity from.

To select a single site: Click that site in the list.

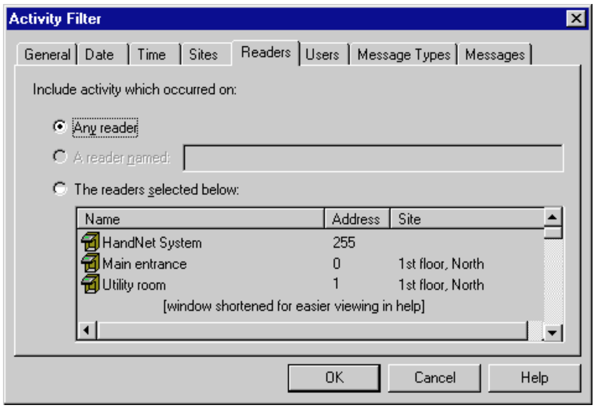
To select multiple sites that are together on the list: Click the first site in the group, hold the *SHIFT* key down, and with the *SHIFT* key down, click the last site that you want to select.

To select multiple sites that are not together on the list: Click the first site to select, hold the *CTRL* key down, and click each other site that you want to select.

If you select specific sites here, make sure you do not select readers from different sites on the *Reader* tab; if you select sites here and select readers from different sites, you will not see any activity with this filter. If you want to select specific readers, select *Any site* on this screen.

Readers

This tab lets you limit to activity that occurred at certain readers. For example, you might want to limit activity only to the readers controlling the entrances to the building so you could see who has come in. Or you might want to limit activity to the readers controlling the most secure areas so you could monitor them more closely.



Include activity which occurred on:

● Any reader

○ A reader named:

○ The readers selected below:

Name	Address	Site
HandNet System	255	
Main entrance	0	1st floor, North
Utility room	1	1st floor, North

[window shortened for easier viewing in help]

Any reader: Leave this selected to not limit the activity based on site.

A reader named: This option is permanently disabled. To get activity for a single reader, use the following option and select only that one reader in the list.

The readers selected below: To limit the report/view to specific readers, click this and then select the readers to include activity from.

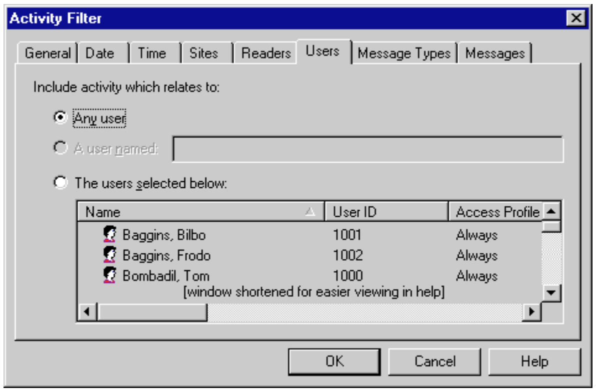
To select a single reader: Click that reader in the list.

To select multiple readers that are together on the list: Click the first reader in the group, hold the *SHIFT* key down, and click the last reader that you want to select.

To select multiple readers that are not together on the list: Click the first reader to select, hold the *CTRL* key down, and click each other reader that you want to select.

Users

This screen lets you limit to activity that occurred for certain users.



Include activity which relates to:

● Any user

○ A user named:

○ The users selected below:

Name	User ID	Access Profile
Baggins, Bilbo	1001	Always
Baggins, Frodo	1002	Always
Bombadil, Tom	1000	Always

[window shortened for easier viewing in help]

Any user: Leave this selected to not limit the activity to particular users.

A user named: This option is permanently disabled. For a single user, use the following option and select only that one user in the list.

The readers selected below: To limit the report/view to specific users, click this and then select the users to include activity for.

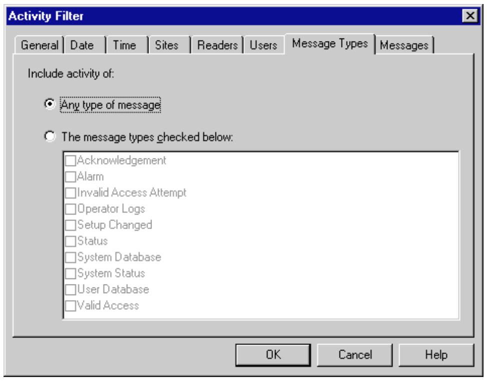
To select a single user: Click that user in the list.

To select multiple users that are together on the list: Click the first user in the group, hold the *SHIFT* key down, and click the last user that you want to select.

To select multiple users that are not together on the list: Click the first user to select, hold the *CTRL* key down, and click each other user that you want to select.

Message Types

This screen lets you limit the activity included to particular kinds of messages. If you need only specific messages within a category, use the *Messages* tab instead.



Include activity of:

● Any type of message

○ The message types checked below:

- □ Acknowledgement
- □ Alarm
- □ Invalid Access Attempt
- □ Operator Logs
- □ Setup Changed
- □ Status
- □ System Database
- □ System Status
- □ User Database
- □ Valid Access

Any message: This includes activity regardless of what type of message it generates.

The messages types checked below: Click this and then check any message type to include. You can check more than one box to include multiple types of messages.

Acknowledgement: This does not list anything.

Alarm: This lists any message that generates an alarm. Which messages generate alarms is controlled by your choices on the *Alarms* tab in *System Settings*. If you change which messages generate alarms, messages that did not generate an alarm when they occurred will not be listed, even if they would generate an alarm now.

Invalid Access Attempt: This lists any message where someone tries to get access and cannot. This includes the messages *Identity Unknown, Access Denied, and Access Refused, Time Zone*.

Operator Logs: This lists when operators log in or log out of HandNet, and it lists invalid login attempts. It does not list the addition of new operators or changes to the operator settings; only when each operator uses the system.

Setup Changed: This lists any setup changes made directly using command mode at the reader. For setup changes made through HandNet, use *System Database*.

Status: This lists any messages that tell whether auxiliary input and output is on or off.

System Database: This lists all setting changes made through HandNet. This includes adding or changing sites and readers, changing system settings, changing time zones, holidays and access profiles.

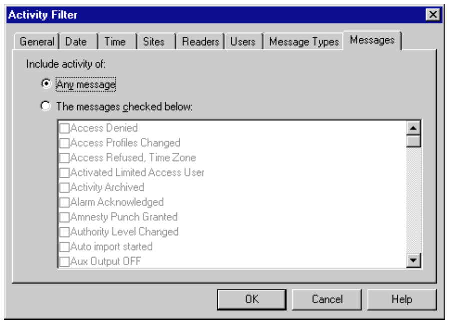
System Status: This lists messages related to when HandNet was started and exited, messages related to enrolling users, messages related to communication problems with readers, and messages related to information being downloaded/uploaded to/from readers.

User Database: This lists messages related to users being added, deleted, or changed. It does not include messages related to users being enrolled or attempted unauthorized enrollments.

Valid Access: This lists *Identity Verified* messages.

Messages

This screen lets you limit the report or activity view to specific messages. For example, if you were trying to track who came into the building, you might select the building entrances on the *Readers* tab, and then choose only the message *Identity Verified* here. Or if you were trying to track access problems, you might limit the output to the messages *Access Denied* or *Identity Unknown*. If you want all of the messages in a particular category, you may find it easier to use the *Message Types* tab instead.



Include activity of:

● Any message

○ The messages checked below:

□ Access Denied
□ Access Profiles Changed
□ Access Refused, Time Zone
□ Activated Limited Access User
□ Activity Archived
□ Alarm Acknowledged
□ Amnesty Punch Granted
□ Authority Level Changed
□ Auto import started
□ Aux Output OFF

Any message: This includes activity regardless of what message it generated.

The messages checked below: Check any message to include. See the list of activity messages starting on page 116 for an explanation of what causes each message. Not all of the messages include what you would expect. For example, the message *Authority Level Changed* does not include users whose authority level was changed on the *Security* screen in *User Properties*; it only includes users whose authority level was changed using the command menus on a reader, which is not how you would typically change a user if you use HandNet. Many of the messages are like this. If you want all of the messages in a particular category, you may find it easier to use the *Message Types* tab instead.

* * * * *

Archiving Past Activity

What Archiving Is

Archiving is moving past activity from the *Current Activity* file to a separate file. This keeps the *Activity* file smaller (and faster) while still keeping the information available for reports if needed. You can set HandNet to remind you to make archives using the *Archives* tab in the *System Settings*; see page 26.

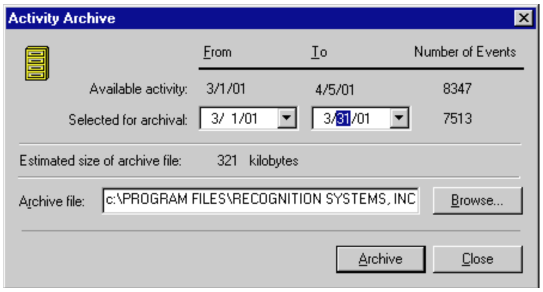
To generate an activity report on activity that is archived, you must indicate that you want to generate the report based on an activity archive (and then pick the appropriate archive).

Effect of Archiving on Reports

When you archive, HandNet removes activity from the current activity file and stores it in a different file. When you generate an activity report, you can use the current activity file OR one of your archive files, but you cannot include activity from more than one file in a single report. This means, for example, that if you make an archive once a month, you cannot generate a single report that looks at the previous year's activity; you would have to generate twelve reports, one for each monthly archive file. If you want an entire year's information in a single report, do not archive until the year is done, so all activity for the year will be in a single file.

Making the Archive

To make an archive of past activity, click the *File* menu and then click *Archive*. You see a screen like this:



Activity Archive

	From	To	Number of Events
Available activity:	3/1/01	4/5/01	8347
Selected for archival:	3/ 1/01	3/31/01	7513

Estimated size of archive file: 321 kilobytes

Archive file: c:\PROGRAM FILES\RECOGNITION SYSTEMS, INC

Available activity: This shows the date of the earliest activity in the activity file and the date of the most recent activity (usually today's date). One the right you will see the total number of events or activities currently in the file.

Selected for archival: This lets you choose the date range to include in the archive. The *From* date is initially set to the date of the earliest activity in the file; you do not normally want to change this date. The *To* date is initially set to today's date; you might sometimes want to make this earlier to keep more activity in the file. For example, suppose you make an archive on the fifth of each month for the previous month. You could change the *To* date to the last day of the previous month so that activity from the beginning of the current month would not be archived yet. Even if you leave the *To* date set to the current date, HandNet may not actually go up to that date: on the *Archives* tab in the *System Settings* there is an entry *Do not archive the latest ___ events*. The archive process keeps at least that many events in the current activity file, even if some of those events are before the date you enter here.

Estimated size of archive file: This is the approximate size that the archive file will be.

Archive file: This lists the name and location of the file that will be created. HandNet uses the location that you have entered for the *Default Archive Directory* on the *Archives* tab in the *System Settings*; see page 27. HandNet names the file using year/month/day hour/minute/seconds. For example *HN Activity Archive 20010406 094542.hna* is the default name for a file made on April 6, 2001 at 9:45 (and 42 seconds) AM. If you sometimes need to generate reports on past activity, and you do not find this naming method very clear, you can change this name. For example, if the archive contained information from the previous month, you might name it something like *Archive March, 2001.hna*. You must keep the .hna extension for HandNet to be able to find the file when you want to generate a report on it.

Once all entries are correct, click the *Archive* button to make the archive.

* * * * *

Exporting Activity

Why Export Activity

If you want to create custom activity reports using some external report tool, *Export Activity* on the *File* menu sends all of your current activity to an Access database file called *expactvt.mdb*. While the main HandNet database files are password protected for security reasons, this file is not, so you can open it (if you have Microsoft Access) and use any information in it. If you are only going to generate reports with *Activity Reports* on the *File* menu, you do not need this option; using it would only create a file that you do not need.

This option only exports current activity, not activity that you have archived, so if you plan to use this option you probably should check the *Export Transactions* box on the *Archive* tab in *System Settings*; see page 27. This causes activity to be automatically exported whenever you archive activity.

You only have access to this option if you have purchased the upgrade to full feature set of Version 2.0.

When you choose *Export Activity*, HandNet pops up a box that tells you how many activity records are going to be exported. Click *OK* to continue.

Avoiding Exporting the Same Information Twice

If you export activity and then export activity again without having archived the activity you exported last time, you will end up with duplicate records in that export file. That is, you will find the same activities listed more than once.

To avoid duplicate activity in the export file you can do one of two things:

- You can export activity and then immediately archive ALL activity. That way, the next time you export activity, the activity that was exported last time will not be in the current activity file, so it will not be exported again.
- If you do not want to archive activity after exporting (you might want to keep more activity in the current activity file so that you could see it in *custom activity* views or create reports that included a longer range of activity), delete or rename the last activity export file (*expactvt.mdb*) before exporting again. If you delete or rename this file, HandNet creates a new *expactvt.mdb* file when you export, and this new file will only contain the information from this export and not what you exported last time.

* * * * *

Activity Messages

You see activity messages in the *Activity* window. You can limit the activity in a custom activity view or in an activity report by checking the corresponding messages on the *Messages* tab in the filter/report design (see page 112). And you can control which messages cause alarms using the *Alarms* tab in the system settings (see page 25).

We have explained the messages in more detail here.

Command Menus in the Reader

Readers have built-in menus that let you change the settings in the reader. Some of the messages below can only occur if you make changes through these menus on the actual readers; you should not typically see these messages. Except for initially setting up the reader to communicate with HandNet, for recalibrating the reader, and for enrolling a user from the reader, you should NOT make changes to the reader through the reader command menus; you should control all other reader settings from within HandNet. See the HandKey manual for more about the reader menus.

Activity Messages

Access Denied: Someone repeatedly entered a valid ID at a reader, and each time the reader did NOT recognize the user's hand (at the reader, the user will see the message *ID Refused*). The number of times that a user can try before getting this message depends on the *Number of Tries* entry on the *Settings* tab in the *Reader Properties*; see page 47. If access is denied for a user, the reader will not accept that ID again until another user has successfully gained access at that reader.

Access Profiles Changed: Someone has changed one or more access profiles. During initial setup, this is a normal message. If you were not expecting access profiles to change, this could be an indication that someone was trying to give inappropriate access.

Access Refused, Time Zone: A valid ID was entered at a reader, but the user is not authorized to have access during the hours or days of the week based on the time zone associated with the reader in the access profile.

Activated Limited Access User: A user was set up with access for a limited date/time range. The computer's date and time matched the date/time the user was scheduled to start having access, so HandNet made the user active and sent the user's information to each appropriate reader so the user could can access; see page 93 for more about limited access.

Activity Archived: The operator used the *Archive* option on the *File* menu; (see page 113 for more on archiving past activity).

Alarm Acknowledged: An alarm occurred, and an operator went to the *Alarm Properties* screen and clicked one of the acknowledge buttons (following the message on the activity or alarm list, you will see *:ACK* followed by the name of the operator who acknowledged the alarm and when it was acknowledged); see page 103 for more on acknowledging alarms.

Amnesty Punch Granted: You should not see this message.

Authority Level Changed: A user's authority level was changed from the reader's command menu (typically you would change a user's authority

level from the *Security* tab in the *User Properties*; if you change the authority level there, you just see the message *User Record Changed*).

Auto Import Started: An *import.mdb* file (which contains users to import) was found, and HandNet was set up to automatically import users, so HandNet started importing them. Whether HandNet automatically imports users is controlled by the *Enable* box under *Auto Import* on the *User Import/Export* tab in *System Settings*; see page 28.

Aux Output OFF: The auxiliary output has been turned off.

Aux Unlock Via Wiegand Keypad: The auxiliary output has been turned on by a valid ID number at a remote keypad.

Auxiliary Input ON: The auxiliary input on the reader has been activated.

Auxiliary Output ON: The reader has turned on an auxiliary device (like an alarm) that is connected to the reader.

Auxiliary Output Setup Changed: The timing and clearing of an auxiliary output activation has been changed.

Baud Rate Changed: The communications baud rate has been changed using the command menus at the reader.

Command Mode Entered: Someone entered the command mode at a reader. Readers have built in menus that let you change the reader settings. These command menus are mainly needed when someone is using the readers without the HandNet program; HandNet controls most settings in the reader for you. The only tasks you should need to do through the reader command menus are setting up the reader's address and communication settings during initial setup, recalibrating the reader, and enrolling users at the reader if you are not using the *Enroll* option on the *Reader* menu.

Data Base Restored: You should not see this message.

Data Base Saved: You should not see this message.

Data Downloaded to Reader: Someone used one of the *Download* options on the *Reader* menu to send information to the reader; see page 60. Unless there was some problem with the reader that is being corrected, this is not usually necessary; HandNet usually automatically sends all information to the reader that the reader needs.

Data Log Buffer Empty: You should not see this message.

Deactivating Limited Access User: A user was set up with access for a limited date/time range. The computer's date and time matched the date/time the user's access was supposed to end, so HandNet made the user inactive and sent the appropriate information to readers so the user could no longer gain access, see page 93 for more about limited access.

Door Forced Open: A door was forced open without a valid ID and hand recognition at a reader.

Door Open Too Long: A door was kept open for longer than was allowed

based on the time entered in the *Door Switch Shunt Time* on the *Configuration* tab in the *Reader Properties*; see page 48.

Duress Alarm: A user entered the duress code, a code that indicates that the user is in trouble or that someone is forcing the user to give him/her access; see page 47 for more about duress codes.

Exit Granted: The user is permitted to exit.

Extended Datalog: Someone entered command mode on the reader and changed settings that do not have specific messages associated with them (for example, you get this message if you change the language of the reader's display or the format of the date on the reader).

HandNet Exited: Someone picked *Exit* from the *File* menu to shut HandNet down. Under normal circumstances, HandNet is left running continually so it can monitor activity and immediately process any alarm messages. If someone exited HandNet to install a new Version of the program or to perform maintenance on the computer it is on, there is probably no problem; if someone exited the program at some other point, this could be an indication of an attempt to get around security.

HandNet Started: Someone started the HandNet program. Under normal circumstances, HandNet is usually left running continually so it can monitor activity and immediately process any alarm messages. If someone exited HandNet to install a new Version of the program or to perform maintenance on the computer it is on and then restarted, then there is probably no problem. If you see the message *HandNet Started* but you do not see the message *HandNet Exited* earlier in the list, then someone exited the program and restored an older Version of the activity files; this could be an indication that someone is trying to hide activity.

HandNet+ File Converted: Someone used *Convert HandNet+* on the *File* menu to convert users from HandNet+ into HandNet for Windows (HandNet+ was an MS-DOS predecessor to HandNet for Windows); see page 98 for more on converting users from MS-DOS Versions of HandNet.

Holiday Table Changed: Someone has added, changed, or deleted a holiday with the *Holidays* option; see page 65 for more about setting up holidays.

Identity Unknown: Someone entered a valid ID at a reader, but the reader did not recognize the user's hand.

Identity Verified: At a reader, a user entered a valid ID and the reader recognized the user's hand and gave access.

Invalid Operator Login Attempt: Someone tried to log into HandNet but entered an invalid user name or password. This could occur if someone just typed the name or password incorrectly, or it could mean that an unauthorized person was trying to get into the program.

Leave Command Mode: Someone exited or left command mode at a reader. Readers have built-in menus that let you change the reader settings. These command menus are mainly needed when someone is using the readers without the HandNet program; HandNet controls most settings in the reader for you. The only tasks you should need to do through the reader command

menus are setting up the reader's address and communication settings during initial setup, recalibrating the reader, and enrolling users at the reader if you are not using the *Enroll* option on the *Reader* menu.

Lock Output OFF: Someone chose *Relock* from the *Reader* menu to relock an unlocked door; see page 128 for more about locking and unlocking doors.

Lock Output ON: Someone chose to unlock a door using one of the *Unlock* options on the *Reader* menu; see page 128 for more about locking and unlocking doors.

Lock Setup Changed: Using the command menus in the reader, someone changed the number of seconds the lock should be unlocked for or the number of seconds the door is allowed to be open (normally this is changed in HandNet on the *Configuration* tab in *Reader Properties*; if it is changed there, you just see the message *Reader Properties Changed*).

Manual Import Started: The operator selected *Import Users* to import users from the *import.mdb* file; see page 99 for more about importing users (when you must import users manually or whether HandNet imports them automatically is controlled by the *Enable* box under *Auto Import* on the *User Import/Export* tab in *System Settings*; see page 28).

Maximum ID Length Changed: Someone changed the maximum length for a user ID using the command menus in the reader (if you changed the ID length on the *Settings* tab in the *Reader Properties*, you would just see the message *Reader Properties Changed*).

Memory Cleared: Someone used the *Clear Memory* option from the *Command* menus in the reader. This erases all the users from the reader (typically you would do this if you were changing the use of the reader and wanted to make sure that those who previously had access through this reader no longer had access through it).

Messages Read: You should not see this message.

No Hand Read For Card: You should not see this message.

Operating Mode Changed: The operating mode of the reader has been changed using the command menus in the reader.

Operator Added: A new operator (someone authorized to use HandNet) was added on the *Operators* tab in *System Settings*; see page 24 for more about adding operators.

Operator Deleted: An operator (someone authorized to use HandNet) was removed from the *Operators* tab in *System Settings*; see page 24 for more about deleting operators.

Operator Login: An operator logged into HandNet.

Operator Logout: An operator logged out of HandNet.

Operator Properties Changed: Someone changed the tasks that an operator is allowed to do on the *Operators* tab in *System Settings*; see page 24 for more about controlling which options an operator can use.

Output Mode Changed: The output mode of lock output or card reader emulation has been changed using the *Command* menus in the reader.

Passwords Changed: Someone changed the passwords for the reader *Command* menus, using the command menus in the reader. Generally this setting is controlled from HandNet on the *Passwords* tab in *Reader Properties* rather than from the reader (if you change this or other settings for the reader in HandNet, you just see the message *Reader Properties Changed*).

Printer Setup Changed: If a serial printer is attached to the reader, the printer settings have been changed using the command menus in the reader.

Reader Action Failed: HandNet was unable to complete a communication attempt with the reader. This could be an indication that the connection to the reader is not set up correctly; see the *Troubleshooting* resolving this error.

Reader Added: A reader was added to HandNet.

Reader Connection Failed: HandNet was not able to establish communications with the reader. This could be an indication that the connection to the reader is not set up correctly; see *Troubleshooting* resolving this error.

Reader Connection Timeout: HandNet lost its connection with the reader. This could be an indication that the connection to the reader is not set up correctly; see the troubleshooting for help resolving this error.

Reader Data Uploaded to HandNet: Someone used *Upload Users* on the *Reader* menu to get user information from the reader; see *Getting User Information from a Reader* on page 99.

Reader Deleted: A reader was deleted from HandNet.

Reader Properties Changed: Someone went to the *Reader Properties* and changed the settings on one of the tabs there. HandNet does not keep track of which settings were changed. For more about *Reader Properties*, see page 45.

Record Imported for Creation: An new user was added to HandNet by the import process.

Record Imported for Deletion: A user that was already in HandNet was deleted based on information in the *Import* file.

Record Imported for Modification: A user that was already in HandNet was changed to match a user with the same ID in the *Import* file.

Record Imported, Empty Template Overwrote Local Enrollment: A user that was not enrolled was imported. This replaced an enrolled user, so the user is not longer enrolled in HandNet. You can prevent enrolled users by being replace by either preventing the exporting computer from exporting users that are not enrolled yet, or by changing the import settings so non-enrolled users cannot replace enrolled ones; see the explanation for the *Import/ Export* settings on page 28.

Reject Override Changed: Someone changed the reject threshold for an individual user using the command menus in the reader. Generally this setting is controlled in HandNet with the *Override* setting on the *Security* screen in *User Properties*; HandNet users would not typically change this at the reader (if you change this or other user settings in HandNet, you just see the message *User Properties Changed*).

Reject Threshold Set: Someone changed the reject threshold using the command menus in the reader. Generally this setting is controlled from HandNet using *Reject Threshold* on the *Configuration* tab in *Reader Properties* rather than from the reader (if you change this or other settings for the reader in HandNet, you just see the message *Reader Properties Changed*).

Remote Enrollment Started: A user was enrolled with the *Enroll* option on the *Reader* menu (for users enrolled from the *Command* menu on the reader, you see the message *User Enrolled*); see page 87 for more about enrolling users.

Report Engine Unavailable: You should never see this message.

Request to Exit Activated: A user has pressed the *Request to Exit* button in order to get out of the secure area.

Score Is: You should never see this message.

Site Added: A site was added to HandNet.

Site Code Changed: The site code was changed using the *Command* menus in the reader.

Site Connected: HandNet is set up to connect with the site by modem, and HandNet connected to the site.

Site Deleted: A site was deleted in HandNet.

Site Disconnected: HandNet is set up to connect with the site by modem, and HandNet disconnected from the site when it was done communicating with the site.

Site Properties Changed: In HandNet, one or more changes were made to the *Site Properties*; for more about *Site Properties*, see page 34.

Special Enrollment: The *Command* menus in the reader was used to enroll a user who does not require hand recognition to gain access.

Supervisor Override: You should not see this message.

System Re-calibrated: Someone recalibrated the reader; see page 124.

System Settings Changed: Someone changed one or more entries on one of the *System Settings* tabs that you get to with settings on the *View* menu; for more about system settings, see page 22.

Tamper Activated: Someone has shaken the reader roughly or has opened the reader. Unless someone was servicing the reader, this message generally

warrants further investigation.

Time and Date Set: Someone changed the time and date in the reader using the command menus in the reader (generally, rather than changing date and time in the reader, you would just make sure that the date and time were correct in the computer and then send the date and time to the reader using *Download Time* on the *Reader* menu).

Time Restrictions Turned On/Off For All Users: You should not see this message.

Time Zone Data Changed: Someone changed a time zone using the *Command* menus in the reader. Generally this setting is controlled with the *Time Zone* settings in HandNet and not changed at the reader (if you change time zones in HandNet, you see the message *Time Zones Changed*).

Time Zones Changed: In HandNet, someone changed *Time Zones*; see page 61 for more on setting up *Time Zones*.

Two Man Timeout: Two people were required to verify at the reader, and they have not done so within the permitted time period.

Unable to Close Communications Port: HandNet was unable to close the *Serial Communications* port.

Unable to Install Communications Port or Unable to Open Communications Port: You get this message if HandNet tries to establish communication with a reader through a serial port and it cannot. Generally this only happens if you are running another program that is already controlling that serial port. You cannot have two different devices connected to the same port, so if a reader really is connected to that port, nothing else should be. Either you have selected the wrong port on the *Connection* tab in the *Site Properties*, or the other program that you are running has the wrong port selected. If you were previously running another program (especially one trying to connect to a modem, fax, or printer), it is possible that the other program tried to use the port and did not close it properly. Make sure that other programs that might try to control the port are closed. If the problem still exists, trying shutting everything down and restarting the computer.

Unable to Retrieve Datalog: An attempt to get information from the reader failed.

Unauthorized Enrollment Attempted: Someone tried to enroll a user at a reader and the user had not been added to HandNet yet. Your settings do not allow this (to change your settings so this is allowed, check the box by *Do not delete unauthorized enrollments* on the *Security* tab in *System Settings*; see page 23).

Unit Address Changed: Someone changed the address of the reader using the command menus in the reader.

User Added From Card: You should not see this message.

User Database Field Added: Someone went to the *Custom* tab in the *User*

Database properties and added a new custom entry; see page 97.

User Database Field Deleted: Someone went to the *Custom* tab in the *User Database* properties and removed a custom entry.

User Database Import Finished: The process of importing users (from the *import.mdb* file) is done.

User Enrolled: A user was enrolled using the command menu on the reader (for users enrolled with the *Enroll* option on the *Reader* menu, you see the message *Remote Enrollment Started*); see page 87 for more about enrolling users.

User Record Added: A user was added in HandNet.

User Record Changed: *User Properties* were changed for a user in HandNet. The change could be on any of the three tabs of user information; see page 90 for more on user properties.

User Record Deleted: A user was deleted in HandNet.

User Removed: A user was removed using the command menus in the reader. A user who was removed in this way is only removed from that one reader; the user is not removed from HandNet or from any other reader. If you ever download users to a reader, the user will be added to the reader again if the user is still in HandNet (to remove a user from HandNet, click the user on the list of users and press the *DEL* key. Removing a user from HandNet generates the message *User Record Deleted*).

Users Listed: Someone listed users using the command menus in the reader (if you want a list of users, its generally much easier to just look at the list of users in HandNet or to print the *Users* report; see page 13).

Users Time Zone Changed: When a user can access the reader was changed from the command menus in the reader (typically, this is not changed at the reader; you would instead change the user's access profile on the *Security* tab in *User Properties* to change when the user has access to particular readers. If you did this, you would see the message *User Properties Changed*).

* * * * *

Other Ongoing Activities

Reader Maintenance

Cleaning Readers

You should periodically clean hand readers; if you do not, users may get rejected more often.

Spray any ordinary, non-abrasive cleaner on a clean cloth, and then use the cloth to wipe the platen, the mirror and reflector on the sides of reader, and the window above the platen. When wiping the platen, start from the back corners and wipe forward.

Never spray cleaning fluid directly onto the reader! Always spray a cloth and then wipe the reader with the cloth.

Never use an abrasive or gritty cleaner! An abrasive cleaner could scratch the reader; this would damage it.

Recalibrating Readers

If users are often being rejected at a particular reader, try recalibrating it. To do this:

1. Check the list of users to make sure you have an authority level of one or higher. If you have an authority level of *None*, you cannot do this (to change your authority level, double-click your name on the list of users, click the *Security* tab, click the *Authority Level* entry, and select the appropriate level).

2. Go to the reader to be recalibrated, and enter command mode on the reader:

   If you have a HandKey II or HandKey CR reader: Press *CLEAR*, and then press *ENTER*.

   If you have an ID3D HandKey reader: Press *#* AND *** (you can press them at the same time, or one after the other).

   The display on the reader should look like this:

```
    READY
  * :
```

3. Type your *User ID* number (the same one you enter to get access through the reader), and press *ENTER* or *#.* The reader asks you to place your

```
ENTER PASSWORD
```

hand. Once it recognizes your hand, this display looks like this:

4. Type *1* and press *ENTER* or *#* (this is the standard password for the *Service* menu in the reader; if you have changed this on the *Passwords* screen in the *Reader Properties*, enter the password you have set up). The display should now look like this:

```
    CALIBRATE
 *  NO     YES #
```

If the reader shows the *READY* screen again instead of this screen, either you placed your hand improperly or you do not have the rights to do this; carefully check step one again.

5. Press the *YES/#* button. This display should now look something like this:

```
 r0  c0  e100  s
RECAL  (Y#/N*)?:
```

(The actual numbers on the first line may be different).

6. Press the *YES/#* button again. After telling you to please wait, you will see the *Calibrate No/Yes* display again. At this point, the reader should be recalibrated.

7. Press the *CLEAR* button to leave the *Service* menu and return to the reader to its normal display.

* * * * *

Making Backups

Why Make Backups

Occasionally computer hard drives fail, losing the information on them. Occasionally computer files get damaged, making the information in them unusable. And occasionally computer users make mistakes and delete information they should not. A backup is an extra copy of the information on your computer, so that if the information gets damaged or lost, you have another copy to protect you.

The information in HandNet—information about readers, access profiles, and users—represents many hours of work. The record of activity (including archived historical activity) is often an important security record. So you should protect your many hours of work by periodically making a backup copy of this information.

Making Backups a Scheduled Event

In practice, many computer users understand that backups are important, but they still go months or even years without actually making one. Then, when a problem occurs, the backup they have is so old that it does not save them all that much work. The way to avoid this is to make backing up your information a scheduled part of your routine. How often you need to make them depends on how many changes to the information you make. If you are continually adding and removing users, a weekly backup might be appropriate. If you make fewer changes and losing a month’s changes would not be that hard to redo, a monthly backup might be enough. Regardless, decide how often to make a backup, and then put it on your calendar; do it every Friday morning, or every month before you print your activity reports. If you do not schedule backups, they probably will not happen. And if you do not make them, sooner or later most computer users regret it.

How to Make a Backup of Your HandNet Information

You should periodically be making backups of all the information on your computer. How to best do that is beyond the scope of these instructions. Here, we will just tell you how to make a backup of your HandNet information.

1. Use *Windows Explorer* to go to the folder HandNet is in (if you installed HandNet in the standard location, it is in *C:\Program Files\Schlage Biometrics, Inc\HandNet for Windows*).

2. Make a copy of all of the Microsoft Access Database files (**.MDB*) and all of the HandNet Activity Archive files (**.HNA*) in this directory. You can copy these files to a floppy disk or to a network drive. If the files are large, WinZip is a helpful and inexpensive utility that lets you both compress a number of files into a single archive and spread the archive over a number of disks if needed (to get WinZip, go to *www.winzip.com*. For help making an archive span several floppy disks, look up “spanning” in the index of WinZip’s help).

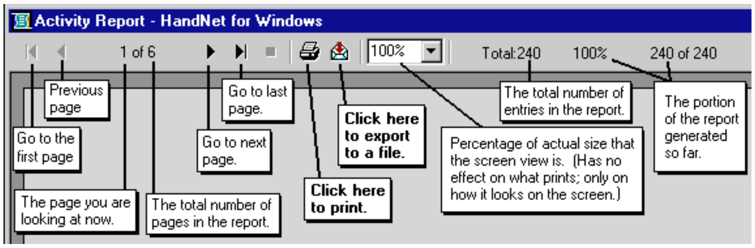
The best protection is to store the backup disks in a different place than the computer. That way, if the computer is damaged by fire or water, or if the computer equipment is stolen, there is no chance of the backup disks being damaged or taken.

* * * * *

Reporting and Exporting Information

Printing or Viewing Reports

Whenever you generate a report, HandNet shows the report in a new window. The header of that window lets you move from page to page, print the report, or export the report to a file. The header looks like this:



Go to the first page

Previous page

The page you are looking at now.

The total number of pages in the report.

Go to next page.

Go to last page.

Click here to print.

Click here to export to a file.

Percentage of actual size that the screen view is. (Has no effect on what prints; only on how it looks on the screen.)

The total number of entries in the report.

The portion of the report generated so far.

To print the report: Click the printer icon near the middle of the header to print the report.

If the printer icon is disabled and grayed out, you do not have a printer set up yet on this computer (to set up a printer, go to the Windows *Start* menu, highlight *Settings*, pick *Printers*, and click *Add Printer*).

To export the report to a file: Click the icon with the envelope. You can export to a variety of formats including Word, Excel, Lotus 1-2-3, ...rtf, text, and others.

To close the report window when done: Click the *X* in the upper-right corner of the window.

Getting Information from HandNet Database Files

HandNet for Windows stores information in access database files (*actions.mdb, activity.mdb,* and *HandNet.mdb*). These files are password-protected for security; we do NOT ever give these passwords out for any reason. If we did, it would put the integrity of your security at risk.

Exporting activity to an access database file

However, HandNet can export activity to an access database file that is not password protected so you can open it and access any information in it at will. If you want to create custom activity reports using some external report tool, *Export Activity* on the *File* menu sends all of your current activity to an access database file called *expactvt.mdb*.

Exporting the content of any report to various formats

To save HandNet information to a file, you can also generate any *Activity Report* or other report on the *Reports* menu and, when you see the report on the screen, click the *Export* button.

You will then be able to save the content of the report in a number of different formats so you can import it into other programs. These formats include: character-separated values, comma-separated values, Crystal Reports, Data Interchange Format (DIF), Excel (Versions 5.0, 7.0, or 8.0; either extended or not), Lotus 1-2-3 (WK1, WK3, or WKS), Access 97 database, paginated text, record style (columns of values(report definition, Rich Text Format (RTF), tab-separated, text, or Word for Windows)).

* * * * *

Locking and Unlocking Doors

Automatically Unlocking a Door on a Scheduled Basis

If you regularly want a door unlocked during certain hours:

1. If you have not already done so, set up a time zone that corresponds to the days and times you want the door unlocked.

2. Select the reader(s) in the list of readers.

3. Pick *Reader* from the main menu, and then pick *Properties* from the *Reader* menu.

4. Go to the *Configuration* tab.

5. In the *Auto Unlock Time Zone*, choose the time zone when the door should be automatically unlocked. HandNet automatically unlocks the door at the beginning of the time zone, and locks it again at the end of the time zone.

Unlocking a Door on a Non-Scheduled Basis

Unlock on the *Reader* menu lets you unlock a door without setting it up to be regularly unlocked.

1. Select the reader(s) in the list of readers.

2. Pick *Reader* from the main menu, and highlight *Unlock* on the *Reader* menu. You will see another menu with two choices: *Indefinite* and *Timed*.

   To unlock a door so that it stays unlocked until you lock it again: Choose *Indefinite*. This leaves the door unlocked until you lock it again with *Relock* on the *Reader* menu.

   To unlock the door momentarily: Choose *Timed*. This unlocks the door connected to that reader only for the number of seconds specified in *Lock Open For* on the *Configuration* tab in the *Reader Properties* (that is, it unlocks the door for the same number of seconds that the door would be unlocked if it were opened by a reader).

Locking a Door so it cannot be Opened from the Reader

Lockup on the *Reader* menu disables the lock on the door for the selected reader. The reader will still let users enter their ID numbers and still verify hands, but the door will stay locked and will not open even for valid users. No one will be able to open the door from the reader until you choose *Unlock* or *Relock* from the *Reader* menu.

Locking an Unlocked Door

If you have unlocked a door with *Unlock, Indefinite* on the *Reader* menu, *Relock* locks it again (if you unlocked the door using *Unlock, Timed* on the *Reader* menu, the door automatically relocks after the number of seconds specified in *Lock Open For* on the *Configuration* tab in the *Reader Properties* just as it would if the door were unlocked by the reader, so you do not have to anything special to relock it).

If you have disabled access through a door with *Lockup* on the *Reader* menu, *Relock* releases so the reader can open it again.

* * * * *

Turning an Auxiliary Device On or Off

HandNet can be set up to automatically turn on external auxiliary devices when certain conditions occur. For example, it might trigger an alarm, turn on lights or a security camera, and so on.

HandNet can turn an auxiliary device on automatically when certain conditions occur. When this can happen is controlled by the *Auxiliary (AUX) Settings* tab; see page 48 (the HandKey II and HandKey CR support up to three auxiliary devices; this option only controls the first of these, the same one controlled by the *Auxiliary Settings* tab in *Reader Properties*. The other two are only controlled by the *Extended Settings* tab in *Reader Properties*).

Manually Turning an Auxiliary Device On

Auxiliary Output on the *Reader* menu lets you turn manually turn an auxiliary device on or off without anything happening at the reader. For example, suppose a reader, in addition to being connected to a door, is also connected to an auxiliary light. You could use this option to turn the light on without doing anything at the reader.

To turn on an auxiliary device that is connected to a reader:

1. Click a reader in the right pane of the *Network* window (if the *Network* window is not shown, press *CTRL-N* to open it).

2. Click *Reader* from the main menu bar at the top of the screen.

3. Click *Auxiliary Output* on the *Reader* menu, and then click *On*.

Manually Turning an Auxiliary Device Off

If you have manually turned an auxiliary device on, or if an alarm condition has turned it on, you can also turn the device off from HandNet. For example, suppose an auxiliary alarm is connected to the reader, and suppose the alarm is set to sound for fifteen minutes after the condition occurs. You could use this option to turn the alarm off before the fifteen minutes was done.

To turn off an auxiliary device that is connected to a reader:

1. Click a reader in the right pane of the *Network* window (if the *Network* window is not shown, press *CTRL-N* to open it).

2. Click *Reader* from the main menu bar at the top of the screen.

3. Click *Auxiliary Output* on the *Reader* menu, and then click *Off*.

* * * * *

Troubleshooting

Answers to Common Questions

Enroll Option Disabled

If the *Enroll* option on the *Reader* menu is disabled or grayed out, there are several possible reasons. Check each of the following:

1. Make sure you are logged in. If you are not logged in, you cannot change anything.
2. Make sure that you have selected a reader on the list of readers. Since enrollment has to be done at a reader, you must pick the reader to enroll at before the enroll option will work (to see the list of readers, type *CTRL-N* or pick *Network* from the *View* menu).
3. Pick *About HandNet for Windows...* from the *Help* menu. Check the bottom of the box that pops up. To be able to use the enroll feature, the last line must say *You may use all features of this software.* If this line says *Your current license does not let you use the enroll...,* you must contact your dealer and upgrade your license before you can use this feature (once you upgrade, we will send you an access code that makes the feature available). If you do not upgrade to the full feature set, you must start the enrollment process using the command menus in the reader; see page 87.
4. Check with your supervisor to see if you are authorized to enroll users (for you to be authorized to enroll users, *Reader Data Download* must be checked in the *Access Rights* for the operator in *System Settings*).

No Current Record Message

You get the message *No Current Record* when you start HandNet if you have not added any users yet. This message stops occurring once you add a user; see page 74 and following for help adding users.

Problems Connecting to a Site by Modem

If you are having trouble getting HandNet to connect to a site by modem, check each of the following:

1. Click the site in the left pane of the *Network* window, pick *Properties* from the *Site* menu, and click the *Connection* tab.
2. Make sure you have picked the serial port that the modem is connected to; if this is set to *None*, HandNet will not connect.
3. Make sure the *Baud Rate* in *Site Properties* in HandNet matches the baud rate the reader is set up for. We recommend 9,600 for a HandKey II or HandKey CR and 2400 for a HandKey reader.
4. Make sure the phone number is entered correctly. If you have to dial some digit to get an outside line, enter this digit followed by a comma before the phone number. If the number is a long distance number, make sure you have entered the 1 and the area code as appropriate. For example, if you

have to dial *9* for an outside line, and the number was a long distance call that required by *1* and an area code, you would enter the number like this:

9, 18025551212

5. Make sure the modem is hooked up to a phone line.

6. Make sure the phone line is plugged into the right jack on the modem connected to your computer (most modems have two jacks: one labeled *Line* and one labeled *Phone*. The phone wire from the phone jack on the wall must connect to the jack on the modem labeled *Line*.

7. Make sure the phone line has a dial tone (hook up a regular phone to the modem jack labeled *Phone* to see if you hear a dial tone; if you do not, there is a problem with the jack or phone line).

8. Make sure no other phone, fax machine, or modem is trying to use the same phone line.

9. Make sure call waiting is not on for this line.

10. On the *Schedule* tab in *Site Properties*, make sure you have set up a time for this site to connect. Make sure this connection time is enabled (checked).

Program Claims to be a Demonstration Version

When HandNet for Windows is installed, it is in demonstration mode: it gives you full functionality for fourteen days, and after that it limits the use of certain features.

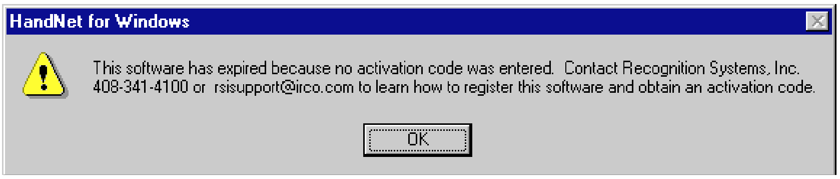
If you purchase a previous Version of HandNet for Windows, you are also authorized to use this Version, but you must register it first, even if you registered your previous Version. Once you send us your registration information, we will give you an authorization code that makes the program permanently functional.

To register this copy of HandNet, please pick *Registration* from the *File* menu and follow the instructions on that screen (we would just repeat the instructions here, but you need the unique ID number that is shown on that screen and you also need to print the registration form).

If you really do have a demonstration Version, please contact us to find out how to purchase a full Version.

Software Expired

After the first time you use this Version of HandNet, you have fourteen days to register it. You must register even if you registered your previous Version of HandNet. If you do not register within fourteen days, you will not be able to log in. When you try to log in, you see this message:



This software has expired because no activation code was entered. Contact Recognition Systems, Inc. 408-341-4100 or rsisupport@irco.com to learn how to register this software and obtain an activation code.

If you get this message, exit HandNet and then restart. This brings up the registration screen. Send us the information requested on that screen. Once we get your information, we will send you an activation code to enter on the registration screen. This will make HandNet permanently functional.

Unable to Acknowledge an Alarm

If you have opened the detail box for an alarm and the *Acknowledge* buttons are disabled or grayed out, check the following:

1. Make sure you are logged in. If you are not logged in, you cannot change anything.
2. Make sure that you are clicking one of the *Acknowledge* buttons at the bottom left of the window; you cannot just click the checkbox by the word acknowledged; you must click one of the buttons.
3. Check with your supervisor to see if you are authorized to acknowledge alarms (for you to be authorized to acknowledge alarms, the *Alarm Acknowledgement* box must be checked in the *Access Rights* for the operator in *System Settings*; see page 24 for more on adding or changing operator settings).

User Often Rejected

If a user is often rejected at readers, you may need to teach the user the correct way to place the hand on the platen; see *Teaching Users How to Place Their Hands on Readers* on page 86.

Creating a new profile of the user's hand

If the user held his/her hand improperly while being enrolled, or if the user has lost or gained a lot of weight, the hand profile may be different enough to prevent recognition. Delete the user (this eliminates the old hand profile), and then add the user again. When you re-enroll the user, this creates a new profile of the hand. Make sure the user correctly places his/her hand. You can usually avoid this situation by allowing HandNet to update the user's hand profile each time the user gains access; see page 23.

If the user has a disability that prevents consistent hand placement

You may need to increase the tolerance for the user. To do this:

1. Double-click the user on the list of users (you could also click once to select the user and then pick *Properties* from the *User* menu).
2. Click the *Security* tab.
3. Check the *Override Reader's Threshold* box if it is not already checked.
4. Drag the pointer to the right (the *Less Sensitive* side).

If many users are rejected at a particular reader

If many users are being rejected at a particular reader, you may need to clean the reader or you may need to recalibrate it; see page 124.

* * * * *

Index

Ingersoll Rand
Security Technologies

Ingersoll Rand's Security Technologies Sector is a leading global provider of products and services that make environments safe, secure, and productive. The Sector's market-leading products include electronic and biometric access control systems; time and attendance and personnel scheduling systems; mechanical locks and portable security, door closures and exit devices, steel doors and frames, architectural hardware and technologies and services for global security markets.

408.341.4110

www.schlage.com www.ingersollrand.com

Schlage
Biometric Solutions
Ingersoll Rand Security Technologies
1520 Dell Avenue
Campbell, CA 95008
Office: 866-861-2480/512-712-1413 (international)
Fax: 866-303-1794/408-341-4111
E-mail: sbssupport@irco.com

HandNet-Lite

Terminal User's Guide

Ingersoll Rand
Security Technologies

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and, if not installed and used in accordance with the Installation Manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at the user's own expense.

This Class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numerique de la classe A respecte toutes les exigences du Reglemente sure le materiel brouilleur du Canada.

Document Part Number: 70100-6210 – Revision 3 – June, 2009

HandPunch is a trademark of Schlage Biometrics, Inc.

The trademarks used in this Manual are the property of the trademark holders. The use of these trademarks in this Manual should not be regarded as infringing upon or affecting the validity of any of these trademarks.

Schlage Biometrics, Inc. reserves the right to change, without notice, product offerings or specifications.

Contents

Getting Started

Introduction

What HandNet Lite Does

HandNet Lite lets you control and monitor many connected FingerKey and/or HandKey readers. In this one program, you can control who can use each reader and when. You can also monitor activity and alarms for all readers at once.

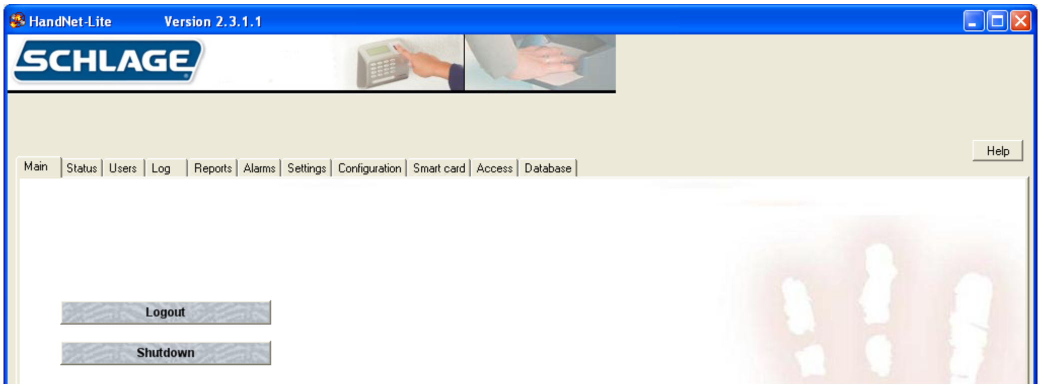
HandNet Lite System Requirements

Operating System: Windows XP SP3, Vista, Windows Server 2003 SP1 or greater, Windows 2000 Professional or Server Editions SP4, and Windows 95 & 98.

Screen Resolution: Screen resolution must be set to at least 1024 x 768; the HandNet Lite window won't fit on your screen if you use a lower resolution. The actual screen size is 1020 x 720, so if your screen resolution is 1024 x 768, your task bar must be on the top or bottom of the screen, and the task bar must be no more than two lines high; if the task bar is three lines or higher or if it is on the side of your screen, part of the HandNet Lite window will run off the screen.

Starting HandNet Lite

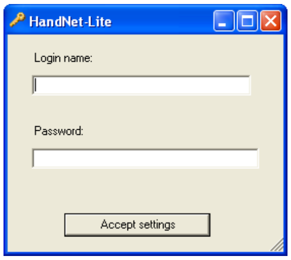
To start HandNet Lite, either double-click the HandNet Lite icon on your Windows desktop or click the Start menu on your Windows taskbar, highlight Programs, highlight Schlage Biometrics, highlight the HandNet Lite folder, and click HandNet Lite. The main window opens.


HandNet-Lite Version 2.3.1.1
SCHLAGE
Help
Main | Status | Users | Log | Reports | Alarms | Settings | Configuration | Smart card | Access | Database
Logout
Shutdown

Logging into HandNet Lite

HandNet Lite requires you to log in before you can make any changes; this prevents unauthorized people from changing information. If you aren't logged in, you can look at the current status of readers and get on-line help, but you can't change any information or use any other options.

1. **Click Login on the Main window. You'll see:**



HandNet-Lite

Login name:

Password:

Accept settings

2. **Type your Login name and Password and click Accept.**

   If this is a new system: Use a Login name of "1234" and a Password of "new." (After logging in for the first time, you should add one or more new operators. See Managing Operators on page 26 for more information.)

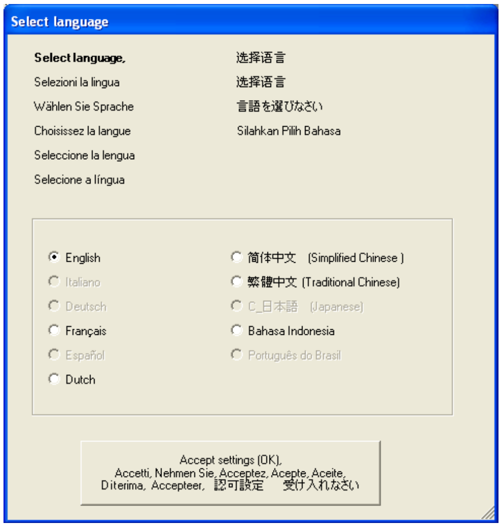
   After initial setup: If you forget your Login name or Password, see your supervisor or security administrator.

   The login name and password are case sensitive. For example, the passwords new, New, and NEW are all different.

After you are done using HandNet Lite, log out so unauthorized people won't be able to use the program.

Select Language

After HandNet-lite version 2.3 is installed, the first time it is run the following screen will be presented so that the displayed language can be selected. If you do not see the special characters on your computer, use Control Panel, Regional and Language Settings, Advanced tab and select the desired character sets.



Select language

Select language,	选择语言
Selezioni la lingua	选择语言
Wählen Sie Sprache	言語を選びなさい
Choisissez la langue	Silahkan Pilih Bahasa
Seleccione la lengua	
Selecione a língua	

● English	○ 简体中文　(Simplified Chinese)
○ Italiano	○ 繁體中文 (Traditional Chinese)
○ Deutsch	○ C_日本語　(Japanese)
○ Français	○ Bahasa Indonesia
○ Español	○ Português do Brasil
○ Dutch	

Accept settings (OK),
Accetti, Nehmen Sie, Acceptez, Acepte, Aceite,
Diterima, Accepteer, 認可設定　受け入れなさい

This is the "Select Language" screen. Current language choices are English, French, Dutch, Simplified Chinese, Traditional Chinese, and Bahasa Indonesian.

Getting Help in HandNet Lite

The on-line help has the same information as this manual. To get help in HandNet Lite, click the Help button. Use the contents, index, or search tabs at the left of the help window to find any topic.

For Basic Topics

Click the Contents tab at the top of the left pane, click a book to open, and then click a topic. Not every topic is in the Contents though, so if you don't find what you need, try the Index or Search tabs.

For Groups of Topics on a Single Theme

In addition to the contents you can also click on the pull-down list right under the Previous/Next buttons (in the bottom middle of the header). This list contains a number of important groups of topics. Once you are on one of these topics, the Next and Previous buttons work as well.

Marking a Topic to Return To

In the on-line help, to mark a topic that you want to come back to:

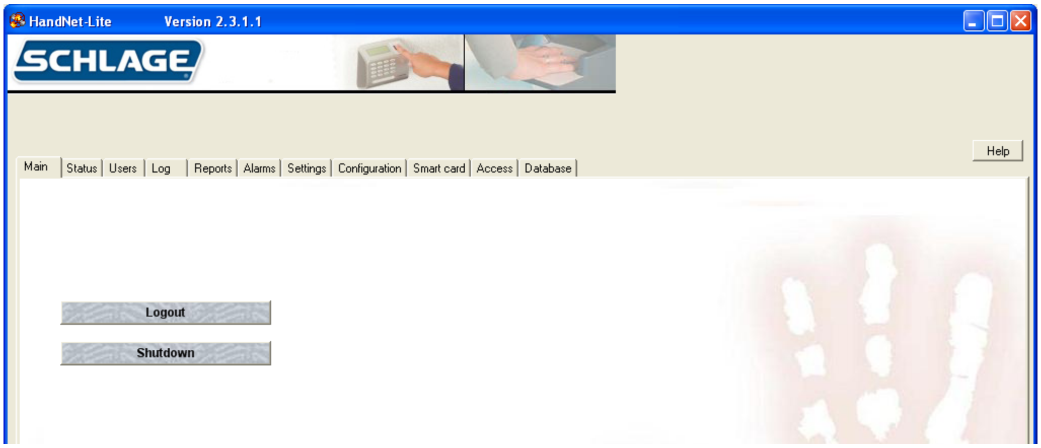
1. Go to the topic that you want to mark.
2. Click the Favorites tab at the top of the left pane.
3. Click the Add button at the bottom of the pane. This adds the topic to your favorites list.

To get back to any marked topic later:

1. Click the Favorites tab at the top of the left pane of the help window.
2. Double-click the topic.

Main HandNet Lite Window

After you log into HandNet Lite, a number of additional tabs appear that let you get to the different parts of the program. Which tabs you see depends on which operator login you used. The screen below shows all of the options.



What You Can Do On Each Tab

Each of the tabs are explained in further detail later in the following chapters.

Status: The Status tab lists every reader in HandNet Lite and the network (group of readers) the reader is connected to. It gives information about each reader and the state of its connection. See page 7 for more information.

Users: The Users tab lists every user that has been added to HandNet Lite, including the user's name, ID, access profile (the group of readers the user has access to), authority level (which reader menus the user can program), and whether the user is enrolled; see page 9. You can add, change, or delete users through the buttons in this tab.

Log: The Log window lists significant events at any connected reader. It doesn't list user accesses, but it lists user additions and enrollment, alarm conditions, and so on. It also lists significant changes made in HandNet Lite. For each event you see the date and time, network and reader, user name and IDs, a brief description of what happened, and an icon showing the type of activity. See page 17 for more information.

Reports: The Reports tab lets you generate reports on all of your users and all of your readers. See page 19 for more information

Alarms: The Alarms tab shows a subset of what you see on the Log tab; this tab lists only those events that are classified as alarm conditions. These generally require immediate attention. See page 23 for more information.

Settings: The Settings tab lets you change HandNet Lite's login name and passwords. It also lets you choose the default Access Profile for users added at a reader, that is, which readers the user has access to. See page 25 for more information.

Configuration: You may add, change, or delete networks and readers. The Configuration tab also allows you to create Wiegand output configurations which can be used for setting FingerKey output. See page 29 for more information.

Smart card: The Smart Card tab is used to manage iCLASS, DESFire and MiFare cards. See page 49 for more information.

Access: The Access tab lets you define access profiles. Access profiles control which readers different groups of people have access through. See page 61 for more information.

Database: The Database Tab is used to backup, restore, delete, detach and attach the database. See page 63 for more information.

Getting Around with the Keyboard

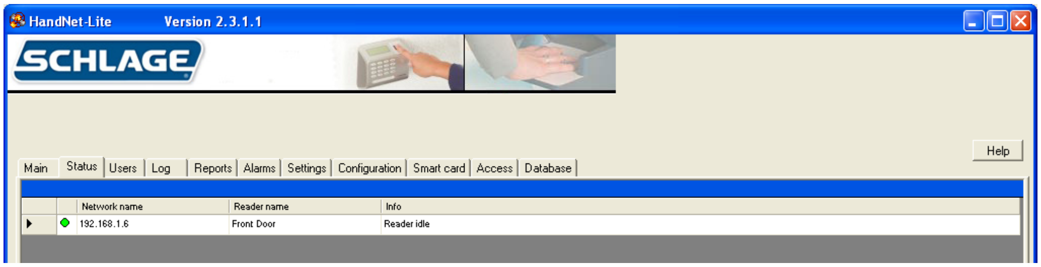
To move from tab to tab: Press ctrl tab.

To move from entry to entry with a tab: Press tab to move to the next entry, and shift tab to move to the previous entry.

Status Tab

The *Status* tab lists every network and reader that has been configured in HandNet Lite.

Figure 4-1: Status Tab



		Network name	Reader name	Info
▸	🟢	192.168.1.6	Front Door	Reader idle

Table 4-1: Reader Status

Column	Description
Status Indicator (untitled)	Indicates the current status of the reader
Network name	Name of the reader's network
Reader name	Name of the reader
Info	Details about the status of the reader's connection

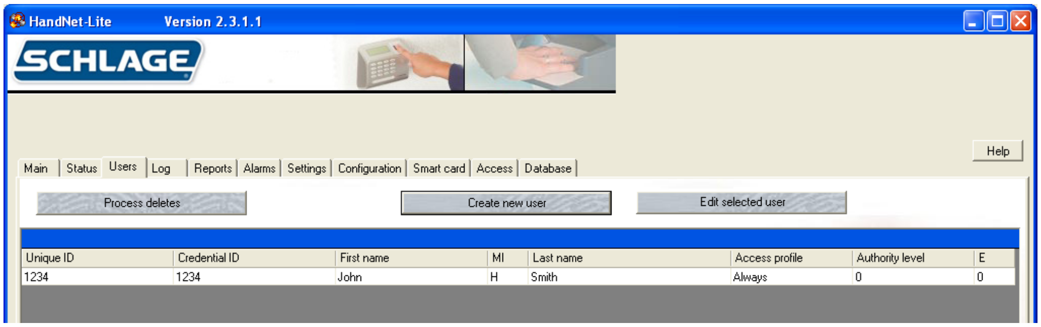
Click the heading of any row to sort the list by that heading. Click the heading again to reverse the sort order.

Table 4-2: Reader Status Indicators

Icon	Description	Additional Information
🟢	Reader is communicating	• Click the green icon to display download and conditionally upload user choices. • If the reader is a FingerKey you will have a Download (Download from PC to the reader) choice. • If the reader is a HandKey you will have both a Download (from the PC to the reader) and Upload (from the reader to the PC) choices.
○	Reader is not enabled	• Readers must be first created (see create new reader) and then enabled (see enable reader).
🔴	Reader is not communicating.	• The reader is not configured correctly, or is disconnected. • Click the red icon for further details.

Users Tab

The *Users* tab lists every user and is used to add or change users. Users are individuals who are enrolled in readers.



Unique ID	Credential ID	First name	MI	Last name	Access profile	Authority level	E
1234	1234	John	H	Smith	Always	0	0

List of Users

Table 5-3: List of Users

Column	Description
Unique ID	ID by which the user is identified in the database
Credential ID	ID the user enters at the reader in order to gain access
First Name	User’s first name
MI	User’s middle initial
Last Name	User’s last name
Access profile	Access profile that is associated with the user (See page 61 for more information.)
Authority Level	• Authority level for the user. • Zero (0) for most users, meaning the user can gain access through the reader, but not use the command menus in the reader to change settings. (See page 14 for more information.)
E	• Indicates enrollment status • Zero (0) indicates that the user is not enrolled. • One (1) indicates that a HandKey template has been captured for the user • Two (2) indicates that a FingerKey template has been captured for the user • Three(3) indicates that HandKey and FingerKey templates have been captured for the user.

Click the heading of any row to sort the list by that heading. Click the heading again to reverse the sort order.

Clicking on a user row will display actions that can be performed for that user.

Enroll Users

Users must be enrolled on a reader. For help enrolling users, see the reader's manual.

A user may be added to HandNet Lite in one of two ways:

- **Enroll the user at a reader before entering the user in HandNet Lite.** If the reader is connected, the user is automatically added to HandNet Lite. If users are enrolled in readers before they are connected to HandNet Lite, when the reader is initially connected to HandNet Lite, all users are imported then.

  If a user is enrolled first, the user ID in the reader (the Credential ID) is used in HandNet Lite for the user's First name, Last name, and Unique ID (an identifier used only by HandNet Lite to help distinguish users with similar names). Edit these entries by selecting the user in the Users window and clicking the Edit selected user button; see Edit Fingerprint Settings page 41.
- **Enter the user in HandNet Lite before enrolling the user in a connected reader.** Enter the user in the User edit window. See Add a User on page 11 for more information. The user will be listed as unenrolled in the Users window (denoted by a zero (0) in column E). See the User Fields table on page 13 for more information. When you enroll the user at a reader, HandNet Lite will import the finer template.

! NOTE *When enrolling users at the reader, you must completely leave the reader's command menus before HandNet Lite will detect the enrollments.*

Problems with User Enrollment

Since bypassing finger or hand recognition gives you reduced security, it should only be used as a last resort. Try these options first:

- The user might have placed the finger or hand badly during the initial enrollment.
  1. Remove the user from the reader.
  2. Instruct the user on correct finger or hand placement. Make sure the user is placing the right finger.
  3. Add the user again.

  This creates a new template for the user.
- If using a FingerKey, Remove the user, and enroll the user again using different fingers. Try the thumb if other fingers don't work
- If the user has a mild disability that prevents consistent finger or hand placement, change the user's reject level. See Biometric threshold on page 13 for more information. See the reader manual for instructions on how to set the appropriate reject setting for the user.

If these options aren't possible, or if you try them and they don't work, then check the Verify on ID only (no biometric verification) box on the User edit screen. See Verify on ID only on page 14 for more information

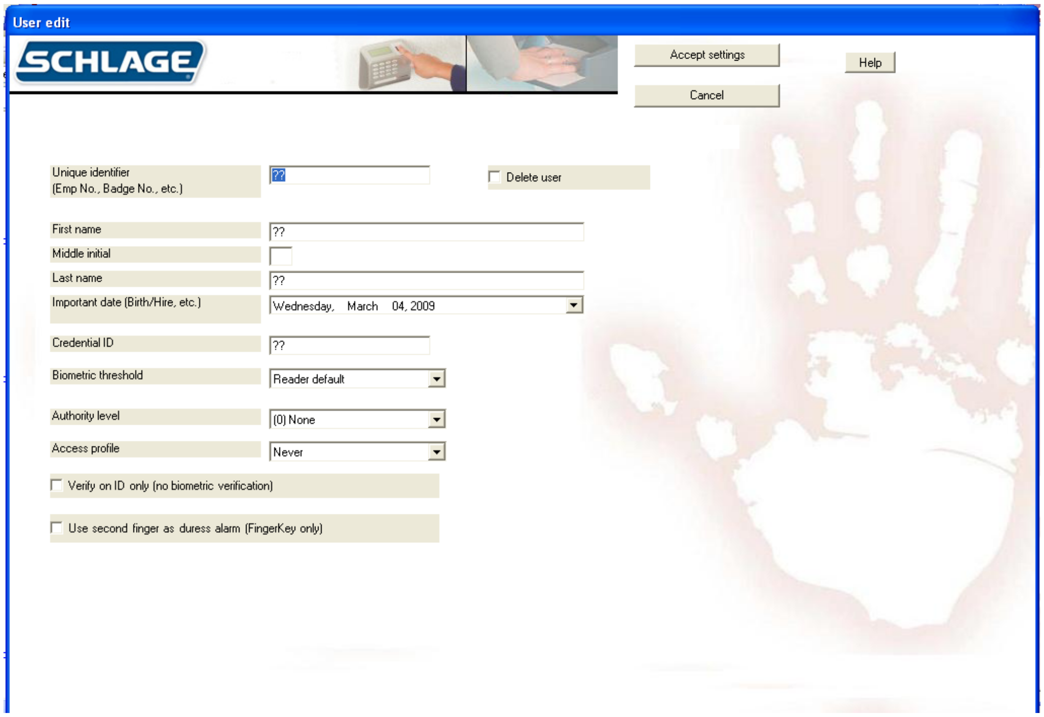
Adding a Special User

When using a FingerKey, if a user's fingerprint cannot be scanned (for any reason), the user can be added as a special user. Special users are still required to place a finger on the scanner, but the scanner does not try to match a finger template.

If a user has unrecognizable fingerprints, severe arthritis, or other conditions that keep the user's finger from being recognized, you can give the user access without finger recognition. If you choose this, the reader still asks the user to place a finger on the reader so it won't be apparent to others that finger recognition isn't required, but the reader doesn't check the finger template; it gives access regardless of whose finger is placed there.

Add a User

1. Click the *Users* tab.
2. Click the *Create new user* button.



Unique identifier (Emp No., Badge No., etc.)	??
□ Delete user	
First name	??
Middle initial	
Last name	??
Important date (Birth/Hire, etc.)	Wednesday, March 04, 2009
Credential ID	??
Biometric threshold	Reader default
Authority level	(0) None
Access profile	Never

□ Verify on ID only (no biometric verification)

□ Use second finger as duress alarm (FingerKey only)

3. Complete the fields on the screen. See the User Fields Table on page 13.
4. Click the *Accept Settings* button.
5. If the user has not been enrolled on a reader, do so now. See Enroll Users on page 10 for more information.

Edit a User

1. Click the *Users* tab.
2. Click to select the name of the user you want to edit.
3. Click the *Edit selected user* button.
4. Complete the fields on the screen. See the User Fields table on page 13 for more information.
5. Click the *Accept Settings* button..

Delete a User

1. Click the *Users* tab.
2. Click to select the name of the user you want to delete.
3. Click the *Edit selected user* button.
4. Click the *Delete user* check box.
5. Click the *Accept Settings* button.

Note: You can also edit, delete, and enroll an existing user by clicking on that user listed on the User's tab and selecting the desired action from the pop-up menu.

User Fields

Table 5-4: User Fields

Field	Req'd?	Description
Unique Identifier	Yes	• Up to 30 characters (any combination of letters, numbers, spaces, or special characters) • If user was added from the reader, will initially match credential ID in the reader but can be changed.
First Name	Yes	• User's first name • If user was added at the reader, will initially match the credential ID
Middle Initial	No	• User's middle initial
Last Name	Yes	• User's last name • If user was added at the reader, will initially match the credential ID
Important Date	No	• Used to distinguish between users with similar names • Type a date directly into the entry box using the format Thursday, January 01, 2009 • Click the drop-down button to select the date from a calendar.
Credential ID	Yes	• User's credential ID • ID number from user's card (when card readers are used) or the number a user enters manually at the reader. See the reader's manual for help with designing an ID numbering system.
Biometric Threshold	Yes	• Controls how closely user's finger or hand must match the stored template in order for access to be granted. • Reader default uses the Reject Threshold from the reader's setup. See Reject Threshold on pages 36 and 38 for more information. In most cases, Reader default is the appropriate choice. • To override the reader's reject threshold, choose from values of 30-250 in the drop down list (common values of 250, 150, 75, 50, and 30 are singled out at the top). • Use a lower number for higher security. • Use a higher number if a user has trouble gaining access. See the reader's manual for more information.
Authority Level	Yes	• Determines what menus the user can access at the reader. • Each level gives access to all the lower levels. • See the Authority Levels table on page 14 for more information.
Access Profile	Yes	• Controls which readers the user can use. • Always allows access to all readers. • Never blocks access to all readers. • Additional choices correspond to the profiles configured in the Access tab. See Access Tab on page 61 for more information.

Field	Req'd?	Description
Verify on ID only (no biometric verification)	No	• Check for users who fingerprints or hand cannot be scanned • Since bypassing finger or hand recognition gives you reduced security, only use this as a last resort. See Adding a Special User on page 11 for more information.
Use Second Finger as Duress Alarm (FingerKey only)	No	• When checked, user's second finger will be used as a duress indicator.
Delete User	No	• Check to delete user from HandNet Lite. • User will be deleted from HandNet Lite and from all connected readers when you click the *Accept* button.

Authority Levels

Table 5-5: Authority Levels

Authority Level	Description
(0) None:	• Allows user to gain access through the reader, but not use the command menus in the reader to change the reader's settings. • This choice is appropriate for most users.
(1) Service:	• Allows the master reader to display the status of all readers on the network. • Not relevant on readers that are not configured as a master.
(2) Setup:	• Allows user to control reader setup • See reader's manual for more information.
(3) Management:	• Allows user to list all of the users in the reader • Allows master reader to send/acquire user databases to/from readers in a network.
(4) Enrollment:	• Allows user to add or remove users.
(5) Security:	• Allows user to modify security settings • See reader's manual for more information.

See the reader's manual for information on directly changing settings through the reader.

Process Deletes Button

When the Process Deletes button is pressed, HandNet-Lite looks for a RemoveUserXML. Xml file in the root directory of the C: Drive.   If this file is found, any users listed in that file will be removed from Handnet-lite.   Figure 3.1 provides a sample C:\RemoveUserXML. Xml file which would remove users with UserIDs of 1000, 1001, 1002, 1003, and 1004 when the Process Deletes button is pressed.

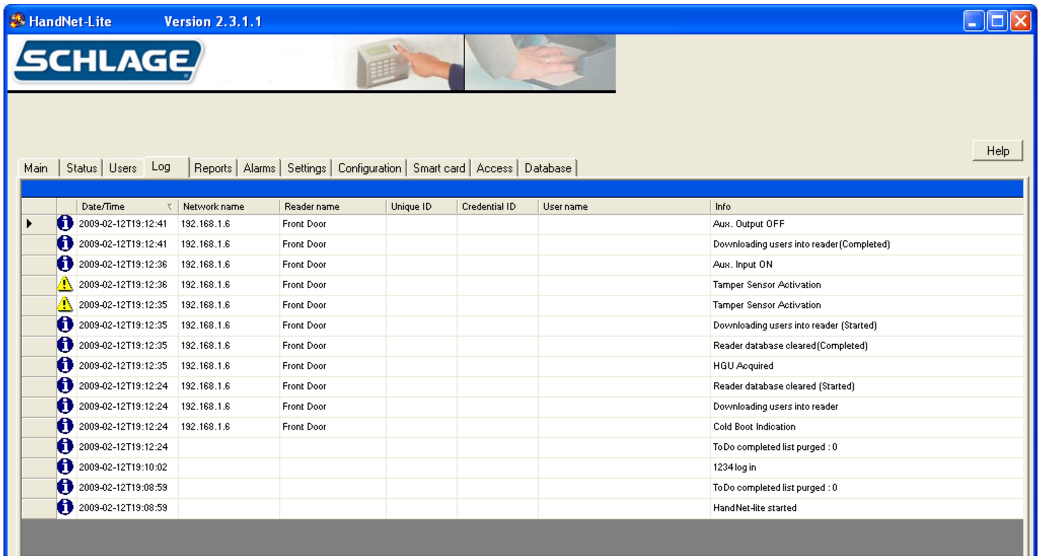
Figure 5-1: Example of RemoveUserXML.xml

```
<?xml version=”1.0” standalone=”yes”?>
<RemoveUser xmlns=”http://tempuri.org/RemoveUser.xsd”>
 <CRsiRemoveUser>
  <UserID>1000</UserID>
 </CRsiRemoveUser>
 <CRsiRemoveUser>
  <UserID>1001</UserID>
 </CRsiRemoveUser>
 <CRsiRemoveUser>
  <UserID>1002</UserID>
 </CRsiRemoveUser>
 <CRsiRemoveUser>
  <UserID>1003</UserID>
 </CRsiRemoveUser>
 <CRsiRemoveUser>
  <UserID>1004</UserID>
 </CRsiRemoveUser>
 <CRsiRemoveUser>
  <UserID>1005</UserID>
 </CRsiRemoveUser>
</RemoveUser>
```

Log Tab

The *Log* tab lists events that occur in any connected reader. It also lists any changes made in HandNet Lite.

Figure 6-1: Log Tab



	Date/Time	Network name	Reader name	Unique ID	Credential ID	User name	Info
ℹ	2009-02-12T19:12:41	192.168.1.6	Front Door				Aux. Output OFF
ℹ	2009-02-12T19:12:41	192.168.1.6	Front Door				Downloading users into reader(Completed)
ℹ	2009-02-12T19:12:36	192.168.1.6	Front Door				Aux. Input ON
⚠	2009-02-12T19:12:36	192.168.1.6	Front Door				Tamper Sensor Activation
⚠	2009-02-12T19:12:35	192.168.1.6	Front Door				Tamper Sensor Activation
ℹ	2009-02-12T19:12:35	192.168.1.6	Front Door				Downloading users into reader (Started)
ℹ	2009-02-12T19:12:35	192.168.1.6	Front Door				Reader database cleared(Completed)
ℹ	2009-02-12T19:12:35	192.168.1.6	Front Door				HGU Acquired
ℹ	2009-02-12T19:12:24	192.168.1.6	Front Door				Reader database cleared (Started)
ℹ	2009-02-12T19:12:24	192.168.1.6	Front Door				Downloading users into reader
ℹ	2009-02-12T19:12:24	192.168.1.6	Front Door				Cold Boot Indication
ℹ	2009-02-12T19:12:24						ToDo completed list purged : 0
ℹ	2009-02-12T19:10:02						1234 log in
ℹ	2009-02-12T19:08:59						ToDo completed list purged : 0
ℹ	2009-02-12T19:08:59						HandNet-lite started

Log Tab Fields

Table 6-6: Log Tab Fields

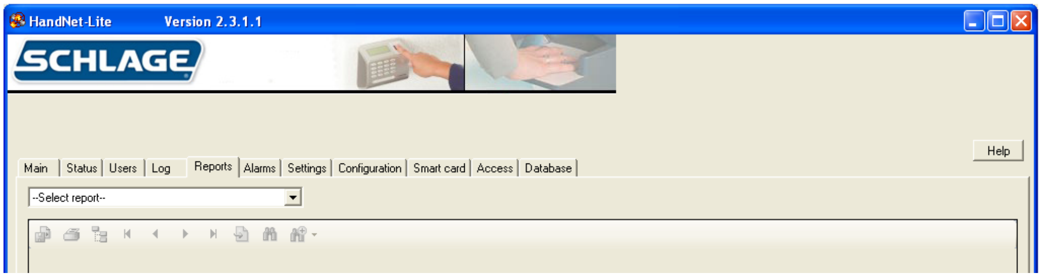
Column	Description
Event type (untitled)	One of the following icons: ℹ: Indicates a standard informational message. ⚠: Indicates that the condition is important and warrants further investigation. These conditions are also listed on the Alarms tab.
Date/Time	Shows the date and time when the event occurred. The date is listed in year-month-day order, and the time lists hours:minutes:seconds
Network name	Network name if activity occurred at a reader
Reader name	Reader name if activity occurred at a reader
Unique ID	User's unique ID if event is associated with a particular user
Credential ID	User's credential ID if event is associated with a particular user
User name	User's name if message is event with a particular user
Info	Explanation of event

Click the heading of any row to sort the list by that heading. Click the heading again to reverse the sort order.

Reports Tab

The Reports tab is used to generate and view reports on users and readers.

Figure 7-1: Reports Tab


HandNet-Lite Version 2.3.1.1
SCHLAGE
Help
Main | Status | Users | Log | Reports | Alarms | Settings | Configuration | Smart card | Access | Database
--Select report--

Generate a Report

1. Click the *Reports* tab.
2. Click the drop-down list at the top of the reports tab and choose the report you want to generate.

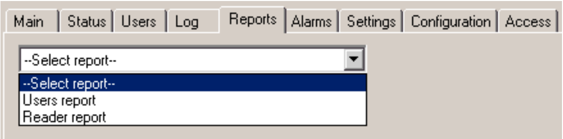
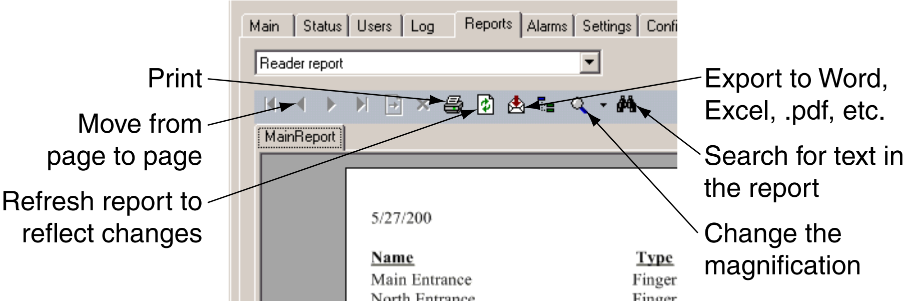

Main | Status | Users | Log | Reports | Alarms | Settings | Configuration | Access
--Select report--
--Select report--
Users report
Reader report

Table 7-7: Report Types

Report Type	Description
Users Report	Lists key information about every user in the system
Readers Report	Lists key information about every reader in the system

3. To print or move around in the report, click the corresponding icon in the bar above the report window.

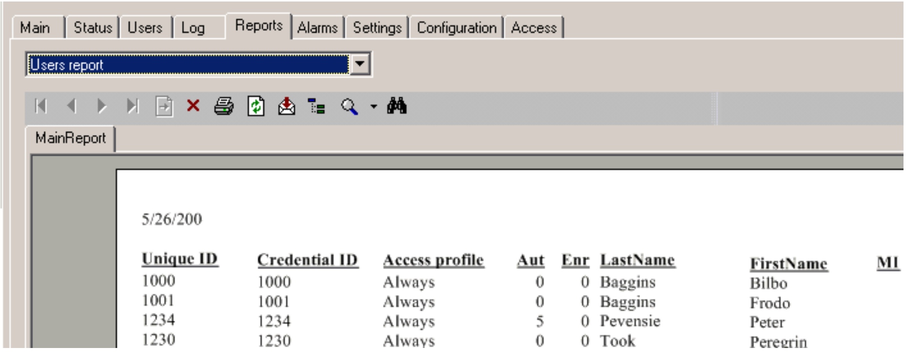

Main | Status | Users | Log | Reports | Alarms | Settings | Confi
Reader report
MainReport
Print
Move from page to page
Refresh report to reflect changes
Export to Word, Excel, .pdf, etc.
Search for text in the report
Change the magnification

5/27/200

Name	Type
Main Entrance	Finger
North Entrance	Finger

Users Report

The Users report lists the information for each user in the program.



5/26/200

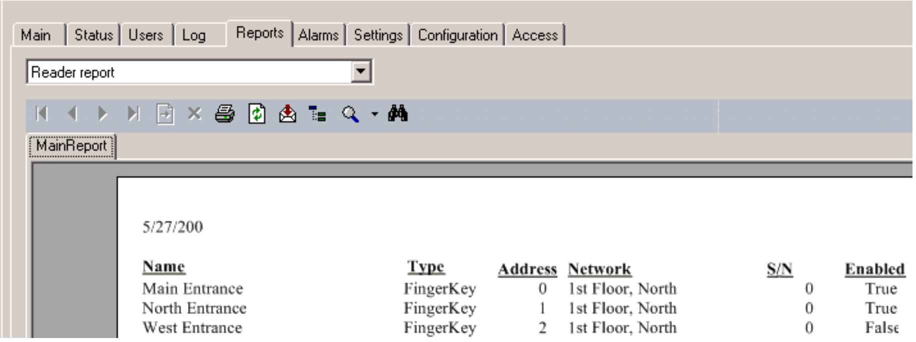
Unique ID	Credential ID	Access profile	Aut	Enr	LastName	FirstName	MI
1000	1000	Always	0	0	Baggins	Bilbo	
1001	1001	Always	0	0	Baggins	Frodo	
1234	1234	Always	5	0	Pevensie	Peter	
1230	1230	Always	0	0	Took	Peregrin	

Table 7-8: Users Report

Column	Description
Unique ID	User’s Unique identifier
Credential ID	User’s credential ID (card or manual ID)
Access Profile	Access profile associated with the user
Aut	User’s authority level
LastName	• User’s last name • If you added the user at the reader and have not changed the name, user ID is listed
FirstName	• User’s first name • If you added the user at the reader and have not changed the name, user ID is listed
MI	User’s middle initial.

Reader Report

The Reader report lists information for each reader in the program.



5/27/200

Name	Type	Address	Network	S/N	Enabled
Main Entrance	FingerKey	0	1st Floor, North	0	True
North Entrance	FingerKey	1	1st Floor, North	0	True
West Entrance	FingerKey	2	1st Floor, North	0	False

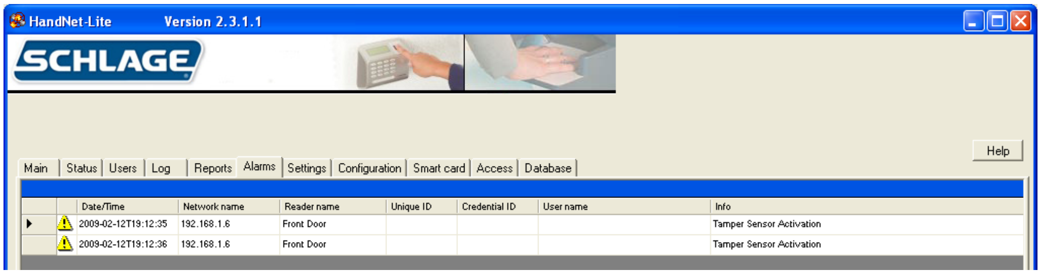
Table 7-9: Reader Report

Column	Description
Name	Reader's name
Type	Indicates whether the reader is a hand or fingerprint reader
Address	Reader's address
Network	Network to which reader is connected
S/N	Reader's internal serial number
Enabled	• true: program attempts to communicate with the reader • false: program does not attempt to communicate with the reader

Alarms Tab

The *Alarms* tab shows all alarms that have been recorded in the system. Alarms are also listed with the rest of the activity in the *Log* tab

Figure 8-1: Alarms Tab



	Date/Time	Network name	Reader name	Unique ID	Credential ID	User name	Info
▶ ⚠	2009-02-12T19:12:35	192.168.1.6	Front Door				Tamper Sensor Activation
⚠	2009-02-12T19:12:36	192.168.1.6	Front Door				Tamper Sensor Activation

Alarms Fields

Table 8-10: Alarms Fields

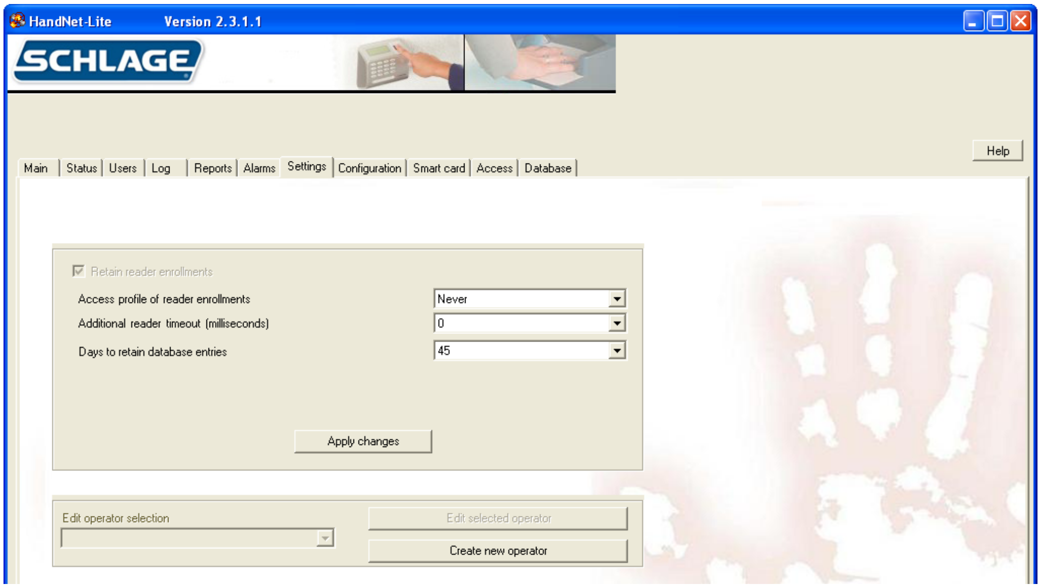
Column	Description
Date/Time	Date and time when the alarm occurred. The date is listed in year-month-day order, and the time lists hours:minutes:seconds
Network name	Network name if alarm is associated with a particular reader
Reader name	Reader name if alarm is associated with a particular reader
Unique ID	User's unique ID if alarm is associated with a particular user
Credential ID	User's credential ID if alarm is associated with a particular user
User name	User's name if alarm is associated with a particular user
Info	Description of alarm

Click the heading of any row to sort the list by that heading. Click the heading again to reverse the sort order.

Settings Tab

The *Settings* tab allows you to set default settings and add operators to the system.

Figure 9-1: Settings Tab



☑ Retain reader enrollments

Access profile of reader enrollments: Never

Additional reader timeout (milliseconds): 0

Days to retain database entries: 45

Edit operator selection

Settings Fields

Table 9-11: Settings Fields

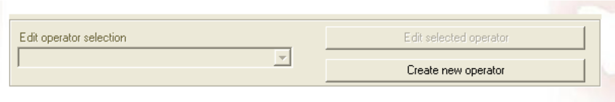
Setting	Description
Retain reader enrollments	This box is always checked and cannot be changed.
Access profile of reader enrollments	• Access profile assigned to users by default when users are added at a reader before being added in the system. • Choices are Always, Never or any custom profiles created by an operator. See Access Tab on page 61 for more informaiton.
Additional reader timeout	• Additional time that is added globally to the command timeout. • Select additional time if command timeout errors are generated on the network. These errors would be displayed on the Alarms tab. See Alarms Tab on page 23 for more information.
Days to retain expired database entries	• Number of days expired database entries are retained • Choose default of 45 days initially. If database becomes too large, make this number smaller.

Managing Operators

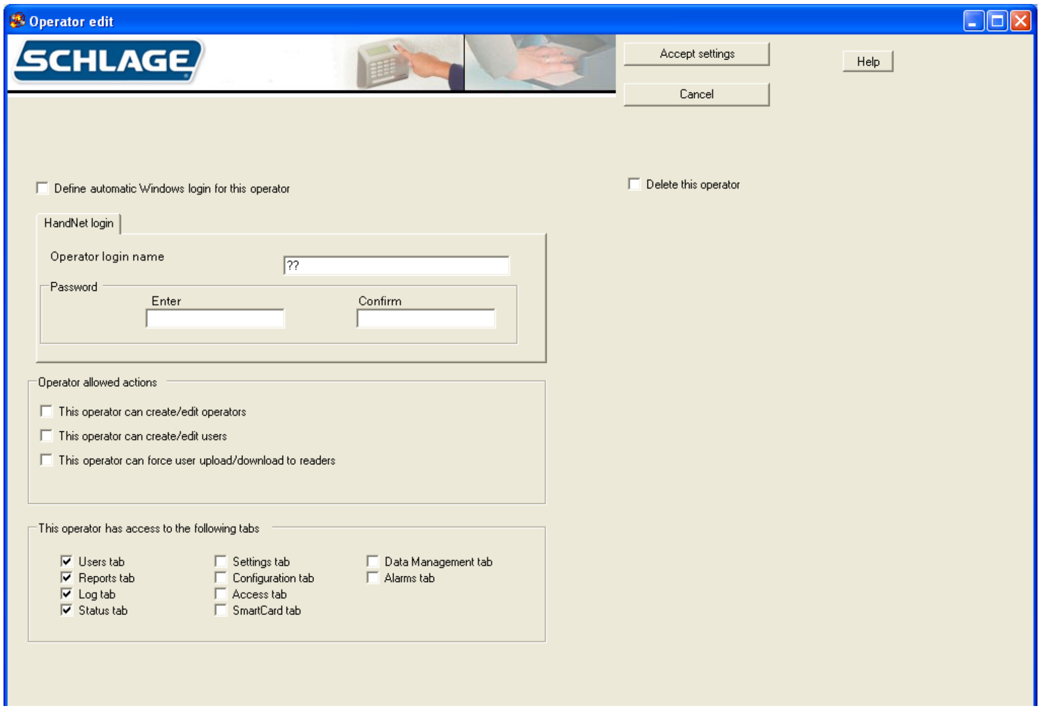
Operators are individuals who can control the system. The level of control can be set individually for each operator.

Add a New Operator

1. Click the *Settings* tab.
2. Click the *Create new operator* button.



The Operator edit screen will appear:



☐ Delete this operator

☐ Define automatic Windows login for this operator

HandNet login

Operator login name: ??

Password

Enter

Confirm

Operator allowed actions

☐ This operator can create/edit operators

☐ This operator can create/edit users

☐ This operator can force user upload/download to readers

This operator has access to the following tabs

☑ Users tab	☐ Settings tab	☐ Data Management tab
☑ Reports tab	☐ Configuration tab	☐ Alarms tab
☑ Log tab	☐ Access tab	
☑ Status tab	☐ SmartCard tab	

3. Click the *Define automatic Windows login for this operator* box to use Windows login information for this operator. See Enable Automatic Windows Login 27.
4. Enter a login name in the operator login name box. This name is case sensitive.
5. Enter the password and confirmation in the enter and confirm boxes. The password is case sensitive.
6. Choose the operator allowed actions by clicking the corresponding check box(es).
7. Choose the tabs to which the operator has access by clicking the corresponding check box(es).
8. Click the *Accept Settings* button.

Edit an Operator

1. Click the *Settings* tab.
2. Select the operator you want to edit from the *Edit operator selection* drop-down box.
3. Click *Edit selected operator* button.
4. Edit the necessary settings. See Add a New Operator on page 26 for more information.
5. Click the *Accept Settings* button.

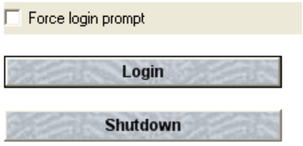
Delete an Operator

1. Click the *Settings* tab.
2. Select the operator you want to delete from the *Edit operator selection* drop-down box.
3. Click the *Delete this operator* check box.
4. Click the *Accept Settings* button.

Enable Automatic Windows Login

If you wish to allow automatic Windows login for HandNet Lite:

1. Click the *Main* tab.
2. Log off.
3. Click to un-check the *Force login prompt* checkbox.
4. Shut down HandNet Lite. The next time you start HandNet Lite, you will be automatically logged in.



□ Force login prompt

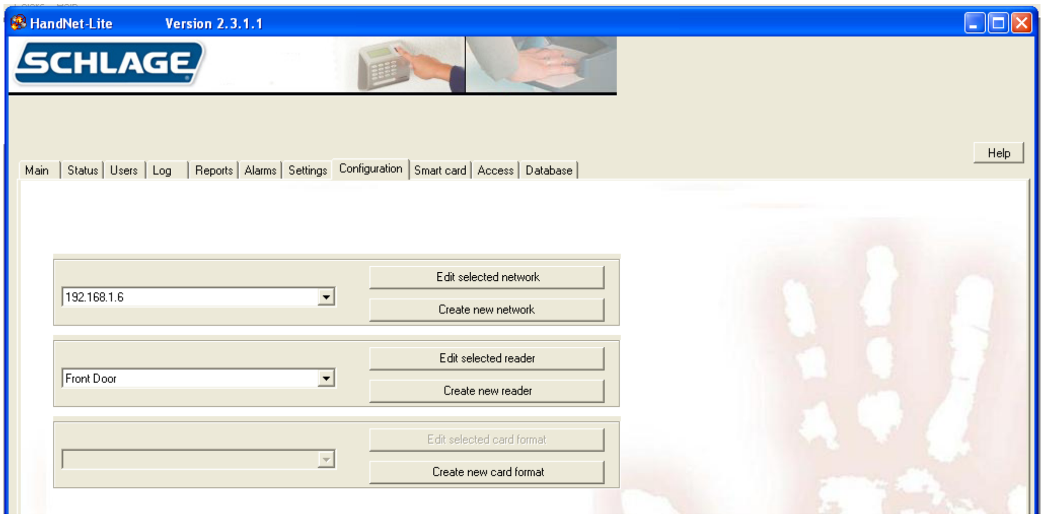
Disable Automatic Windows Login

1. Click the *Main* tab
2. Log off.
3. Click to check the *Force login prompt* checkbox.
4. Shut down HandNet Lite. The next time you start HandNet Lite, you will be prompted for login name and password.

Configuration Tab

The *Configuration* tab is used to add or edit networks, readers and card formats.

Figure 10-1: Configuration Tab



192.168.1.6

Front Door

Managing Networks

A network is a group of up to 32 daisy-chained readers connected though a single serial port using 2 wire RS485, a single reader connected to a computer with RS232, or a single TCP/IP (ethernet) reader. (See the reader manual for wiring and connection detail.)

You control access to each reader separately using HandNet Lite, so having readers with unrelated purposes in one network is fine.

There are two parts to setting up a network and readers: you must physically set the readers up and connect them to each other and to the computer, and you must add the network and readers in HandNet Lite. This manual only explains how to set up the network and readers in HandNet Lite. For help setting up and connecting the readers, see the manual that came with the readers.

Add a Network

1. Click the *Configuration* tab.
2. Click the *Create new network* button
3. Choose the Network type from the drop-down box. The remaining fields displayed will be determined by this selection.
4. Complete the fields on the screen. See page 30 for TCP/IP network. See page 32 for Serial network.
5. Click *Accept settings*.

Edit a Network

1. Click the *Configuration* tab.
2. Select the network you want to edit from the drop-down box.
3. Click the *Edit selected network* button
4. Complete the fields on the screen. See page 30 for TCP/IP network. See page 32 for Serial network.
5. Click *Accept settings*.

Delete a Network

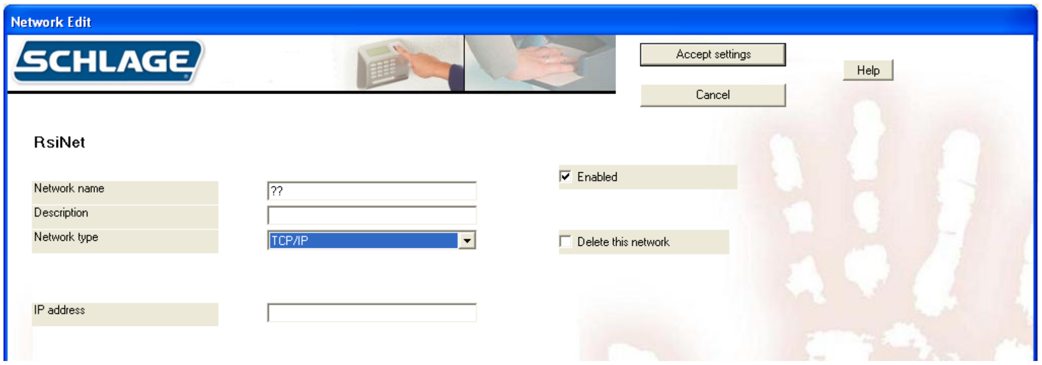
Only networks with no readers can be deleted.

1. Click the *Configuration* tab.
2. Select the network you want to delete from the drop-down box.
3. Click the *Edit selected network* button
4. Click the *Delete this network* check box.
5. Click *Accept settings*.

Connecting through a TCP/IP network

To connect to a site through the network, you must have a TCP/IP network with static IP addresses. Your computer must have a network card and be connected to the network. If the network is faster than 10baseT, you must have a switching hub. To use TCP/IP, you must have either ordered readers with the Ethernet option enabled or purchased an Ethernet upgrade.

Figure 10-2: Edit a TCP/IP Network



RsiNet

Network name: ??

Description:

Network type: TCP/IP

IP address:

☑ Enabled

□ Delete this network

Table 10-12: TCP/IP Network Fields

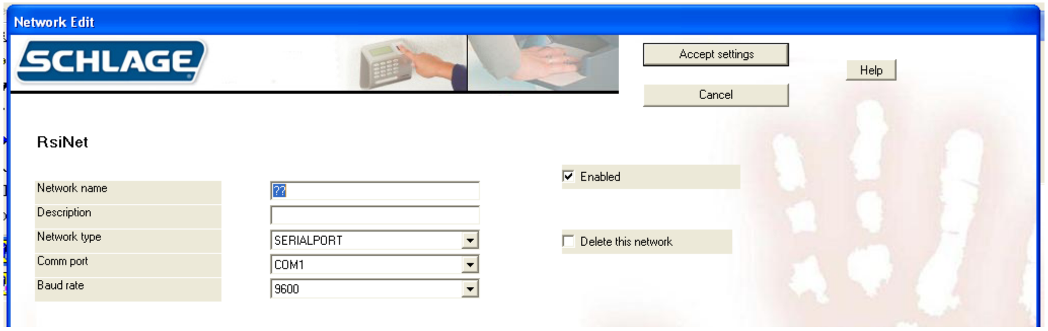
Field	Req'd?	Description
Network Name	Yes	• Name of the network • Any combination of letters, numbers, spaces, and special characters, up to 30 characters long
Description	No	Brief description of the network

Field	Req'd?	Description
Enabled	No	• Must be checked for HandNet Lite to communicate with the network and monitor any readers connected to it. • Generally you would only uncheck this if you were in the process of setting up or reconfiguring the network and didn't want the program to try to communicate • Having the Enabled box checked if the network isn't really connected to HandNet Lite causes the program to slow down significantly. Make sure that this is only checked if the network is actually set up and connected
Delete This Network	No	• Check to delete this network and remove it from the Schlage Biometrics network selection list. If there are no readers in the network, it will be deleted when you click Accept settings. • You can't delete a network with readers on it
Network Type	Yes	• Choose Serial port or TCP/IP • The remaining fields will be determined by this selection.
IP address	Yes	• Only available if TCP/IP was chosen in the Network type field. • The IP address (xxx.xxx.xxx.xxx) of the reader • Must match the IP address set in the reader. See the reader manual for more information • Ask your network administrator for an appropriate address

Connecting through a serial port

To connect to a site by running a cable from your computer to the reader, you must have a free serial port on your computer. See the reader manual for more on the requirements for the cable.

Figure 10-3: Serial Network Edit Screen



RsiNet

Network name	??
Description	
Network type	SERIALPORT
Comm port	COM1
Baud rate	9600

☑ Enabled

☐ Delete this network

Table 10-13: Serial Network Fields

Field	Req'd?	Description
Network Name	Yes	• Name of the network • Any combination of letters, numbers, spaces, and special characters, up to 30 characters long
Description	No	• Brief description of the network
Enabled	No	• Must be checked for the system to communicate with the network and monitor any readers connected to it. • Uncheck when in the process of setting up or reconfiguring the network to keep the program from trying to communicate • If checked when the network is not really connected, the system will slow down significantly.
Delete This Network	No	• Check to delete this network and remove it from the network selection list. • You cannot delete a network with readers in it
Network Type	Yes	• Choose Serial port or TCP/IP • The remaining fields will be determined by this selection.
Comm Port	Yes	• Only available if Serial port was chosen in the Network type field. • Must match the serial port to which the reader is connected • Only the ports that are currently available on your computer are listed.

Field	Req'd?	Description
Baud Rate	Yes	• Only available if Serial port was chosen in the Network type filed. • Choose from values of 4800, 9600, 19200, 28800, 38400, or 57600. • Choose 9600 initially. Increase the rate after a working connection has been established. Longer wire distances require lower rates. • Must match the rate set in all readers on the network. See the reader manual for more information.

Managing Readers

There are two parts to setting up readers: physically setting up the readers and connecting them to each other and to the computer, and adding the network and readers in HandNet Lite. This manual only explains adding the network and readers in HandNet Lite. For help setting up and wiring readers, see the manual that came with the readers.

Before you add readers, you must set up the network to which they are connected. See Add a Network on page 29 for more information.

If You've Been Using Readers Already

If you've been using readers without HandNet Lite, when you add the network and readers to the system, HandNet Lite automatically gets the users from the readers and adds them to the system; see How Users Are Enrolled and Added to HandNet Lite on page 39.

Add a Reader

1. Click the *Configuration* tab.
1. Select the network in which the new reader will exist from the network drop-down box.
2. Click the *Create new reader* button.
3. Choose the *Reader type* from the drop-down box. The entries on the screen will differ depending on the reader type chosen.
4. Fill in the entries on the Reader Edit screen. See page 35 for FingerKey. See page 37 for HandKey.
5. Click the *Test reader* button. If the reader is properly configured, the reader will be able to communicate.
6. To change the security settings for the reader, click the *Security settings* button. See Security Settings Screen on page 40 for more information.
7. If you are editing a FingerKey and want to edit the fingerprint settings, click the *Fingerprint settings* button. See Fingerprint Settings Screen on page 41 for more information.
8. Click the *Accept settings* button.

Edit a Reader

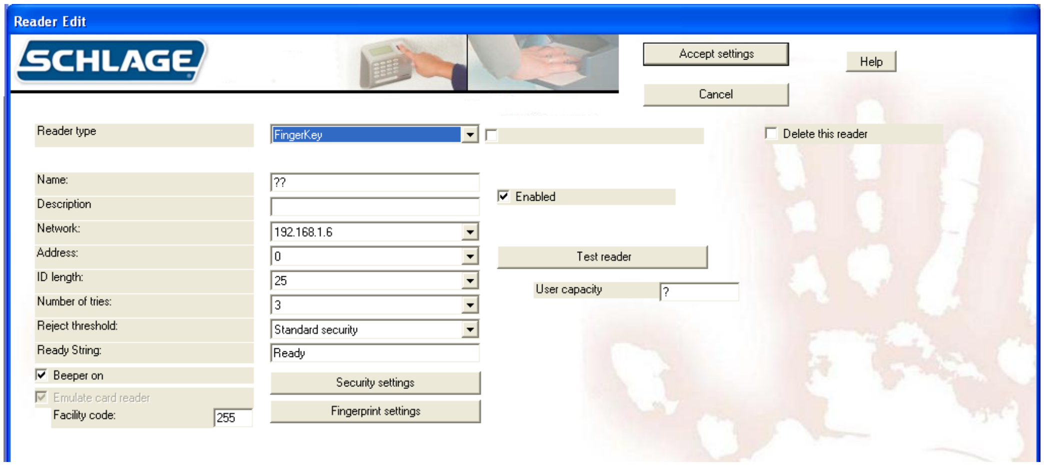
1. Click the *Configuration* tab.
1. Select the network in which the reader you want to edit exists in the network drop-down box.
2. Click the *Edit selected reader* button.
3. The entries on the screen will differ depending on the reader type chosen.
4. Fill in the entries on the Reader Edit screen. See page 35 for FingerKey. See page 37 for HandKey.
5. Click the *Test reader* button. If the reader is properly configured, the reader will be able to communicate.
6. To change the security settings for the reader, click the *Security settings* button. See Security Settings Screen on page 40 for more information.
7. If you are editing a FingerKey and want to edit the fingerprint settings, click the *Fingerprint settings* button. See Fingerprint Settings Screen on page 41 for more information.
8. Click the *Accept settings* button.

Delete a Reader

1. Click the *Configuration* tab.
1. Select the network in which the reader you want to delete exists in the network drop-down box.
2. Click the *Edit reader* button.
3. Click the *Delete this reader* check box.
4. Click the *Accept settings* button.

FingerKey Reader Edit Screen

Figure 10-4: FingerKey Reader Edit Screen



Reader type: FingerKey

Name: ??

Description:

Network: 192.168.1.6

Address: 0

ID length: 25

Number of tries: 3

Reject threshold: Standard security

Ready String: Ready

User capacity: ?

☑ Beeper on

☑ Emulate card reader

Facility code: 255

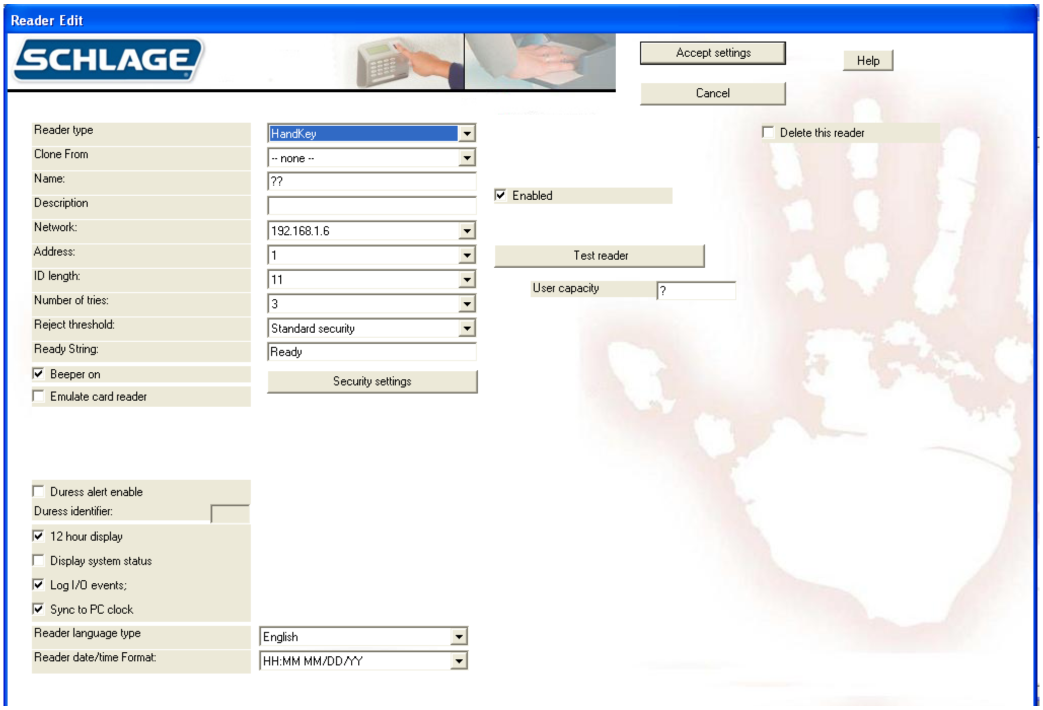
Table 10-14: FingerKey Reader Fields

Field	Req'd?	Description
Clone From	No	• Appears only after at least one reader has been configured. • Allows you copy the settings from another reader, including the underlying Fingerprint and Security Settings. • If this option is chosen, all of the following fields will be populated automatically.
Name	Yes	Any combination of letters, numbers, spaces, and special characters, up to 30 characters.
Description	No	Briefly describe the reader.
Network	Yes	• Select the network in which the reader exists. • Network must be set up before you can add the reader. See Add a Network on page 29 for more information.
Address	Yes	• Must match the address set in the reader. See the reader's manual for information on setting the address in the reader. • Field will be automatically populated with the first available address that hasn't been used. Choose another number from the pull-down list if desired. • Changing the address on this screen does NOT change the address in the physical reader. If you change an address here, you must also change the address in the reader.
ID Length	No	• If all user IDs are the same length, choose the number of digits here (any value from 1-25) so users don't have to press enter after typing the ID at the reader. • If user IDs are different lengths, choose the longest number of digits. Users with the longest IDs will not have to press ENTER after typing the ID at the reader. • Entry does not affect the length of IDs on cards. It only affects IDs entered at the keypad.

Field	Req'd?	Description
Number of Tries	Yes	• Controls how many times the user can try to get access before the reader will block the user's ID and not allow further tries. • Prevents someone from making repeated tries to gain access with someone else's ID. • Normally 3 is a good setting.
Reject threshold	Yes	• The lower this number is, the more closely the user's finger must match the template of the finger stored in the FingerKey. • 30 (the lowest possible number) requires the fingerprint to match very closely; 250 (the highest possible number) will grant access if the finger match is close but not exactly the same. • 75 is good for most contexts. Choose a lower number if you have an especially high security situation. • If particular users have trouble placing their fingers consistently, you can override the reader's setting for an individual user on the User edit screen in the Users window. See Edit a User on page 12 for more information.
Ready String	Yes	• This text appears in the reader display when the reader is ready and waiting for the user to enter an ID. • Any combination of letters, numbers, spaces, and special characters, up to 20 characters
Beeper On	No	• When checked, the reader beeps each time you press a button • In a high security setting, you might want the beeps off to make it harder for a casual observer to figure out how many digits are in the ID number.
Emulate Card Reader	Yes	• FingerKey readers always emulate a card reader, so you can't uncheck this box
Facility Code	Yes	• Facility code that should be passed to the access control panel. • Numeric value from 0 (zero) to 65535
Enabled	No	• Check if the reader is physically set up and ready to be used. • Checking the Enabled box if the reader is not really connected slows the program down significantly. Make sure this is only checked if the reader is actually set up and connected
User capacity	Yes	• Will be filled in automatically by the reader.
Delete This Reader	No	• Check ONLY to delete reader and remove it from the reader selection list.

HandKey Reader Edit Screen

Figure 10-5: HandKey Reader Edit Screen



Reader Edit

Reader type: HandKey
Clone From: -- none --
Name: ??
Description:
Network: 192.168.1.6
Address: 1
ID length: 11
Number of tries: 3
Reject threshold: Standard security
Ready String: Ready
☑ Beeper on
☐ Emulate card reader
☐ Duress alert enable
Duress identifier:
☑ 12 hour display
☐ Display system status
☑ Log I/O events;
☑ Sync to PC clock
Reader language type: English
Reader date/time Format: HH:MM MM/DD/YY
☐ Delete this reader
☑ Enabled
User capacity: ?

Table 10-15: HandKey Reader Fields

Field	Req'd?	Description
Clone From	No	• Appears only after at least one reader has been configured. • Allows you copy the settings from another reader, including the underlying Fingerprint and Security Settings. • If this option is chosen, all of the following fields will be populated automatically.
Name	Yes	Any combination of letters, numbers, spaces, and special characters, up to 30 characters.
Description	No	Briefly describe the reader. You may leave this blank if you wish
Network	Yes	• Select the network in which the reader exists. • Network must be set up before you can add the reader. See Add a Network on page 29 for more information.

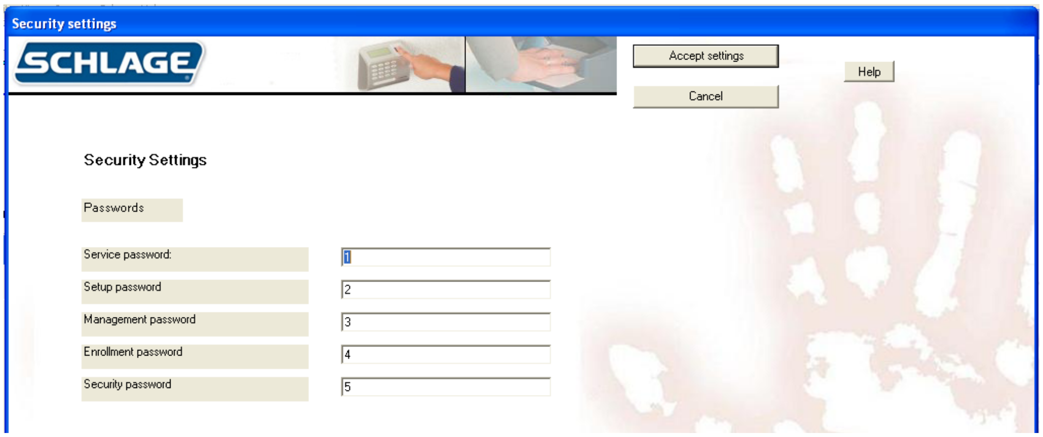
Field	Req'd?	Description
Address	Yes	• Must match the address set in the reader. See the reader's manual for information on setting the address in the reader. • Field will be automatically populated with the first available address that hasn't been used. • Choose another number from the pull-down list if desired. • Changing the address on this screen does NOT change the address in the physical reader. If you change an address here, you must set the reader to the same address or the program won't be able to communicate with the reader
ID Length	No	• If all user IDs are the same length, choose the number of digits here (any value from 1-25) so users don't have to press enter after typing the ID at the reader. • If user IDs are different lengths, choose the longest number of digits. Users with the longest IDs will not have to press ENTER after typing the ID at the reader. • Entry does not affect the length of IDs on cards. It only affects IDs entered at the keypad.
Number of Tries	Yes	• Controls how many times the user can try to get access before the reader will block the user's ID and not allow further tries. • Prevents someone from making repeated tries to gain access with someone else's ID. • Normally 3 is a good setting.
Reject threshold	Yes	• The lower this number is, the more closely the user's finger must match the template of the finger stored in the FingerKey. • 30 (the lowest possible number) requires the fingerprint to match very closely; 250 (the highest possible number) will grant access if the finger match is close but not exactly the same. • 75 is good for most contexts. Choose a lower number if you have an especially high security situation. • If particular users have trouble placing their fingers consistently, you can override the reader's setting for an individual user on the User edit screen in the Users window. See Edit a User on page 12 for more information.
Ready String	Yes	• This text appears in the reader display when the reader is ready and waiting for the user to enter an ID. • Any combination of letters, numbers, spaces, and special characters, up to 20 characters

Field	Req'd?	Description
Beeper On	No	• When checked, the reader beeps each time you press a button • In a high security setting, you might want the beeps off to make it harder for a casual observer to figure out how many digits are in the ID number.
Emulate Card Reader	Yes	• Controls the Output Mode of teh reader (Lock Output mode if unchecked, Card Reader Emulation Output if checked).
Enabled	No	• Check if the reader is physically set up and ready to be used. • Checking the Enabled box if the reader is not really connected slows the program down significantly. Make sure this is only checked if the reader is actually set up and connected
User capacity	Yes	• Contains the number of users the reader is capable of storing (this field is filled in after the Test Reader button is pressed)
Delete This Reader	No	• Check ONLY to delete reader and remove it from the reader selection list.
Duress alert enable	No	• If checked, duress activates AUX output
Duress identifier	No	• This is the key which, when pressed, will generate the DURESS event. • Must be a digit 0 through 9. Other values will disable the duress feature.
12 hour display	No	• If checked, displays terminal time in 12 hour format, otherwise 24 hour time format.
Display system status	No	• If checked, the reader's LCD will display system status on line 2. If unchecked, line 2 of the LCD will display the unit's date and time.
Log I/O events	No	• Currently ignored by HandKey units, I/O Events will always generate a DataLog
Sync to PC clock	No	• The reader's clock will be synchronized to this PC's system time.
Reader language type	No	• Selects the language used on the reader for LCD prompts.
Reader date/time Format	No	• Selects the format that the reader will display date & time on the LCD display.

Security Settings Screen

The Security Settings Screen controls the passwords needed to access the menus in the reader.

Figure 10-6: Security Settings Screen



Security Settings

Passwords

Service password: 1

Setup password 2

Management password 3

Enrollment password 4

Security password 5

Generally the default passwords shown above are adequate since a user must be set up with the appropriate Authority level on the User edit screen in the Users window (see page 12 for more information), and the user must know how to get to these menus in the reader before the passwords below would do any good.

Edit Security Settings

1. Click the *Configuration* tab.
2. Select the network in which the reader you want to edit exists in the network drop-down box.
3. Select the reader you want to edit from the reader drop-down box.
4. Click the *Edit selected reader* button.
5. Click the *Security settings* button.
6. Edit the passwords. See the Security Settings Fields Table on page 40 for more information.
7. Click the *Accept settings* button.

Table 10-16: Security Settings Fields

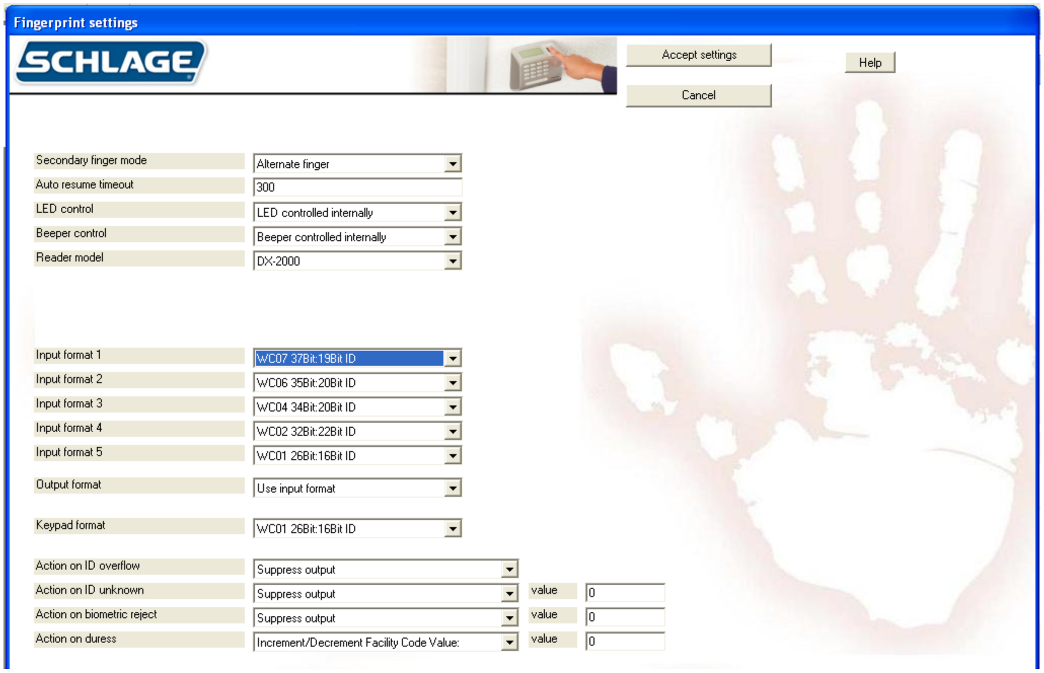
Field	Req'd	Description
Service	Yes	Allows the master reader display the status of all readers on the network
Setup	Yes	Controls reader setup including the reader's address, ID length, auxiliary output settings, facility codes, network configuration, the duress indicator, etc. It also contains an option to upgrade the maximum number of users
Management	Yes	Allows display of a list all of the users in the reader and lets the master reader send/acquire user databases to/from readers in a network
Enrollment	Yes	Allows you to add or remove users
Security	Yes	Allows you to customize user settings, control how closely user fingerprints must match templates, set the menu passwords, clear all the users from reader, etc

For more detail on the reader menus, see the reader manual.

Fingerprint Settings Screen

The Fingerprint Settings screen controls a number of the reader's internal settings.

Figure 10-7: Fingerprint Settings Screen



Secondary finger mode	Alternate finger		
Auto resume timeout	300		
LED control	LED controlled internally		
Beeper control	Beeper controlled internally		
Reader model	DX-2000		
Input format 1	WC07 37Bit:19Bit ID		
Input format 2	WC06 35Bit:20Bit ID		
Input format 3	WC04 34Bit:20Bit ID		
Input format 4	WC02 32Bit:22Bit ID		
Input format 5	WC01 26Bit:16Bit ID		
Output format	Use input format		
Keypad format	WC01 26Bit:16Bit ID		
Action on ID overflow	Suppress output		
Action on ID unknown	Suppress output	value	0
Action on biometric reject	Suppress output	value	0
Action on duress	Increment/Decrement Facility Code Value:	value	0

Edit Fingerprint Settings

1. Click the *Configuration* tab.
2. Select the network in which the reader you want to edit exists in the network drop-down box.
3. Select the reader you want to edit from the reader drop-down box.
4. Click the *Edit selected reader* button.
5. Click the *Fingerprint settings* button.
6. Edit the necessary fields. See the Fingerprint Settings Fields table on page 41 for more information.
7. Click the *Accept settings* button.

Table 10-17: Fingerprint Settings Fields

Field	Req'd?	Description
Secondary Finger Mode	Yes	• Disabled: reader collects only one finger for each user. • Alternate finger: Scan of second finger grants access exactly as the first does. If user cannot verify with one finger, the other enrolled finger can be used. • Duress finger: Scan of second finger grants access and triggers a duress alarm. (Accomplished by either sending an alternate facility code or with reverse parity, depending on how your access control panel is set up.)

Field	Req'd?	Description
Auto Resume Timeout	Yes	• Number of seconds that reader stays in idle mode after being set into idle mode by a host command. • Number between 60 and 65535 • Default value is 300. • DO NOT change this setting unless advised to by technical support
LED Control	Yes	• Determines what controls the reader's LED display. • LED controlled internally: reader controls the LED display • LED controlled externally: access control panel control the LED display • For more information on setting up the LED control, see the reader's manual.
Beeper Control	Yes	• Determines what controls the reader's beeper. • Beeper controlled internally: reader controls beeper • Beeper controlled externally: access control panel controls beeper • For more information on setting up the beeper control, see the manual that came with the readers.
Reader Model	Yes	• Select the FingerKey model type from the drop down choices which are: • DX-2000 - Select this if you are using a DX-2000 model FingerKey. • DX-2100 HID Prox - Select this if you are using a DX-2100 model FingerKey using HID Prox cards. • DX-2200 HID iClass - Select this if you are using a DX-2200 model FingerKey with HID iClass cards. • DX-2400 Philips Mifare Standard - Select this if you are using a DX-2400 model FingerKey with Mifare Standard cards and settings. • DX-2400 Philips Mifare DESFire - Select this if you are using a DX-2400 model FingerKey with Mifare DESFire cards and settings.
iCLASS Configuration	Yes	• Choose None unless you are using iCLASS readers and cards. • If using iCLASS readers and cards, choose any iCLASS configuration that you've defined. • See Add an iCLASS Definition on page 50 for more information.
Mifare standard Configuration	Yes	• Choose None unless you are using Mifare Standard readers and cards. • If using Mifare Standard readers and cards, choose any Mifare Standard definition that you've defined. • See Add a Mifare Standard Definition on page 57 for more information.

Field	Req'd?	Description
DESFire Configuration	Yes	• Choose None unless you are using Mifare DESFire readers and cards. • If using Mifare DESFire readers and cards, choose any Mifare DESFire definition that you've defined. • See Add a DESFire Definition on page 55 for more information.
Input Format 1-5	Yes	• Card formats reader will accept from an internal or external card reader. • Choose either Wiegand or Magstripe formats but not both. Most companies use only one format. See the Card Formats table on page 65 for more information. • If you change from Wiegand to Magstripe format, or from Magstripe to Wiegand, you must reboot the reader. See the reader manual for further detail
Output Format	Yes	• Format reader sends to the access control panel if you use an internal or external card reader. • Use Input Format: Passes through whatever format is received • None: Reader sends no output when the ID is entered with a card. • Formats 1-11: Choose one of the formats from the Card Formats table on page 65.
Keypad Format	Yes	• Format the reader sends to the access control panel when a user enters his ID on the keypad instead of using a card. • None: Reader sends no output when the ID is entered with the keypad. • Formats 1-11: Choose one of the formats from the Card Formats table on page 65.
Action on ID Overflow	Yes	• Indicates what reader sends to access panel when card ID is longer than maximum length permitted by selected formats. • Suppress Output: Reader sends no output • Substitute all 1 bits: All 1 (one) bits are sent instead of the ID that was entered • Substitute all 0 bits: All 0 (zero) bits are sent instead of the ID that was entered

Field	Req'd?	Description
Action on ID Unknown	Yes	• Controls what the reader sends the access panel when ID is not recognized • Suppress Output: reader sends no output • Alternate Facility Code Value: reader sends facility code entered in the value entry, instead of the normal facility code • Increment/Decrement Facility Code Value: Reader sends facility code increased or decreased by the amount in the Value entry. • Toggle All Parity Bits: reader toggles the output parity bits.
Action on Biometric Reject	Yes	• Controls what the reader sends the access panel when a valid ID is entered but the finger doesn't match the template. • Same four options here as for Action on ID Unknown
Action on Duress	Yes	• Controls what the reader sends the access panel when a user places a duress finger • Same four options here as for Action on ID Unknown
Value	Yes	• Number between 0 and 32767 • Used when either Alternate Facility Code Value, Increment/Decrement Facility Code Value is chosen in the previous three fields • Enter a minus (-) sign before the number if you want to decrement the value.

Enabling a Secondary Finger Later

If users are enrolled with Seconday finger mode disabled, only one finger will be collected. If Secondary finger mode is later changed, all users need to be removed and re-enrolled in order to obtain a template for the second finger. The first finger will still function normally, but the second finger functionality will not be available until the user is re-enolled.

Interpreting the Format Detail

In the explanation of the format detail, you'll see an elaboration on the format that looks like this:

```
         1         2
12345678901234567890123456
PFFFFFFFFIIIIIIIIIIIIIIIIP
EXXXXXXXXXXXX.............
.............XXXXXXXXXXXXO
```

The numbers at the top: Identify the bit numbers; this example has 26 bits.

F: Indicates which bits contain the facility code; in this example, bits 2-9 have the facility code.

I: Indicates which bits contain the ID; in this example, bits 10-25 contain the ID.**P/E/O/X/.:** P indicates a parity bit; the E under the first parity bit here indicates that this parity is even. The X's following indicate which bits are used to determine that parity bit; the periods following indicate that those bits are not used in determining that parity bit; in this example, bits 2-13 are used to determine parity bit 1, and bits 14-26 do not affect this parity bit. The O under the second parity bit (bit 26) indicates this parity bit is odd; the preceding X's indicate that bits 14-25 are used to determine this parity bit.

For a list of available card formats, see the Card Formats table on page 65.

Managing FingerKey Card Formats

Most users don't need to define additional formats; the predefined formats that we initially provide cover almost all situations. However, if you need some other Wiegand format, you can define any format that you want.

We don't recommend changing or deleting any of our standard card formats. If you need a format that is similar to one of our existing formats, choose to add a new format; there's an option on the screen that lets you clone (copy) an existing format; you can then change the copy rather than changing the original.

Add a Card Format

1. Click the *Configuration* tab.
2. Click the *Create new card format* button.
3. Complete the fields on the screen. See the Card Format Fields table on page 46 for more information.
4. Click the *Accept settings* button.

Edit a Card Format

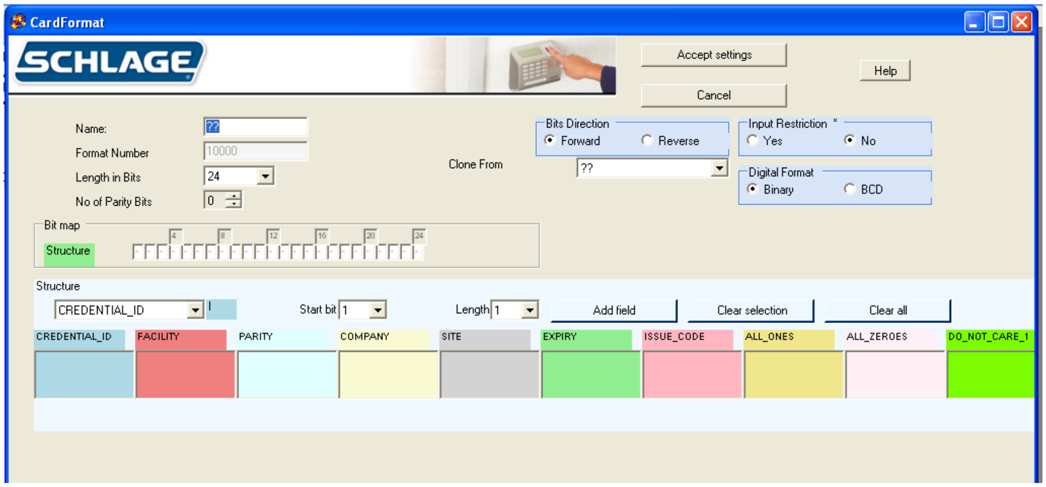
1. Click the *Configuration* tab.
2. Select the card format you want to edit from the drop-down box.
3. Click the *Edit selected card* format button.
4. Make changes to the fields on the screen. See the Card Format Fields table on page 46 for more information.
5. Click the *Accept settings* button.

Delete a Card Format

1. Click the *Configuration* tab.
2. Select the card format you want to edit from the drop-down box.
3. Click the *Edit selected card format* button.
4. Click the *delete* check box.
5. Click the *Accept settings* button.

Card Format Screen

Figure 10-8: The Card Format Screen



Name: ??

Format Number 10000

Length in Bits 24

No of Parity Bits 0

Clone From ??

Bits Direction ● Forward ○ Reverse

Input Restriction * ○ Yes ● No

Digital Format ● Binary ○ BCD

Structure

CREDENTIAL_ID

Start bit 1

Length 1

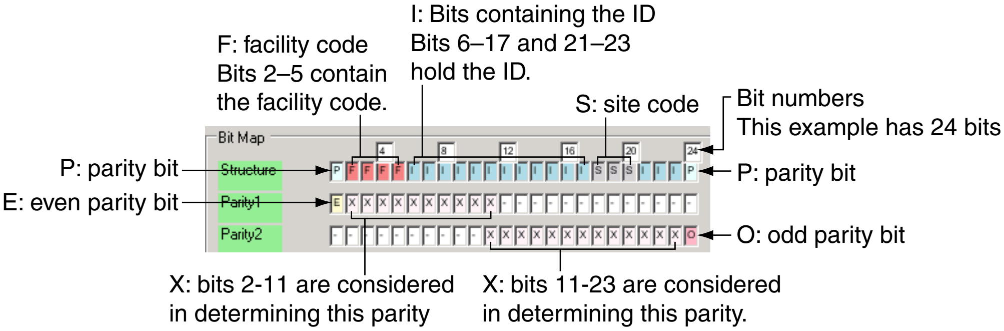
CREDENTIAL_ID | FACILITY | PARITY | COMPANY | SITE | EXPIRY | ISSUE_CODE | ALL_ONES | ALL_ZEROES | DO_NOT_CARE_1

The appearance of this screen varies depending on what you choose. The width of the Bit Map section changes based on the length you define for the ID. The Parity sections at the bottom only appear if you indicate that there are parity bits

Table 10-18: Card Format Fields

Field	Req'd?	Description
Name	Yes	Name that clearly identifies the format
Format Number	Yes	Internally generated number to identify the format. Cannot be changed.
Length in Bits	Yes	Number of bits in the format. This is the total number of bits, not just the number of bits in the ID
No of Parity Bits	No	If there are any parity bits, enter the number (1-4) here. For each parity bit specified here, a Parity section appears below
Bit Map	Yes	Structure of the format and how each bit is used. To change how different bits are used, see Card Format Structure on page 47, and the Bit Map example on page 47 for more information.
Delete	No	Deletes the current format.
Bits Direction	Yes	Forward: bits will be read in from left to right Reverse: bits will be read in from right to left
Clone From	No	Only appears if you are creating a new format. Allows you to make a copy of an existing format. Entries on the screen will be set to match the settings for the format you choose.
Input Restriction	Yes	Yes: only an exact format match will be accepted. Gives higher security since cards that are not issued by you will not be accepted. No: any input and parses will be accepted
Digital Format	Yes	Leave this set to Binary unless you understand what BCD is and have a specific reason for choosing it

Figure 10-9: Bit Map Example


Bit Map
Structure
Parity1
Parity2
4
8
12
16
20
24
P F F F F I I I I I I I I I I I I S S S I I I P
E X X X X X X X X X X
X X X X X X X X X X X X O

F: facility code
Bits 2–5 contain
the facility code.

I: Bits containing the ID
Bits 6–17 and 21–23
hold the ID.

S: site code

Bit numbers
This example has 24 bits

P: parity bit

E: even parity bit

P: parity bit

O: odd parity bit

X: bits 2-11 are considered
in determining this parity

X: bits 11-23 are considered
in determining this parity.

Card Format Structure

1. Under Structure, choose the type of bit you want to add from the drop-down box.

   - Credential ID
   - Facility
   - Parity
   - Company
   - Site
   - Expiry
   - Issue Code
   - All Ones
   - All Zeros
   - Do Not Care 1
   - Do Not Care 0

   To add parity bits, see Set Up the Parity Bits on page 48 for more information
2. Choose the first bit you want to use for the structure from the *Start bit* drop-down box.
3. Choose the number of sequential bits from the *Length* drop-down box.
   - For example, if bits 2-11 should contain the ID, select 2 from the Start Bit drop-down box, and 10 from the Length drop-down box.
   - If a particular structure is broken up, the structure will be added in multiple steps. For example, if you have a 15 bit ID, but that ID is contained in bits 2–6, 8–12, and 14–18, add the Credential ID three times: the first time with a Start Bit of 2 and a Length of 5, the second time with a Start Bit of 8 and a Length of 5, and the third time with a Start Bit of 14 and a Length of 5.
   - Similarly, suppose a particular structure is scrambled. For example, suppose bit 2-11 are used for the ID, but instead of being in order, bit 9 is the first bit of the ID, bit 3 is the second, etc. You would simply add this one bit at a time, starting with the first bit (bit 9), then the second, etc. Bits are considered in the order they appear in the structure list. (If you add bits in the wrong order, there's no way to rearrange them. You must delete the incorrect bits and then add them again in the correct order.)
   - If the Start Bit is disabled, then you have used all available bits; if you want to change the function of an existing bit, you must delete the incorrect bits before you can add them elsewhere.
4. Click *Add Field*.

   The bit numbers will be added in the corresponding columns in the structure table, and the bits will be reflected in the Bit Map representation above.
5. To remove an incorrect bit, check the box next to the bit and then click the *Clear Selection* button.
6. To clear (delete) the entire structure, click the *Clear All* button.

Set Up the Parity Bits

1. Add the Parity Bit to the Structure
   a. Under Structure, choose *Parity* from the drop-down box.
   b. Choose the first bit you want to use for the parity bit from the *Start bit* drop-down box.
   c. Choose the number of sequential bits (usually 1) from the *Length* drop-down box.
   d. Click the *Add Field* button.

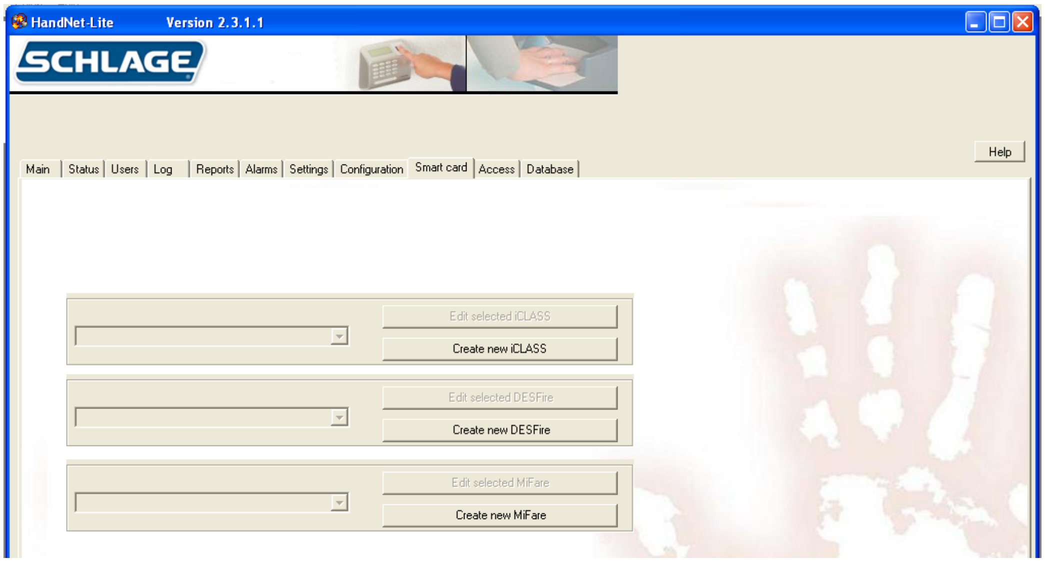
2. Indicate whether that parity bit is even or odd
   a. Under *Parity 1*, choose *Even* or *Odd* from the drop-down box.
   b. Under Start Bit, choose the bit for which you want to identify parity from the drop-down box.
   c. Click *Add Field*.

3. Identify which bits are considered to determine that parity bit
   a. Under *Parity 1*, choose *Included*
   b. Under *Start Bit*, choose the first bit that is used to determine this parity
   c. Under *Length*, indicate the number of bits to consider
   d. Click *Add Field*.
   e. If the bits to consider are broken up (for example, if you want to consider bits 2–10 and bits 14–18), simply repeat this step to add the additional bits.

Smart Card Tab

The Smart Card tab is used only with FingerKeys. It is used to manage FingerKey iCLASS, DESFire and MiFare cards.

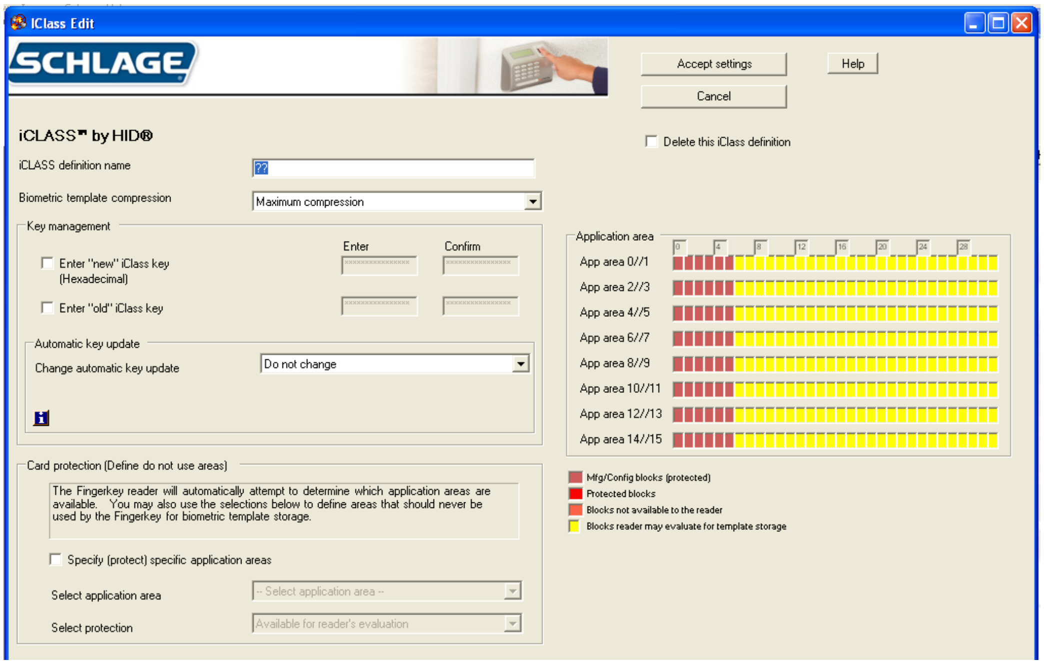
Figure 11-1: Smart Card Tab



Managing FingerKey iCLASS Definitions

iCLASS Definition Screen

Figure 11-2: iCLASS Definition Screen



iCLASS™ by HID®

□ Delete this iClass definition

iCLASS definition name: ??

Biometric template compression: Maximum compression

Key management

	Enter	Confirm
□ Enter "new" iClass key (Hexadecimal)	****************	****************
□ Enter "old" iClass key	****************	****************

Automatic key update

Change automatic key update: Do not change

Card protection (Define do not use areas)

The Fingerkey reader will automatically attempt to determine which application areas are available. You may also use the selections below to define areas that should never be used by the Fingerkey for biometric template storage.

□ Specify (protect) specific application areas

Select application area: -- Select application area --

Select protection: Available for reader's evaluation

Add an iCLASS Definition

1. Click the *Smart Card* tab.
2. Click the *Create new iCLASS* button.
3. Complete the fields on the screen. See the iCLASS Definition Fields table on page 50 for more information.
4. Click the Accept settings button.

Edit an iCLASS Definition

1. Click the *Smart Card* tab.
2. Choose the iCLASS definition you want to edit from the drop-down box.
3. Click the *Edit selected iCLASS* button.
4. Complete the fields on the screen. See the iCLASS Definition Fields table on page 50 for more information.
5. Click the *Accept settings* button.

Delete an iCLASS Definition

1. Click the *Smart Card* tab.
2. Choose the iCLASS definition you want to delete from the drop-down box.
3. Click the *Edit selected iCLASS* button.
4. Click the *Delete this iCLASS definition* check box.
5. Click the *Accept settings* button.

iCLASS Definition Fields

Table 11-19: iClass Definition Fields

Field	Req'd?	Description
iCLASS definition name	Yes	• Name of the iCLASS definition • Any name that distinguishes this definition from others
Biometric template compression		• Controls the amount of compression of the finger template before it is written to the iCLASS card • Maximum compression should be used initially • See the iCLASS Card Compression table on page 51 for more information
Enter "new" iClass key		• A password that encrypts the areas used by the readers on iCLASS cards • Protects the fingerprint data from being read if the same cards are used with other devices. • 16 hex digits (0–9 and A–F.) • A default key is used when a new iCLASS definition is defined. Can be used permanently if desired. • For increased security, change this key periodically.
Confirm "new" iClass key		Confirmation of previous field

Field	Req'd?	Description
Enter "old" iClass key		• Old reader key, usually populated automatically. • Required for the reader to change the key. • All cards should be updated each time the key is changed, to ensure they key is always up-to-date. • See Resetting Old Card Keys on page 52 for more information.
Automatic Key Update		• Indicates whether readers using this definition can automatically change the key on a card. • Defaults to Do Not Change. Whatever setting was previously entered will continue to be used. If you're editing a previously created definition, click the ℹ button to see what the current settings are. • Options: • Do Not Change: Use the previously entered setting. • Disable Auto Key Update: Prevents the reader from changing a key. • Start Unlimited Auto Key Update: Any card with the old key will be automatically updated when used at the reader. • Start Limited Auto Key Update: Any card with the old key will be automatically updated at the reader, until the number of cards and/or date specified is reached. • See Automatic Key Update on page 53 for more information.
Specify (protect) application areas		• Only check this box if you are sharing the iCLASS card with another iCLASS device that does not automatically determine the template location on the card. • See iCLASS Card Protection on page 52 for more information.

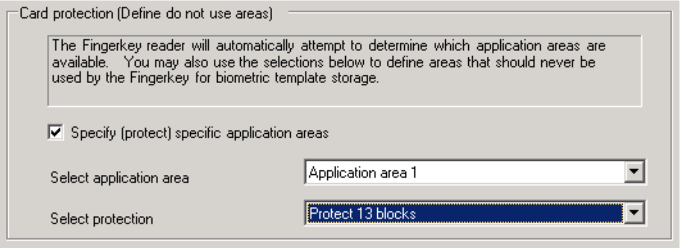
iCLASS Card Compression

Table 11-20: iCLASS Card Compression

	Number of Enrolled Fingers	
	1	2
No Compression	854 bytes	1654 bytes
Minimum Compression	566	1078
Medium Compression	454	854
Maximum Compression	310	566

iCLASS Card Protection

Figure 11-3: iCLASS Card Protection



Card protection (Define do not use areas)

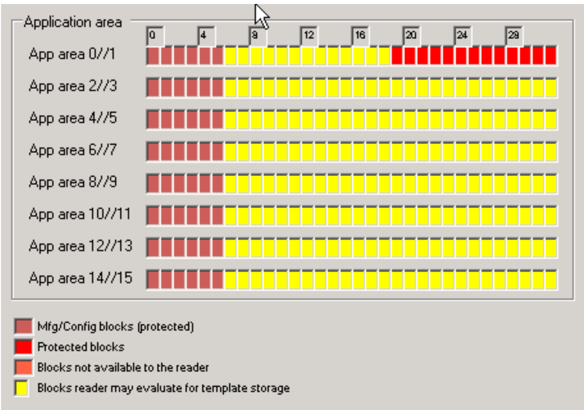
The Fingerkey reader will automatically attempt to determine which application areas are available. You may also use the selections below to define areas that should never be used by the Fingerkey for biometric template storage.

☑ Specify (protect) specific application areas

Select application area: Application area 1

Select protection: Protect 13 blocks

The grid on the right shows the protected blocks in red:



Application area

🟥 Mfg/Config blocks (protected)
🟥 Protected blocks
🟧 Blocks not available to the reader
🟨 Blocks reader may evaluate for template storage

You can protect multiple areas simply by choosing new values for each of these entries. You can clear any protected area by choosing the application area and choosing Available for Reader’s Evaluation in the Select Protection drop down menu.

When you protect blocks in even application areas (0, 2, 4, etc.), blocks are used from the left to the right, that is, starting at block 6 and working up; when you protect areas in odd application areas (1, 3, 5, etc.), blocks are used from right to left, that is, starting at 31 and working down.

If you protect both even and odd sections in any pair (for example, if you protect parts of both area 0 area 1), then the fingerprint reader can’t use that pair at all so the entire area is marked as protected**.**

! NOTE *Programmed iCLASS cards require application area 0 to be blocked off. To do this, click Select Application Area and pick Application Area 0 from the drop down menu. Then click Select Protection and choose Protect 26 blocks.*

Resetting Old Card Keys

To change the key for a previously used iCLASS card, the reader must know what the old key is—this prevents unauthorized people from converting other cards to work with your system. HandNet Lite keeps track of what the last key you used was, so most of the time, you don’t need to change this entry.

For example, suppose you originally set the key to 1234123412341234 and then you entered a New Reader Key of 5678567856785678. HandNet Lite remembers the old key; it would automatically change cards to the new key if you set it to automatically update keys (see Automatic Key Update on page 53).

However, suppose in January you set the key to 1234123412341234, in February change it to 5678567856785678, and in March change it again to 9ABC9ABC9ABC9ABC. Cards that got used during February would have been updated to 5678567856785678; cards that didn’t get used during February would still have January’s key of

1234123412341234. The reader can automatically update those cards with the most recent old key (5678567856785678), but it would no longer recognize the prior old key of 1234123412341234. If you have a situation like this, to update the older cards, you must manually indicate what old key to use by checking the Reset Old Key checkbox and then entering the appropriate value in the old key entries.

If you have an older card and know that one of several keys was used on it but aren't sure which one, enter the various old keys in turn here, trying to update the card each time.

You can avoid ever having to do this if you make sure that all cards get updated each time you change your key.

Automatic Key Update

Some administrators want any reader to update the key; other administrators prefer to only let selected readers update cards. For example, for top security, you might only let a non-networked reader in a security office update cards so that was the only place they could be updated. To do this, the administrator would create one iCLASS definition for the public readers (with Automatic Key Update unchecked), and another iClass definition (Automatic Key Update checked) for the administrative reader.

If you disable automatic updates here, you can still manually update keys using the reader command menus.

If you return to this screen, this entry defaults to Do Not Change; this means that whatever setting was previously entered will continue to be used. If you're editing a previously created definition, click the ℹ button to see what the current settings are. (This button doesn't do anything when creating a new definition.)

Your choices are:

Do Not Change: Use the previously entered setting.

Disable Auto Key Update: This prevents the reader from ever changing a key. With this setting, to update cards, you would have to use a reader associated with another iCLASS definition that allowed updates, or you would have to manually update cards with the reader's command menus.

Start Unlimited Auto Key Update: If any card with the old key is used, this automatically updates the card to the new key. There's no limit to the number of cards that can be updated, and no limit on the date range.

Start Limited Auto Key Update: If any card is used that currently has this old key, this automatically updates the card to the new key until the number of cards and/or date specified in the following two entries is reached. For example, if you had 20 employees, you might set this to only automatically update 20 cards; once that was done, cards would not be automatically updated until you changed the key again. You could also specify a date; cards would then be automatically updated until that date, but would not be updated after that date.

Specify (protect) application areas

Only check this box if you are sharing the iCLASS card with another iCLASS device that doesn’t automatically determine the template location on the card. If fingerprint readers are the only iCLASS device that you use with your cards, or if you use other device that also automatically choose an available space to store information, then you don’t need to change this setting.

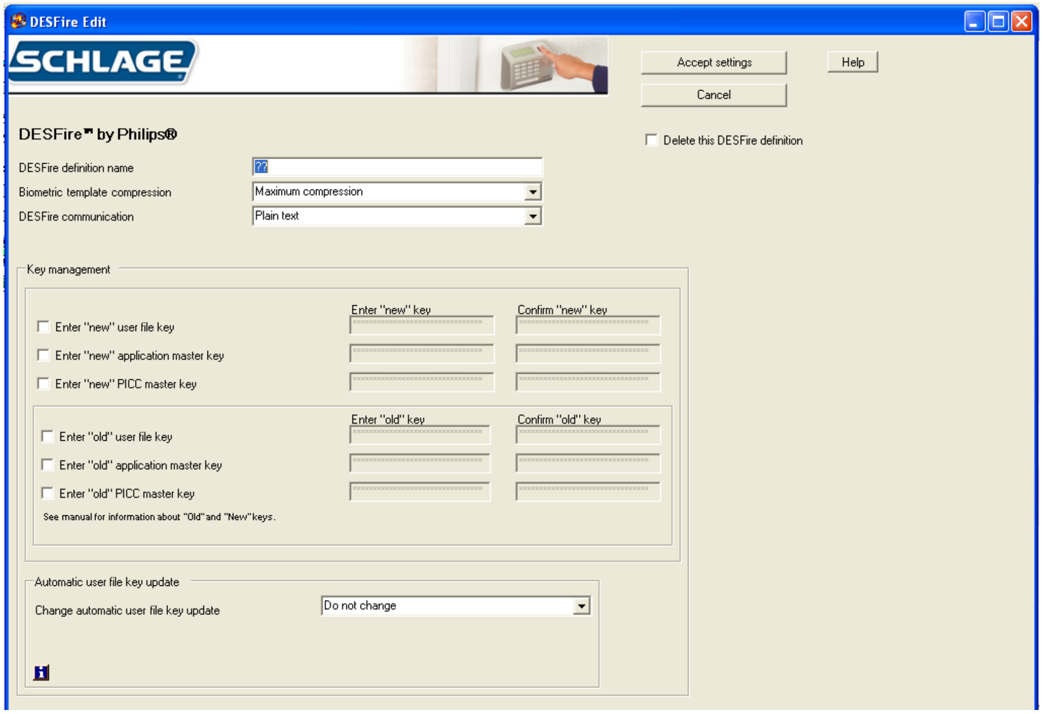
For example, Schlage Biometrics hand readers always store their templates in blocks 19–31 of area 1. If you were using the same iCLASS cards with both Schlage Biometrics hand readers and Schlage Biometrics fingerprint readers, you’d have to protect these blocks so a fingerprint template wouldn’t get written in this area; if it did, the hand reader would write a template over it.

To protect these blocks, check the box by Specify (protect) application areas, click Select Application Area and pick Application Area 1 from the drop down menu, and click Select Protection and choose Protect 13 blocks from the menu:

Managing FingerKey DESFire Card Definitions

DESFire Definition Screen

Figure 11-4: DESFire Definition Screen


DESFire Edit
SCHLAGE
Accept settings
Help
Cancel
DESFire™ by Philips®
□ Delete this DESFire definition
Key management
Enter "new" key
Confirm "new" key
□ Enter "new" user file key
□ Enter "new" application master key
□ Enter "new" PICC master key
Enter "old" key
Confirm "old" key
□ Enter "old" user file key
□ Enter "old" application master key
□ Enter "old" PICC master key
Automatic user file key update

DESFire definition name: ??

Biometric template compression: Maximum compression

DESFire communication: Plain text

See manual for information about "Old" and "New" keys.

Change automatic user file key update: Do not change

Add a DESFire Definition

1. Click the *Smart Card* tab.
2. Click the *Create new DESFire* button.
3. Complete the fields on the screen. See the DESFire Definition Fields table on page 56 for more information.
4. Click the *Accept settings* button.

Edit a DESFire Definition

1. Click the *Smart Card* tab.
2. Choose the DESFire definition you want to edit from the drop-down box.
3. Click the *Edit selected DESFire* button.
4. Complete the fields on the screen. See the DESFire Definition Fields table on page 56 for more information.
5. Click the *Accept settings* button.

Delete a DESFire Definition

1. Click the *Smart Card* tab.
2. Choose the DESFire definition you want to delete from the drop-down box.
3. Click the *Edit selected DESFire* button.
4. Click the *Delete this DESFire* definition check box.
5. Click the *Accept settings* button.

DESFire Definition Fields

Table 11-21: DESFire Definition Fields

Field	Req'd?	Description
DESFire definition name	Yes	• Name of the DESFire definition • Any name that distinguishes this definition from others
Biometric template compression	Yes	• Controls the amount of compression of the finger template before it is written to the DESFire card • Maximum compression should be used initially • See the DESFire Card Compression table on page 56 for more information
DESFire communication	Yes	Select either *Plain Text* or *DESFire* ciphered
Enter "new" user file key	Yes	• Check the box to edit these fields. • Key entered must be exactly the same in both boxes.
Enter "new" application master key	Yes	• Check the box to edit these fields. • Key entered must be exactly the same in both boxes.
Enter "new" PICC master key	Yes	• Check the box to edit these fields. • Key entered must be exactly the same in both boxes.
Enter "old" user file key	Yes	• Check the box to edit these fields. • Key entered must be exactly the same in both boxes.
Enter "old" application master key	Yes	• Check the box to edit these fields. • Key entered must be exactly the same in both boxes.
Enter "old" PICC master key	Yes	• Check the box to edit these fields. • Key entered must be exactly the same in both boxes.
Change automatic user file key update	Yes	The automatic user key update choices are: • Do not change • Disable auto key update • Start unlimited auto key update • Start limited auto key update (displays two additional fields) • With limited auto key update the operator can select the number of cards to be updated and/or the number of cards to automatically update.

DESFire Card Compression

Table 11-22: DESFire Card Compression

	Number of Enrolled Fingers	
	1	2
No Compression	854 bytes	1654 bytes
Minimum Compression	566	1078
Medium Compression	454	854
Maximum Compression	310	566

Managing FingerKey Mifare Standard Card Formats

Add a Mifare Standard Definition

1. Click the *Smart Card* tab.
2. Click the *Create new Mifare* button.
3. Complete the fields on the screen. See the Mifare Standard Definition Fields table on page 58, and the Mifare Standard Sector Fields on page 59 for more information.
4. Click the *Accept settings* button.

Edit a Mifare Standard Definition

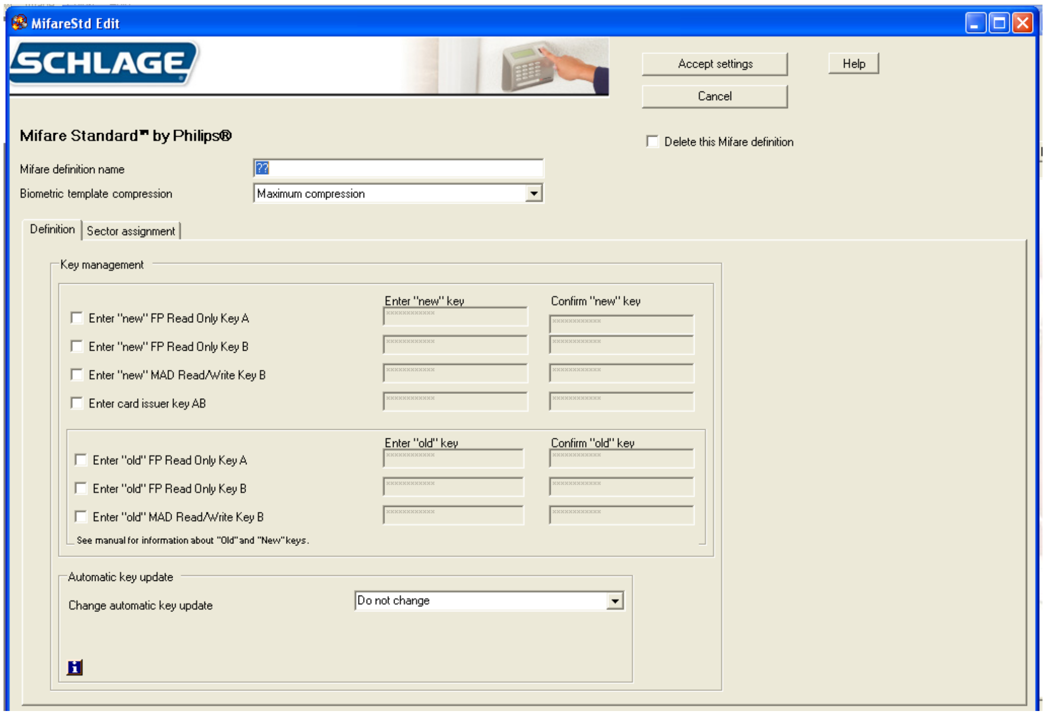
1. Click the *Smart Card* tab.
2. Choose the Mifare definition you want to edit from the drop-down box.
3. Click the *Edit selected Mifare* button.
4. Complete the fields on the screen. See the Mifare Standard Definition Fields table on page 58, and the Mifare Standard Sector Fields on page 59 for more information.
5. Click the *Accept settings* button.

Delete a Mifare Standard Definition

1. Click the *Smart Card* tab.
2. Choose the Mifare definition you want to delete from the drop-down box.
3. Click the *Edit selected Mifare* button.
4. Click the *Delete this Mifare* definition check box.
5. Click the *Accept settings* button.

Mifare Standard Definition Screen

Figure 11-5: Mifare Standard Definition Screen



MifareStd Edit

Accept settings

Help

Cancel

☐ Delete this Mifare definition

Mifare Standard™ by Philips®

Mifare definition name: ??

Biometric template compression: Maximum compression

Definition | Sector assignment

Key management

	Enter "new" key	Confirm "new" key
☐ Enter "new" FP Read Only Key A		
☐ Enter "new" FP Read Only Key B		
☐ Enter "new" MAD Read/Write Key B		
☐ Enter card issuer key AB		

	Enter "old" key	Confirm "old" key
☐ Enter "old" FP Read Only Key A		
☐ Enter "old" FP Read Only Key B		
☐ Enter "old" MAD Read/Write Key B		

See manual for information about "Old" and "New" keys.

Automatic key update

Change automatic key update: Do not change

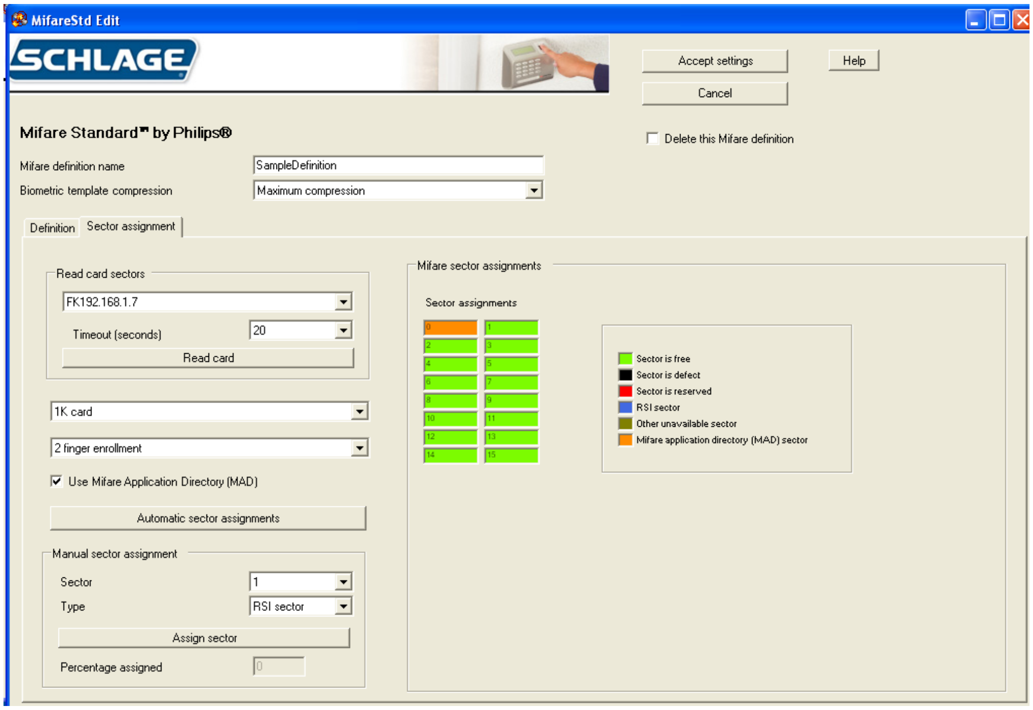
Mifare Standard Definition Fields

Table 11-23: Mifare Standard Definition Fields

Field	Req'd?	Description
Mifare definition name	Yes	• Name of the Mifare definition • Any name that distinguishes this definition from others
Biometric template compression	Yes	• Controls the amount of compression of the finger template before it is written to the Mifare card • Maximum compression should be used initially • See the Mifare Card Compression table on page 60 for more information
Enter “new” FP Read Only Key A	Yes	• Check the box to edit these fields • Key entered must be the same in both boxes
Enter “new” FP Read Only Key B	Yes	• Check the box to edit these fields • Key entered must be the same in both boxes
Enter “new” MAD Read/Write Key B	Yes	• Check the box to edit these fields • Key entered must be the same in both boxes
Enter card issuer key AB	Yes	• Check the box to edit these fields • Key entered must be the same in both boxes
Enter “old” FP Read Only Key A	Yes	• Check the box to edit these fields • Key entered must be the same in both boxes
Enter “old” FP Read Only Key B	Yes	• Check the box to edit these fields • Key entered must be the same in both boxes
Enter “old” MAD Read/Write Key B	Yes	• Check the box to edit these fields • Key entered must be the same in both boxes

Field	Req'd?	Description
Change automatic key update	Yes	The automatic key update choices are: • Diable auto key update • Start unlimited auto key update • Start limited auto key update (displays two additional fields) • With limited auto key update, the operator can select the number of cards to be updated and/or the number of cards to automatically update.

Figure 11-6: Mifare Standard Sector Assignment Screen



MifareStd Edit

Mifare Standard™ by Philips®

☐ Delete this Mifare definition

Mifare definition name: SampleDefinition

Biometric template compression: Maximum compression

Read card sectors: FK192.168.1.7

Timeout (seconds): 20

1K card

2 finger enrollment

☑ Use Mifare Application Directory (MAD)

Manual sector assignment

Sector: 1

Type: RSI sector

Percentage assigned: 0

Mifare sector assignments

Sector assignments

0	1
2	3
4	5
6	7
8	9
10	11
12	13
14	15

🟩 Sector is free
■ Sector is defect
🟥 Sector is reserved
🟦 RSI sector
■ Other unavailable sector
🟧 Mifare application directory (MAD) sector

Mifare Standard Sector Fields

Table 11-24: Mifare Standard Sector Fields

Field	Req'd?	Description
Read card sectors		• Select the desired FingerKey to use in reading an existing Mifare Standard card • Select a card read timeout in seconds • Click the *Read card* button and present the Mifare Standard card to the reader • The card characteristics will be displayed • Use either Automatic Sector Assignment or Manual Sector Assignment to determine where the FingerKey will place the biometric template.
1K Card or 4K Card	Yes	• Allows you to tell HandNet Lite if the Mifare Standard cards you will be using have 1K or 4K capacity. • If you have used the *Read card* button described above, this will be filled in automatically.

Field	Req'd?	Description
Two finger enrollment or One finger enrollment	Yes	• Allows for storage of either one or two fingerprint biometric templates on the card.
Use Mifare Application Directory (MAD)	Yes	• Allows for use of a MAD (Mifare Application Directory) on the card. A MAD is stored in sector 0 (and 16 if a 4K card) and tells devices how the sectors on the card are allocated. • If unchecked, then you can assign any card sectors to fingerprint template storage.
Automatic sector assignments		• If *Use Mifare Application Directory* is checked, then clicking this button will instruct HandNet Lite to automatically assign the sectors on the card to be used for biometric template assignment (Schlage Biometrics Sector).
Manual Sector Assignment		• Allows you to manually assign the sectors for either biometric template assignment (Schlage Biometrics sector) or a free/available sector. You will need to assign sectors as Schlage Biometrics sectors until the percentage assigned is 100%.

As you use either Automatic or Manual sector assignment the display in the Mifare sector assignments group will change showing you the current assignment.

If your installation is currently using Mifare Standard cards with another device and you wish to add FingerKey biometrics to your existing cards you will wish to:

a. Determine if your current cards are formatted to use a Mifare Application Directory. Contact your existing device manufacturer. You can attempt to use the "Read card sectors" button in HandNet lite to attempt to read an existing MAD on the card.
b. If your current cards are not formatted to use a MAD, then you will need to determine which sectors your current device manufacturer uses on your card. It is normal that sector 0 will be used, but your current cards may also contain data in additional sectors. Check with your existing device manufacturer to determine which sectors on your cards are available and begin the Schlage Biometrics sector assignment at the first free sector.

Once you are satisfied with the card definition, click the "Accept settings" button to record the definition. You will then need to go back to the "Configuration" tab, and for each FingerKey to use this Mifare Standard definition you will need to "Edit selected reader", click "Fingerprint settings" and use the drop down for "Mifare standard configuration" and select the saved Mifare Standard Definition.

It is important that each FingerKey be assigned the correct Mifare standard configuration setting.

Mifare Card Compression

Table 11-25: Mifare Card Compression

	Number of Enrolled Fingers	
	1	2
No Compression	854 bytes	1654 bytes
Minimum Compression	566	1078
Medium Compression	454	854
Maximum Compression	310	566

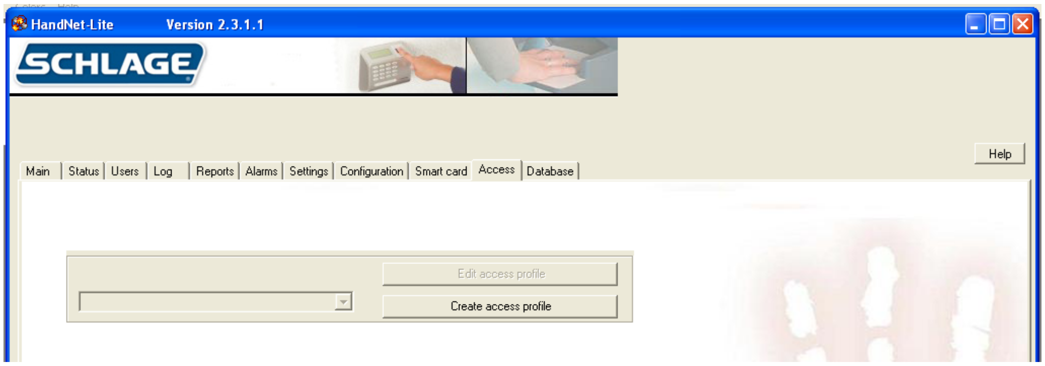
Access Tab

The Access Tab is used to add or edit access profiles. Access profiles define which type of user can use each reader.

For example, suppose your maintenance staff should have access to the maintenance rooms, your office staff should have access to the office, and your supervisors should have access to everything. You would create three access profiles: one for supervisors, one for office staff, and one for maintenance personnel. These profiles would identify which readers each group could use. After creating these profiles, whenever you added a user, you would identify which group the user was a part of, and the access profile for that group would automatically give the appropriate access.

If you want all users to be able to use every reader, you don't need to set up access profiles. HandNet Lite comes set up with an Always profile that lets users use any reader in the system. (It also has a Never profile that doesn't let the user verify at any reader.) You can't change or delete the Always or Never profile.

Figure 12-1: Access Tab



Add an Access Profile

1. Click the *Access* tab.
2. Click the *Create access profile* button.
3. Enter the access profile name.
4. Check the boxes next to the readers you want users with this access profile to be able to access.
5. Click the *Accept settings* button.

Edit an Access Profile

1. Click the *Access* tab.
2. Select the name of the access profile you want to edit from the drop-down box.
3. Click the *Edit access profile* button.
4. Edit the access profile name, if necessary.
5. Check the boxes next to the readers you want users with this access profile to be able to access.
6. Click the *Accept settings* button.

Delete an Access Profile

1. Click the *Access* tab.
2. Select the name of the access profile you want to delete from the drop-down box.
3. Check the box next to *Delete this access profile*.
4. Click the *Accept settings* button.

Figure 12-2: Access Profile Edit Screen

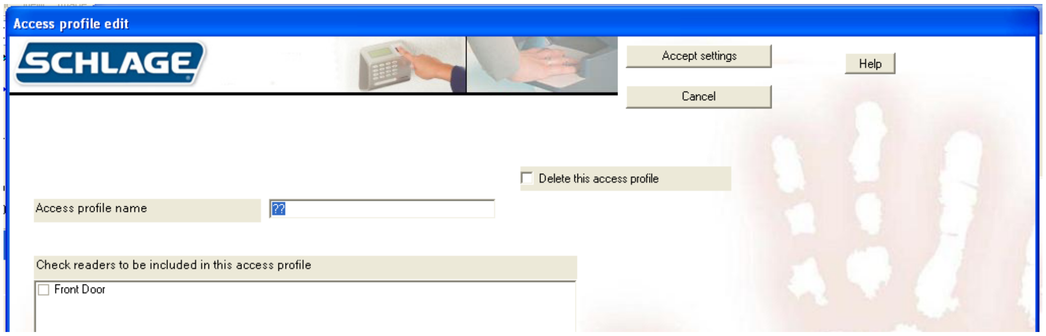


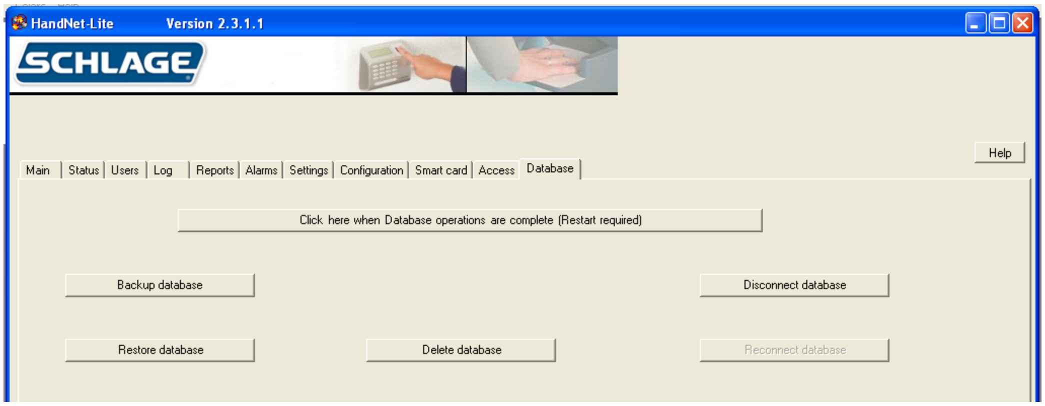
Table 12-26: Access Profile Fields

Field	Req'd?	Description
Access profile name	Yes	• Name of the access profile • Use a name that describes the group of users for which this access profile will be used. • Any combination of letters, numbers, spaces, and special characters up to 30 characters
Check readers to be included in this access profile	No	• Lists all the readers in the system • Check the box next to each reader you want users with this profile to be able to access. • Uncheck the box next to each reader you do not want users with this access profile to be able to access.
Delete this access profile	No	• Check to delete this access profile and remove it from the access profile list. • Access profiles that are assigned to users cannot be deleted. To remove an access profile from a user, see Edit a User on page 12. • If you delete the profile that is the default profile for reader enrollments, the next profile in the list will be selected. To choose a different default profile, go to the Settings window and choose the correct profile; see Settings Fields on page 25 for more information..

Database Tab

The Database Tab is used to backup, restore, delete, detach and attach the database.

Figure 13-1: Database Tab



Back Up the Database

The Backup database button is used to create a backup of the HandNet-lite database. The location of the backup will be displayed at the bottom of the screen:

1. Click the *Database* tab.
2. Click the *Backup database* button.
3. If you have completed all database operations you want to perform at this time, click the *Click here when Database operations are complete* button. See Finish Database Operations and Restart on page 64 for more information.

Restore the Database

The Restore database button is used to restore a backup file of the database.

1. Click the *Database* tab.
2. Click the *Restore database* button.
3. Select the backup file you want to use from the pop-up window and click the *Open* button.
4. If you have completed all database operations you want to perform at this time, click the *Click here when Database operations are complete* button. See Finish Database Operations and Restart on page 64 for more information..

Delete the Database

The Delete database button is used to delete the working copy of the database.

1. Click the *Database* tab.
2. Click the *Delete database* button.
3. Click the *Yes* button on the pop-up window.

   If you delete the database, you will lose all configuration and user information in the system. A new, empty database will replace the current database.

4. If you have completed all database operations you want to perform at this time, click the *Click here when Database operations are complete* button. See Finish Database Operations and Restart on page 64 for more information..

Disconnect the Database

The Disconnect database button is used to disconnect the database from the MS SQL Server Express database engine.

1. Click the *Database* tab.
2. Click the *Disconnect database* button.
3. If you have completed all database operations you want to perform at this time, click the *Click here when Database operations are complete* button. See Finish Database Operations and Restart on page 64 for more information..

Reconnect the Database

The Connect database button is used to reconnect the database to the MS SQL Server Express database engine.

1. Click the *Database* tab.
2. Click the *Reconnect database* button.
3. If you have completed all database operations you want to perform at this time, click the *Click here when Database operations are complete* button. See Finish Database Operations and Restart on page 64 for more information..

Finish Database Operations and Restart

Once you have completed all database operations you want to perform at this time, click the Click here when Database operations are complete button. This will cause HandNet-lite to exit. When you restart HandNet-lite it will take the following actions:

1. If a database is currently attached, HandNet Lite will use that database.
2. If a database is not currently attached, but database files exist, HandNet Lite will reattach the database files and continue.
3. If a database is not currently attached, and there is no database file, HandNet Lite will create a new database.

Appendix A

Table A-27: Card Formats

Type	Format	Description	Format detail
Wiegand formats	1	WC01 26 bit: 16 bit ID	Facility code: 8 bits, bit 2-9 ID: 16 bits, bit 10-25 1 2 12345678901234567890123456 PFFFFFFFFIIIIIIIIIIIIIIIIP EXXXXXXXXXXXX............. .............XXXXXXXXXXXXO
	2	WC02 32 bit: 22 bit ID	Facility code: 8 bits, bit 2-9 ID: 22 bits, bit 10-31 1 2 3 12345678901234567890123456789012 PFFFFFFFFIIIIIIIIIIIIIIIIIIIIIIP EXXXXXXXXXXXXXXX................ ................XXXXXXXXXXXXXXXO
	3	WC03 34 bit: 16 bit ID	Facility code: 16 bits, bit 2-17 ID: 16 bits, bit 18-33 1 2 3 1234567890123456789012345678901234 PFFFFFFFFFFFFFFFFIIIIIIIIIIIIIIIIP EXXXXXXXXXXXXXXXX................. .................XXXXXXXXXXXXXXXXA
	4	WC04 34 bit: 20 bit ID	Facility code: 12 bits, bit 2-13 ID: 20 bits, bit 14-33 1 2 3 1234567890123456789012345678901234 PFFFFFFFFFFFFIIIIIIIIIIIIIIIIIIIIP EXXXXXXXXXXXXXXXX................. .................XXXXXXXXXXXXXXXXO
	5	WC05 34 bit: 32 bit ID	ID: 32 bits, bit 2-33 1 2 3 1234567890123456789012345678901234 PIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIP EXXXXXXXXXXXXXXXX................. .................XXXXXXXXXXXXXXXXO
	6	WC06 35 bit: 20 bit ID	Facility code: 12 bits, bit 3-14 ID: 20 bits, bit 15-34 1 2 3 12345678901234567890123456789012345 PPFFFFFFFFFFFFIIIIIIIIIIIIIIIIIIIIP .EXX.XX.XX.XX.XX.XX.XX.XX.XX.XX.XX. .XX.XX.XX.XX.XX.XX.XX.XX.XX.XX.XX.O OXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
	7	WC07 37 bit: 19 bit ID	Facility code: 16 bits, bit 2-17 ID: 19 bits, bit 18-36 1 2 3 1234567890123456789012345678901234567 PFFFFFFFFFFFFFFFFIIIIIIIIIIIIIIIIIIIP EXXXXXXXXXXXXXXXXXX.................. ..................XXXXXXXXXXXXXXXXXXO
	8	WC08 37 bit: 35 bit ID	ID: 35 bits, bit 2-36 1 2 3 1234567890123456789012345678901234567 PIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIP EXXXXXXXXXXXXXXXXXX.................. ..................XXXXXXXXXXXXXXXXXXO

Type	Format	Description	Format detail
MagStripe formats	9	MS09 MAG1	ABA Track 2 Input ID len 25 Output min len 1 Output max len 25 Do trim leading zeroes Oriented right, no offset
	10	MS10 MAG2	ABA Track 2 Input ID len 25 Output min len 1 Output max len 25 Do trim leading zeroes Oriented left, no offset
	11	MS11 MAG3 Octal 7	ABA Track 2 Input ID len 7 Output min len 1 Output max len 25 Do trim leading zeroes Oriented right, no offset MS11 MAG3 Octal 7 is the format used for FingerKeys with a ProxIF reader.
	12	MS12 MAG 6 AT 5	ABA Track 2 Input ID len 6 Output min len 1 Output max len 25 Do trim leading zeroes Oriented left, offset 5

While these are the most common formats, you can define any additional formats that you need; see Managing Card Formats starting on page 45 for more information.

Custom Splash Screen

1. Shut down HandNet Lite
2. Create a bitmap (.bmp) image that is 100 x 100 pixels.
3. Save the image to the program directory: C:\Program Files\Schlage\HandNet_Lite\Splash100x100.bmp. This path may vary depending on your individual installation.
4. Restart HandNet Lite. The image should appear on the splash screen.

Index

Ingersoll Rand
Security Technologies

Ingersoll Rand's Security Technologies Sector is a leading global provider of products and services that make environments safe, secure, and productive. The Sector's market-leading products include electronic and biometric access control systems; time and attendance and personnel scheduling systems; mechanical locks and portable security, door closures and exit devices, steel doors and frames, architectural hardware and technologies and services for global security markets.

408.341.4110

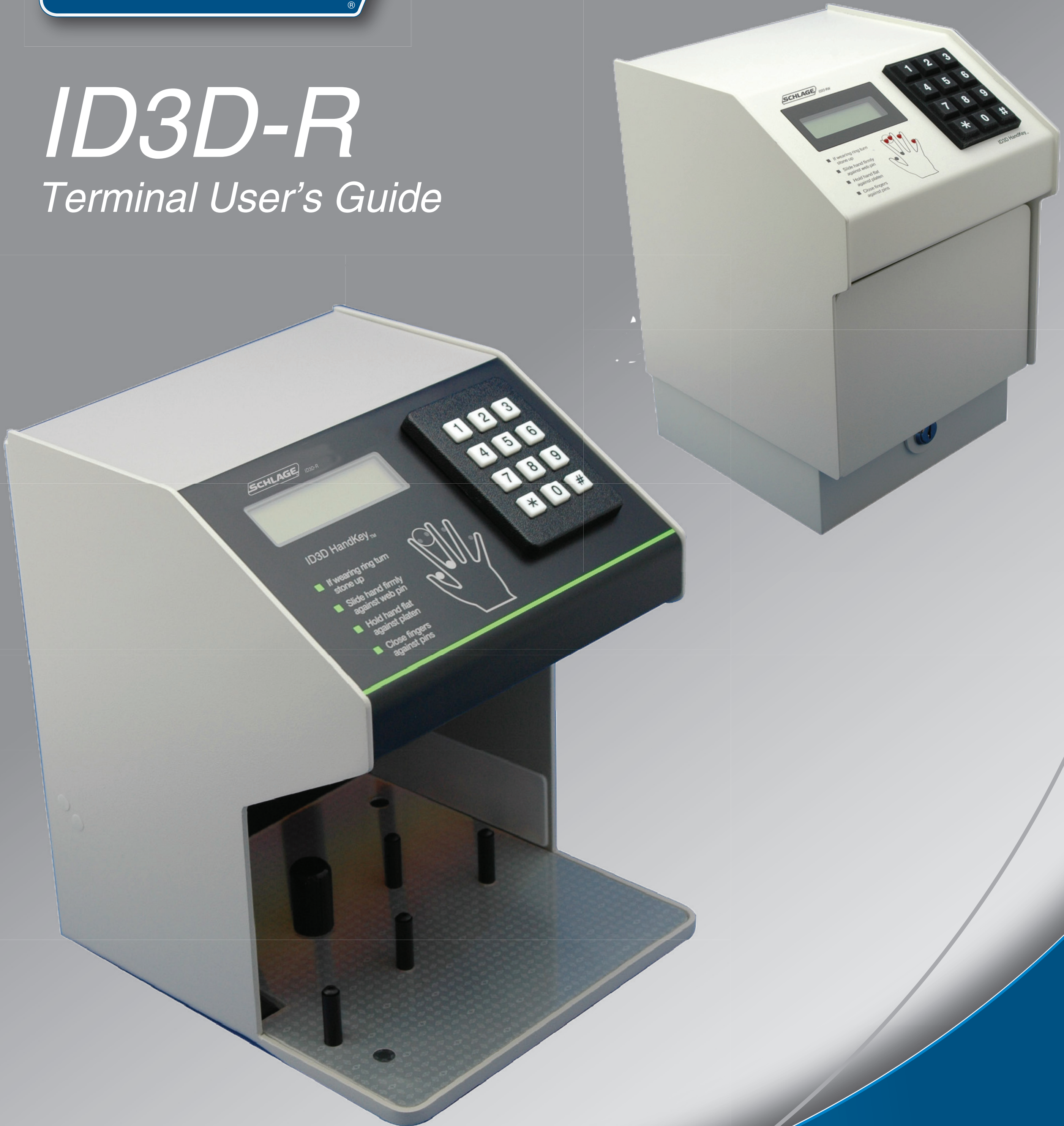
www.schlage.com www.ingersollrand.com

Schlage
Biometric Solutions
Ingersoll Rand Security Technologies
1520 Dell Avenue
Campbell, CA 95008
Office: 866-861-2480/512-712-1413 (international)
Fax: 866-303-1794/408-341-4111
E-mail: sbssupport@irco.com

SCHLAGE®

ID3D-R

Terminal User's Guide


SCHLAGE
ID3D-R
ID3D HandKey™
If wearing ring turn stone up
Slide hand firmly against web pin
Hold hand flat against platen
Close fingers against pins
1 2 3 4 5 6 7 8 9 * 0 #

Ingersoll Rand
Security Technologies

Table of Contents

LIMITED WARRANTY

Schlage Biometrics, Inc. (the “Company”) warrants to the original user the products manufactured by the Company (the “Product”) to be free of defects in material and workmanship for a period of one year from the date of purchase by such user or 15 months from the date of shipment from the factory, whichever is sooner, provided:

1. The Company has been notified within such period by return of any alleged defective product, free and clear of all liens and encumbrances, to the Company or its authorized dealer, transportation prepaid; and

2. The Product has not been abused, misused or improperly maintained and/or repaired during such period; and

3. Such defect has not been caused by ordinary wear and tear; and

4. Such defect is not the result of voltage surges/brownouts, lightning, water damage/flooding, fire, explosion, earthquakes, tornadoes, acts of aggression/war or similar phenomenon; and

5. Accessories used as integral to the Product have been approved by the Company.

The Company shall, at its option, either repair or replace, free of charge, the Product found, upon the Company’s inspection, to be so defective, or if agreed upon, refund the purchase price, less a reasonable allowance for depreciation, in exchange for the Product.

THE COMPANY MAKES NO OTHER WARRANTY AND ALL IMPLIED WARRANTIES INCLUDING ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE ARE LIMITED TO THE DURATION OF THE EXPRESSED WARRANTY PERIOD AS SET FORTH ABOVE.

THE COMPANY’S MAXIMUM LIABILITY THEREUNDER IS LIMITED TO THE PURCHASE PRICE OF THE PRODUCT, IN NO EVENT SHALL THE COMPANY BE LIABLE FOR ANY CONSEQUENTIAL, INDIRECT, INCIDENTAL OR SPECIAL DAMAGES OF ANY NATURE ARISING FROM THE SAME OR THE USE OF THE PRODUCT.

Schlage Biometrics reserves the right to make changes in the design of any of its products without incurring any obligation to make the same change on units previously purchased.

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communicatins. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

This Class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil de la classe A respecte touts les exigences du Reglement sur le materiel brouilleur du Canada.

1.0 Introduction

1.1 About the Manual

This manual describes the function, installation, operation, and maintenance of the ID3D-R HandKey Three Dimensional Hand Geometry identity verifier, and the IS-400 Power Supply. It provides important information for the user, installer, and security system designer. This manual applies to E6 Versions and later of the HandKey firmware. This version includes significant functional enhancements over earlier versions.

Before attempting to operate the unit, please review at least sections five and six.

1.2 ID3D-R General Description

The ID3D-R HandKey is the latest in Schlage Biometrics' line of Hand Geometry Biometric Identifiers. The ID3D-R can be operated as a complete stand-alone access control station or it can be networked with other HandKeys to provide a simple network of biometric identity verification stations with centralized enrollment and event recording or it can be used to a PC and Schlage Biometrics HandNet software package to provide a complete centrally controlled system. A completely specified communications protocol for the ID3D-R is provided so that connections to a host computer is simply a matter of proper host software configuration.

Whether used stand-alone or networked, the ID3D-R will control a lock and auxiliary alarm signalling circuit directly, or can be configured to provide verified code data output in emulation of standard Wiegand or Magnetic Stripe card readers. The availability of this card reader emulation output enables the hand reader to be connected directly into standard card type access control systems.

When used as a stand-alone access control station, the ID3D-R provides RS-232 output to a standard serial type printer. All system activity can be printed. Each printed line shows the time, date, location, activity, and users ID number where applicable.

When used in a networked configuration, up to 31 Access Control Hand Readers can be connected to a central Enrollment Reader or host computer using a two wire RS-485 network or a four wire RS-422 network of up to 4,000 feet in length. The card reader emulation capability of the ID3D-R can also be used to integrate the HandKey into an existing Wiegand or Magnetic Stripe card access control system with no change required to the existing system hardware or software.

When an ID3D-R network is used without a host computer, the ID3D-R as an enrollment reader (master unit), must be used to enroll new users on to the system and remove users. The enrollment reader has the capability to broadcast enrollment data to allother hand readers on the network. There may be only one enrollment reader per network. When used as the network enrollment reader, the ID3D-R still maintains its capability to act as an access control station, verifying identity, controlling a door lock and emulating a card reader.

ID3D-R's also serve as the network access control remote readers. There may be up to 32 remote readers installed per network. The remote readers receive user enrollment data from the network master, verifies user identity each time a user ID is entered via the keypad or card reader, and transmits the verified card or keypad data to an optional host access control system via the card reader emulation output port. The controlled door lock may be operated directly by the ID3D-R if card reader emulation is not used, or from the optional host sytem.

ID numbers may be entered either using the built-in keypad, or Magnetic Stripe or Wiegand card readers. ID numbers may be up to ten digits long. Wiegand and Magnetic Stripe card reader emulation outputs are provided so that interface with many existing access control systems is simply a matter of connecting the hand reader in place of a card reader. ID length may be limited by Wiegand format when using the Wiegand interface.

In addition to entering the user's ID number from the keypad, the HandKey can also be programmed to request an account code. This account code wil then be data logged along with the ID number and may be used in time and attendance and labor tracking applications.

The HandKey has the capability to control access by time as well as users ID number. 62 programmable time zones (1-60) are available for assignment to users. Special time zones may be assigned to holidays. The lock and auxiliary control outputs can be programmed to operate by time zone as well.

A duress code mode of operation may be set. With this mode, the entry of a programmed "duress digit" will cause an alarm. This feature provides a useful method for creating an alarm if the user is being forced to operate the HandKey.

Alarm monitoring capability is provided for a door switch, an auxiliary alarm monitoring circuit, and tamper. An auxiliary output control circuit can be programmed to activate in response to any combination of the above alarms, as well as in response to invalid access attempts or a duress code entry from the keypad. This auxiliary output can be used to control local or remote alarm enunciators.

The ID3D-R has a standard internal memory capacity for 256 users. An expanded memory version of 3,328 or 9,728, or 27,904 users are also available. An internal lithium battery provides five years of memory retention for hand template and system setup data.

The ID3D-R HandKey can be table or wall mounted. An optional wall mount kit facilitates either flush or recessed wall mounting.

1.3 Specifications

SPECIFICATIONS
ID3D-R HANDKEY

POWER REQUIREMENTS:

Input Voltage............12 to 14 VDC.
Input Current............0.450 Amps Min. -0.5 Amps Max.
Input Power...............7 Watts Max.

LOCK and AUXILIARY:

Switched 12 VDC at 0.1 Amp maximum for operating a control relay or low current actuation device. Schlage Biometrics recommends the use of an isolation relay for this application.

ALARM MONITORING CIRCUITS:

Door switch, auxiliary input circuit, and tamper. 0.5 Ma. current loops. Breaking circuit produces alarm.

COMMUNICATION PORTS:

Two serial ports:

CH-0................RS-422 or RS-485
CH-1................RS-232 (Printer only)

IDENTIFICATION NUMBER INPUT DEVICE:

A keypad for ID number entry is built in. Wiegand and Magnetic Stripe card reader input are also available.

ID NUMBER SIZE:

ID numbers may be one to ten digits in length.

WIEGAND OUTPUT:

Wiegand compatible output is available for host system interface. Upon verification of identity, the entered ID number along with the site code, is transmitted in 26 bit Wiegand with eight bit site code format to the optional Wiegand compatible host. Other formats and Magnetic Stripe (ABA/ANSI track two) compatible outputs are also available in a +5 VDC = data high or a 0VDC = data high format.

STANDARD WIEGAND FORMAT:

A 26 bit Wiegand format is standard. The first bit transmitted or received is even parity over the next 12 bits. The last bit is odd parity over the preceding 12 bits. The second through ninth bits are the assigned facility code with the second bit most significant. The tenth through twenty-fifth bits are the ID number entered at the keypad, with the tenth bit most significant. The card reader emulation port transmits Wiegand data with a pulse width of 100 microseconds and an interpulse period of 1,200 microseconds. Other code formats can easily be accommodated, but the factory must be consulted first.

MEMORY CAPACITY:

Memory is available to store hand data for a minimum of 256 users. This is expandable to 3,328 or 9,728 or 27,904 users. Transaction data log buffering is also available for networked systems. Up to 3,405 transactions are buffered in a fifo buffer until transmission of stored data is requested by the host computer.

REQUEST TO EXIT INPUT:

A request to exit switch or keypad (KP-103) may be connected for secure side exit.

HANDKEY SIZE:

6.50 in. (16.5 cm) wide
8.38 in. (21.3 cm) high
7.38 in. (18.7 cm) deep

OPERATING TEMPERATURE:

32 to 110 F. limited by platen temperature.

RELATIVE HUMIDITY:

95% Max. non-condensing.

HAND READ AND VERIFICATION TIME:

Less than two seconds.

THROUGHPUT:

15 per minute.

VERIFICATION THRESHOLD:

User programmable on system and individual user basis.

AUXILIARY ALARM CONDITIONS:

User programmable.

2.0 Unpacking

2.1 Inspection

Carefully unpack the ID3D-R. Remove protective packing material and inspect each item for damage. Report any damage to the carrier and to Schlage Biometrics, Inc. Retain the container and packing material for use in transporting the equipment to the job site.

2.2 List of Materials

The ID3D-R Hand Reader shipping container should contain:

1 ea. ID3D-R hand reader assembly

1 ea. ID3D-R installation and operating manual

1 ea. Enclosure key envelope

The IS-400 hand reader power unit shipping container should contain:

1 ea. IS-400 power supply

The WM-200 wall mount kit shipping container should contain:

1 ea. wall mount enclosure assembly

1 ea. enclosure key envelope

2.3 Enclosure Key

Shipped with each hand reader or wall mount kit is an envelope containing the key which unlocks the enclosure. This envelope must only be opened by a person authorized and cleared to do so.

2.4 Bench Check

Upon completion of the unpacking, it is useful to connect the hand reader and test its operation. The only connections required for an operational test are two wires to the power supply. These connections are made to the ID3D-R terminal strip as per the wiring diagram in Appendix “D” of this manual. The hand reader can then be turned on and tested by verifying that it operates in accordance with the operating instructions.

****IMPORTANT**** **Before applying power, be sure that the correct power supply voltage will be applied and that the power supply polarity is correct. Otherwise, serious damage may result. Refer to the connection diagrams at the rear of this manual for proper hook-up.**

When first powering up the hand reader, the camera exposure is automatically set. In order for this to function properly, be sure that the platen and mirrors are clean and free of foreign objects. The hand reader is ready for operation when the front panel display shows.

****READY****

Remember that any changes to the system setup made using the command mode will be permanently stored. Particular care should be taken if passwords are changed as it is possible to lock oneself out of the command mode if a password is forgotten. If this happens, consult Section 7 of this manual for memory reset instructions.

During bench check is a good time to review the operating instructions, performing each operations as it is described.

3.0 ID3D-R HandKey Functional Capabilities

3.1 Identity Verification

There is a fundamental rule of access control that is often overlooked.

CARD READERS CANNOT IDENTIFY PEOPLE,
neither can
KEYPADS
PIN CODES
BRASS KEYS
DOCUMENTS

PEOPLE CAN IDENTIFY PEOPLE.
DOGS CAN IDENTIFY PEOPLE.
BIOMETRICS CAN IDENTIFY PEOPLE.

And Biometrics does it best!!!

Biometric access control has brought a new dimension to access control security systems. Biometric access control devices use key characteristics such as hand geometry that are unique to the individual. For the first time true automatic access control is possible. With hand geometry, it is the authorized person who is granted access, not merely the keyholder.

3.2 The ID3D-R HandKey

The ID3D-R is a biometric identification device that uses a three-dimensional image of the hand to uniquely verify a person's identity. This image is acquired by a television-like camera. The system is small, simple, quick, and uses no moving parts.

The ID3D-R contains a digital camera which records an image of the hand, and a microprocessor which extracts identity discriminating characteristics from the hand image. During the inital enrollment process three hand measurements are made and the results averaged. This forms a template of the user's hand which is stored for later use in identity verification. The stored template is automatically updated with each successful use. This assures that changes in the hand that occur over a period of time are accommodated for.

To use the system, the enrolled user enters an ID number via a keypad or by presenting a standard access control card. The system prompts for the hand to be placed on the measuring surface (platen), and once the hand is detected to be properly positioned, takes a TV-like picture. The identity discriminating characteristics are extracted from the picture and compared to the previously stored template. The results of the comparison are displayed, in the form of a score, in about a second. The results can be used to operate an access control device, such as a door lock, or to signal a higher level system device that identity has been verified or rejected.

3.3 ID3D-R HandKey Functional Capabilities

The ID3D-R HandKey hand reader provides-in one compact, low cost package-fast and accurate biometric identification and access control. It can store up to 27,904 nine-byte hand templates locally. It has lock and auxiliary control outputs, and alarm monitoring input circuits. A HandKey can control access by time as well as by individual users. Communication ports provide for audit trail information and networked system operation. The HandKey has a local keypad for PIN entry and can accept ID information from most commonly used card readers as well as from a host computer. System management functions are all controllable from the front panel of the hand reader, or by central host computer.

3.3.1 Operating Modes

The ID3D-R HandKey can be operated as a stand-alone access control station, as a network master enrollment station or as a networked access control station which receives and processes commands from a network host or a master unit. Operating mode selection is made by menu selections using the hand reader keypad.

When operated as a stand-alone access control station the ID3D-R provides complete capability for access control of a single door. In addition to controlling the door lock, it will also monitor door status and auxiliary alarm switches and signal a local or remote alarm enunciator. It datalogs all activity to a serial printer. Users can be enrolled or removed from the system without the need for an additional programmer or enrollment unit.

When used as a networked access control station, the ID3D-R can be controlled by the network master in a wide variety of ways. The network master may be a host computer or another HandKey. Communication between the networked hand readers and the host is via RS-485 or RS-422 data link. This data lnk may extend up to 4,000 feet, and up to 31 hand readers can be connected to it in addition to the network master. If your network will exceed the 4,000 feet maximum length, a RS-422 network should be used with either short haul or dial-up modems installed.

When another HandKey is used as a network master the networked hand readers operate in essentially the same manner as the stand-alone reader described above, with the exception that the enrollment or removal of users must be handled by the master HandKey and all datalogs are transmitted to the master for printing by its printer.

The network master HandKey functions as the central enrollment and datalogging unit for a network of up to 32 HandKeys. The enrollment master provides for central data logging by sending data logs from all of the hand readers on the network to its local printer. The enrollment master can also function as an access control station when not being used for enrollments. In this configuration, only user's hand data, and the time and date is transmitted from the master HandKey to the other readers on the network. All setup information such as lock operate times, time zone tables, passwords, and so on, are set locally at each HandKey so each can be different.

A host computer can also serve as the network master. The complete network communications protocol is documented in the software manual. With a computer as the network host, complete central control of all hand reader functions is possible. Schlage Biometrics has available host software for PC compatible computers.

3.3.2 ID Number Entry

The ID3D-R uses a keypad or card reader for ID number entry. Wiegand type card readers input and output circuits are standard with the HandKey. The ID3D-R is also compatible with Magnetic Stripe card readers that provide TTL level clock and data signals. Suitable readers will read ANSI encoded data from track two. If both a card reader and keypad are installed, either may be used for ID number entry.

Versions of the ID3D-R which accommodate Wiegand or Magnetic Stripe formats other than described above are available. Consult the factory for details.

3.3.3 Keypad ID Entry

ID numbers up to ten digits in length may be used. Shorter ID numbers may also be used if they are ended by pressing the # key. The maximum ID length may be set so that pressing the # key is not required.

3.3.4 Card Reader ID Entry

Wiegand type card readers may also be used for ID number entry. The ID3D-R provides a Wiegand compatible interface to accomplish this. The ID3D-R comes configured as standard for 26-bit Wiegand format cards. The required card format is as follows: the first bit transmitted must be even parity over the next 12 bits; the last bit transmitted must be odd parity over the preceding 12 bits. The second through ninth bits must be the assigned facility code with the second bit most significant. The tenth through twenty-fifth bits must be the ID number, with the tenth bit most significant.

Other Wiegand, proximity, and Magnetic Stripe card formats can be provided for. For proper interfacing, consult with the factory.

3.3.5 Card Reader Emulation

The ID3D-R HandKey provides output signals which can be used to emulate Wiegand or, optionally, Magnetic Stripe card readers. Thus, the HandKey can be used with any access control system that is compatible with such card readers. Data is transmitted from the card reader emulation port only in the case of a successful identity verification. If the verification is the result of an ID number entered from a card reader, then the complete bit pattern read from the card is transmitted from the emulation port. If the ID number was entered from the keypad, then a Wiegand compatible card image is constructed from the entered ID number and the hand reader facility code (user defined), and transmitted as described below.

The host interface to the ID3D-R is the same as for a Wiegand or Magnetic Stripe card reader. In the case of Wiegand reader emulation the data is transmitted from the hand reader via DATA1 and DATA0 signal lines. In the case of a Magnetic Stripe reader emulation, clock and data signals are provided.

Wiegand data is transmitted using a 26-bit format. The first bit transmitted is even parity over the next 12 bits. The last bit transmitted is odd parity over the preceding 12 bits. The second through ninth bits are the assigned facility code with the second bit most significant. The tenth through twenty-fifth bits are the ID number with the tenth bit most significant. See Section 4.2.8 for setup.

3.3.6 Duress Code

A duress code mode of operation may also be programmed for the HandKey. In this mode the entry of a pre-selected single digit code as a first additional digit of and ID number will cause a duress alarm to be given. The alarm will be sent to the printer or host computer, and the auxiliary output can be programmed to operate in response to this alarm.

3.3.7 Time and Attendance Code

A time and attendance code entry mode of operation is available on the HandKey. When this mode is selected, entry of an ID number is followed by a request for account code entry. The user may enter an account code of up to ten digits in length. When the user's identity is verified, the account code will be sent to the datalogging device (printer or host computer), along with the user's ID number, the time, date, and reader number. This operating mode is especially useful for time and attendance applications. The account code can be as simple as a single digit number to indicate clocking in or out, or a more extensive code to indicate transfer from department to department, and so on.

The ability to specify the maximum ID number length can be used in conjunction with account code entry to provide for time keeping operation. Consider the case where the ID length is set to four, and the account code mode is set. To clock in a user would enter xxxx1, to clock out xxxx2, to exit without changing clock status xxxx3, and so on (where xxxx is the user's ID number). These transactions would be recorded for ID number xxxx with transaction codes one, two, and three, respectively.

3.3.8 Time Zones

A time zone specifies at which time a user may be granted access. Up to 62 time zones may be defined, any one of which may be assigned to a user. Time zones 0 and 61 are special. Time zone 0 is Always, and time zone 61 is Never. The other 60 time zones may be defined, as described below, to provide the required time control.

Additionally, both the lock and the auxiliary outputs can be automatically operated under the control of an assigned time zone. These outputs will then activate whenever their assigned time zone becomes active, and deactivate whenever their time zone becomes inactive. Note that the lock and auxiliary outputs are activated or deactivated only when the controlling time zone becomes valid or invalid. For example, if the auxiliary output is turned on by its associated time zone, and then turned off by the host computer in a networked system. Then it will remain off until its associated time zone next becomes valid or some other event turns it on.

Time zones are made up of four time intervals. Each time interval consists of a start time, a stop time and the days of the week the time zone will be valid.

The start and stop times are specified on six minute boundaries. The days of the week include the seven days plus a holiday selection. A separate table allows any days of the year to be specified as holidays.

The table below shows the definition for a single time zone. Up to 60 such time zones, plus the two special zone 0 and 61, that can be established for a system.

Time Zone 1

				Su	Mo	Tu	We	Th	Fr	Sa	Hol
ON:	08:00	**OFF:**	18:00		2	3	4	5	6	7	8
ON:	13:00	**OFF:**	14:00							7	8
ON:	00:00	**OFF:**	00:00								
ON:	00:00	**OFF:**	00:00								

This time zone permits access from 8:00 am to 6:00 pm on Monday through Friday, and from 1:00 pm to 2:00 pm on Saturday or on any day designated as a holiday in the holiday table. Note that if any time interval is valid, the time zone is valid.

A single time zone can be assigned to each user at enrollment, and later changed if required. One use of the special time zone 61 can be used to deny a user access at all times while maintaining the hand template data in memory. That user can then be reinstated at a later time by assigning another valid time zone.

3.3.9 Host System Interface

The ID3D-R can be interfaced to a central host computer via a serial communication link. When so interfaced, all hand reader operations are under the control of the central computer. Hand data may be added to, or removed from the hand reader, verification cycles can be initiated from the computer host, the hand reader lock circuits can be activated, and so on. The host communication protocol and operation are described in the software manual.

The host computer is connected to the hand reader using a shielded two-wire RS-485 or a shielded four-wire RS-422 data link. Data converters are readily available that convert the common RS-232 computer interface to RS-485 and/or RS-422 such as a DC-101. Up to 31 hand readers can be connected in multi-drop fashion to the host computer.

3.3.10 Status Monitoring

In addition to providing access control functions as described above, the ID3D-R also provides extensive status monitoring capability. Conditions that are monitored are:

1. HandKey tamper circuit.
2. Door switch. Door opened or closed.
3. Auxiliary input circuit. Auxiliary circuit opened or closed.
4. Request to Exit switch.

Circuits one through four are energized with a 0.5 mA current loop. Except for the request to exit circuit, the circuits are triggered to the alarm state if the current loop is broken. Request to exit is activated when the current loop is completed.

The tamper circuit is completely contained within the HandKey and is activated by attempts to gain access to the internals of the HandKey.

The door switch circuit is intended to be connected to a magnetic type door switch. This switch will be closed when the door is closed and open when the door is opened. A door alarm is signaled only if the door switch is open when the door is locked and the door alarm shunt timer has timed out. This prevents door alarms when the door is unlocked and opened in response to a valid access request, and assures alarms if the door is forced open or held open too long after a valid opening. If a request to exit switch is used, the door alarm is inhibited in the same manner as described above. If the door switch is closed while the lock time is counting down, the HandKey lock output will lock the door automatically.

The auxiliary input circuit can be connected to any alarm initiating device, such as a common series burglar alarm loop, microwave or infrared intrusion detectors, and so on. These devices should be connected such that the auxiliary alarm circuit is broken in the event of an alarm condition.

3.3.11 Door and Auxiliary Circuit Control

Two output control circuits are provided. One is for controlling an electrified unlocking device, and the other is a general purpose control output that can be programmed to activate in response to certain alarm conditions or at pre-programmed times. These outputs are only available when the unit is configured for lock output control. The alternate card reader emulation configuration is defined via the “Set Output Mode” command in the setup menu in the hand reader or HandNet software.

Both of these circuits are 12 VDC outputs which switch to ground when activated. They can switch currents up to 0.1 amps. In the typical case they will be used to drive a control relay which operates the ultimate device such as a lock or alarm indicator.

In the case of a door lock, it is recommended that the control relay be located either at the door or at the lock power supply, thus minimizing the length of the high current lock circuit wiring.

The auxiliary output circuit can be set to activate in response to any combination of the alarm conditions or at programmed times. This allows for local or remote signaling of alarm conditions using lights, sirens, or other devices. Deactivation can be set to occur after a specified time period, after a valid access has occurred, or after either of these two events.

3.3.12 Serial I/O Channels

The ID3D-R has two serial I/O channels. Channel One is an RS-232 channel with only transmit and receive data signals available. It is used to communicate with a serial printer. Channel Zero can be configured by jumper selection to operate as an RS-422 or RS-485 port. Channel Zero is used for network communications. Baud rates are individually defined from 600 to 19.2K baud. RS-485 communications are half-duplex which must be taken into account in system design and software.

3.4 Memory Capacity

The HandKey memory is divided into two major areas: user memory, and transaction memory. User memory contains ID numbers, enrollment templates and user status information. Memory is provided for at least 256 users in all cases, with expanded memory options increasing the capacity to 3,328 or 9,728 or 27,904 users. In host controlled networks, the user capacity is limited only by the capacity of the host computer if using custom software. If HandNet software is utilized the memory capacity is equal to the installed memory on the HandKey.

Transaction memory is used to buffer transaction data logs in networked systems. There is capacity to buffer 3,405 transactions. Printer messages are not buffered.

4.0 Installation

4.1 Mechanical Installation

The hand reader should be located conveniently close to the portal being controlled. It should be placed so that it will **not be in direct sunlight**, and will be free from exposure to rain, dust, or other contaminants.

The base of the hand reader should be mounted so that it is 40 inches above the floor if it is to be used while standing, or at normal desk height if used while seated. If the surface mount option is being used, at least three inches of clear space should be provided at the rear of the hand reader to assure access to the enclosure lock.

4.1.1 Table Top Installation

When the hand reader is used without the wall mount kit, it can be placed directly on a table. Rubber feet are provided to protect the table surface.

The HandKey can be securely mounted to a table using the four 6-32 threaded female fasteners provided on the bottom surface. These are located at the center of the rubber mounting feet. Be sure to remove the rubber feet before mounting the hand reader.

To fasten the hand reader to its mounting table, use the hand reader outline drawing in Appendix D of this manual to locate the mounting holes and drill four holes through the mounting surface. The holes should be of a diameter to clear the ¼" spacers on the hand reader bottom.

Use four pieces of 6-32 threaded rod ⅜" longer than the thickness of the mounting table. Thread the rod into the four holes on the bottom of the hand reader a maxiimum of four turns and pass the rods through the mounting table. Secure the assembly to the table using a flat washer, a lock washer, and a 6-32 nut on each rod.

When the wall mount kit is not used, electrical connections can be brought out the hole in the back panel. This is a ⅞" hole which accepts standard ½" conduit fittings. Conduit cable clamps should be used to provide proper strain relief for the wiring. If armored cable is used, the proper ½" armored cable fittings must be used.

For an easy and safe installation the terminal strip bodies can be unplugged from the hand reader and the hand reader moved to a safe location until all external wiring is connected. To unplug the terminal strip, pull down on the terminal strip gently, until it is free from its mate. The field wiring can then be attached to the plugin terminal strip bodies.

4.1.2 Wall Mount Installation

The wall mount kit provides a secondary hand reader enclosure and brackets which greatly facilitates recessed or flush wall mounting of the hand reader. Wall mount kit dimensions, cutout and hole location/dimensions are located in Appendix D of this manual. Please note that the rear door of the hand reader is NOT used with the wall mount kit. The hand reader slides into the wall mount enclosure and is locked in place by the enclosure lock.

Electrical connections can be brought into the wall mount enclosure using the conduit knockouts located in the bottom and sides. The wiring runs up the rear of the enclosure to the plugin terminal strip at the rear of the hand reader. The use of a plugin terminal strip allows all field wiring to be connected while the hand reader is removed to a safe location. Once the wiring is completed, the terminal strip holding the field wiring is plugged into the hand reader.

4.2 Electrical Installation

Electrical work must be performed strictly in accordance with all applicable electrival, fire, and building codes. If there is a conflict between the instructions given herein and an applicable code, the code is to take precedence.

Drawings showing typical electrical hook-up are located in Appendix D of this manual. Please refer to these drawings in conjunction with the instructions given on the next page.

Electrical connections to the hand reader are made to a plugin strip within the reader enclosure. This terminal strip is shown on the following page.

HAND READER PLUGIN FIELD WIRING TERMINAL STRIPS

1	.....	+13.8 VDC--------------)	POWER
2	.....	GROUND---------------)	INPUT
3	.....	RXD----------------------)	
4	.....	GROUND---------------)	CH-1 RS-232
5	.....	TXD----------------------)	
6	.....	-RT)----------------------)	RS-
7	.....	+RT)---------------------)	485
8	.....	-TX------------------------)	CH-0 RS-422/485
9	.....	+TX-----------------------)	
10	.....	D0/DAT/AUX-----------)	
11	.....	GROUND---------------)	OUTPUT
12	.....	D1/CLK/LOCK---------)	
13	.....	DOOR SWITCH	
14	.....	GROUND	
15	.....	AUX IN	
16	.....	GROUND	
17	.....	REX SWITCH	
18	.....	+5 VOLTS OUT--------)	
19	.....	D0/DATA-----------------)	CARD
20	.....	CARD PRESENT-----)	READER
21	.....	D1/CLOCK-------------)	INPUTS
22	.....	GROUND---------------)	

4.2.1 Power Connections

The input power requirements of the hand reader are:

Input Voltage	12 to 14 VDC
Input Current	0.450 Amps Minimum, 0.5 Amps Maximum
Input Power	7 Watts Maximum

This power can be supplied by the Schlage Biometrics IS-400 power supply or any other source meeting the above requirements. While the ID3D-R will accommodate a wide range of input voltage, it is intended to be powered from a source that is compatible with float charged Gel Cell type batteries. In this case the battery can be connected directly to the power supply, thus providing simple and automatic power standby capability. A battery of 2.0 amp hour capacity will provide for several hours of operation in the event of mains power failure. Larger or smaller batteries may be used depending upon the particular requirements of the installation. The required float charge voltage is 13.5 to 13.8 VDC. Power from the power source should be connected directly to the +13.8 VDC (1) and power ground (2) terminals of the hand reader.

The wiring distance between the hand reader and the power supply and battery should be kept as short as reasonably practicable. The minimum wire diameter is 16 AWG.

****IMPORTANT**** **The negative terminal of the power supply must be connected to a good earth ground. This connection is to be made at the power supply, not at the hand reader. Failure to provide an adequate earth ground can result in unreliable operation of the unit.**

4.2.2 Door Status Switch Wiring

A door status switch is required if unauthorized door openings are to be signaled. The door status switch must be of the type that is closed when the door is closed, and opens when the door is opened. It must be capable of reliably switching a 0.5 Milliamperes 5 Volt DC circuit.

The door switch should be connected to the door switch (13) and ground (14) terminals of the hand reader. Number AWG 22 or larger twisted-pair wire should be used.

4.2.3 Request to Exit Switch Wiring

A Request to Exit switch can be installed on the secure side of the controlled door to facilitate exit without causing the ID3D-R to signal an intrusion alarm. When the request to exit switch is activated, the door is unlocked for the specified unlock time and the door alarm is disabled for the specified alarm shunt time.

The request to exit switch must be a normally opened momentary action type switch that closes when pressed and then opens when released. It must be capable of reliably switching a 0.5 Milliamperes 5 Volt DC circuit. The request to exit switch is to be connected to the hand reader REX (17) and ground (16) terminals using number 22 AWG or larger twisted-pair wire.

4.2.4 Auxiliary Alarm Monitor Wiring

An auxiliary alarm circuit can be monitored by the hand reader, and the alarm condition of this circuit signaled. This alarm circuit should contain no voltage or current sources, and should consist of a closed circuit in the normal state, and change to an open circuit in the alarm state. It must be capable of reliably switching a 0.5 Milliamperes 5 Volt DC circuit.

The auxiliary alarm switch contacts are to be connected to the aux in (15) and ground (14) terminals of the hand reader.

4.2.5 Lock Wiring

The lock output of the hand reader is shared with the card reader emulation output. If a lock is to be controlled by the hand reader, the reader operating mode must be programmed for lock/aux output and not card reader emulation.

The lock control output fo the ID3D-R is rated for 12 VDC and a load requiring 0.1 Amperes or less.

It is always recommended that if a lock control relay is to be used, it must have a coil requiring 12 VDC at less than 0.1 Amperes. The lock control relay coil should be connected to the 13.8 VDC (1) and lock (12) terminals of the ID3D-R using number 18 AWG or larger wire. The lock is then connected to its power supply through a normally open set of contacts of the lock control relay.

4.2.6 Auxiliary Control Circuit Wiring

An auxiliary output control circuit is provided. This circuit can be used to control local alarms or lighting, or to signal remote alarm monitoring devices. This output provides 12 VDC at 0.1 Amps maximum for control of the auxiliary circuit.

For installations using the aux output a control relay must be used. The control relay must have a coil requiring 12 VDC at less than 0.1 Amperes. The control relay coil should be connected to the Aux Out (10) and +13.8 VDC (1) terminals using number 18 AWG or larger wire. The auxiliary circuit to be controlled is then connected to the relay contacts as required.

If the auxiliary output control is to be used, the hand reader operating mode must be programmed for lock/aux output and not card reader emulation.

4.2.7 RS-485/422 Network Wiring

When used in a network configuration, the hand readers are interconnected via the RS-485 or a RS-422 communication link.This consists of a single twisted-pair for RS-485 or two twisted pairs for RS-422 that run from hand reader to hand reader. The hand readers are connected to this pair with no break in the twisted-pair(s) run. Color coded wire of AWG 22 or larger should be used. In electrically noisy environments shielded twisted-pair(s) should be used. In this case, the shield should be broken at every reader, one side of the shield connected to reader ground terminal (4), and the other side left open. In no case should the shield between two readers be connected at both readers.

The RS-485 twisted-pair connects to RT+ terminal (7) and RT-terminal (6) of the hand reader terminal strip. Color code must be maintained throughout the system, such that all R+ terminals in the system are connected together, and all R- terminals are likewise connected together.

The RS-422 twisted-pairs connect to RT- terminal (6) and RT+ terminal (7) of the hand reader terminal strip to TX- and TX+, respectively, on the data converter. Connect TX-terminal (8) and TX+ terminal (9) of the hand reader to RX- and RX+, respectively, on the data converter. Color code must be maintained throughout the system, such that all R+ terminals between the hand readers are connected together, and all R- terminals as well as the T- and T+ are likewise connected together between the hand readers.

IMPORTANT **If your network is configured for RS-422 communications, 510 ohm pull up reisistors may be needed, especially if modems will be installed in the network. See drawing labeled "Pull up resistor Location" in Appendix "D" of this manual.**

The hand reader(s) at the extreme end(s) of the RS-485 network must have a network termination or "End of Line" resistor installed. This is accomplished by placing dip switch #2 in the on position. If a RS-422 network is installed dip switch #1 must also be in the on position. See the "RS-422 or RS-485 End of Line Resistor Location" drawing in Appendix D of this manual. All network hand readers must have dip switch #3 in the on position for RS-485 communications. RS-422 communications require the dip switch #3 to be in the off position on all hand readers. The dip switch location is described on the drawing labeled "Parts Location, Replaceable Parts, Dip Switch Location" in Appendix D of this manual.

The total length of the twisted-pair(s) run must be less than 4,000 feet.

4.2.8 Card Access System Interface

Card reader emulation enables HandKey to be connected into an existing access control system as if it were a card reader. To set a HandKey for card reader emulation the following steps must be taken:

1. Ensure that the HandKey's outputs, "Data0" (pin 10), "Ground" (pin 11), and "Data1" (pin 12), are connected to the Wiegand data inputs of the host system. See "Typical Wiring Diagram, Card System Interface, Wiegand" drawing in Appendix D of this manual.

2. Set the HandKey output mode for card reader output. See Section “6.7.4” for procedures on setting the output mode.

3. Set site code. The factory default site code is “0”. If the site code is other than “0”, the site code must be set to match the site code of the host system. The range fror site codes is from 0 to 255 on the standard HandKey. See Section “6.7.7” for procedures on setting the site code.

The card reader emulation outputs are shared with the lock and auxiliary output control. Therefore, when card reader emulation is selected, lock and auxiliary control functions are no longer available.

4.2.9 Printer Connection

A serial printer can be connected to the ID3D-R via Channel One. The printer will use the RS-232 interface. The cables must be made or purchased to connect printer to the hand reader terminal strip as shown in Appendix D of this manual.

4.3 Serial Channel Dip Switch Settings

Serial Channel 0 can be selected to operate as an RS-422 or RS-485 communication network. For RS-422 operation, dip switch #3 must be placed in the off position.

The location of dip switch #3 is shown in the drawing labeled “Parts Location, Replaceable Parts, Dip Switch Location” in Appendix “D” of this manual.

4.4 System Turn-On

Once the hand readers have been installed and connected as described above, power can be applied and the installation tested.

****IMPORTANT**** **Before applying power, be sure that the correct power supply voltage will be applied and that the power supply polarity is correct. Otherwise, serious damage may result.**

When first powering up the hand reader, the camera exposure is automatically set. In order for this to function properly, be sure that the platen and mirrors are clean and free of foreign objects. The hand reader is ready for operation when the front panel display shows:

****READY****

Remember that any changes to the system setup made using the command mode will be permanently stored. Particular care should be taken if passwords are changed as it is possible to lock oneself out of the command mode if a password is forgotten. If this happens, consult Section 7 of this manual.

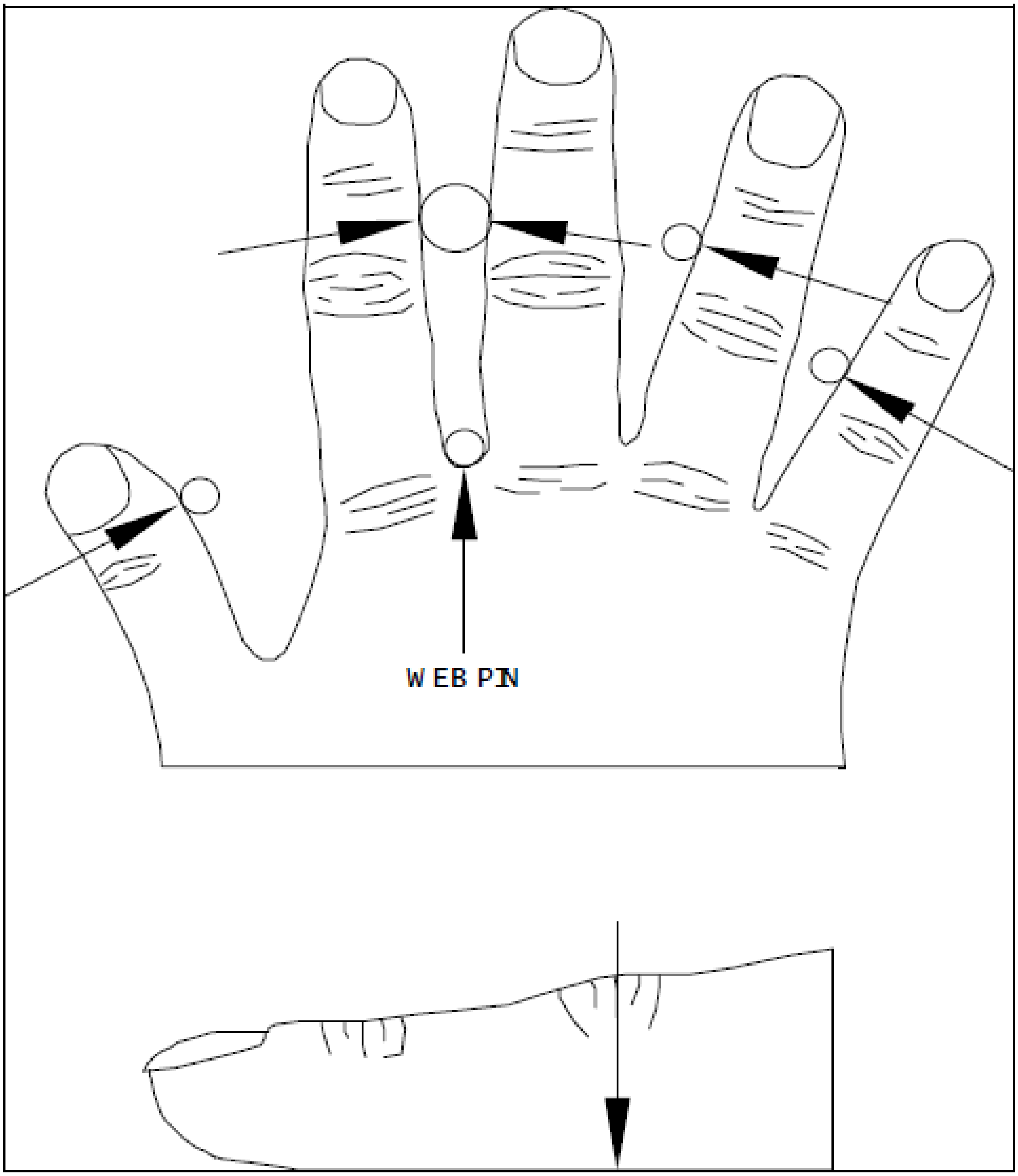
Test each reader by verifying that it operates as described in the operating section. This is best accomplished with the ID-Net connections removed from terminals six and seven so that the reader is not connected to the network. Once each reader has been individually checked out, connect the Enrollment Unit to the network by completing the connections to terminals six and seven. Be sure that the reader has been configured as an enrollment reader. Then enter the command mode setup group and select the network status command. The enrollment unit display will show the status of the network as readers are brought online.

Proceed to bring one access control reader online at a time. Set the reader address to an address in the range 0-31 and connect the reader to the network by completing the connections to terminals six and seven. Remember, all readers must be set to a different address for the network to function properly. Using the enrollment unit network status display, verify that network communications have been established between the enrollment unit and the access control reader.

Once all readers have been connected, test the network by enrolling several individuals using the enrollment readers and verifying that they are then enrolled on all access control stations. This is a good time to completely check out the system and become familar with its operation by testing all of the system commands.

Identity Verification Procedures

1. **If wearing a ring, rotate until stone is facing up.**
2. **Enter ID number at keypad.**
3. **Slide hand firmly against web pin.**
4. **Close fingers against finger pins until lights on top panel go out.**
5. **Hold fingers and palm flat against platen.**
6. **Remove hand when HandKey prompts “Remove Hand” or “ID Verified”.**



5.0 Operation-Access Control Mode

The acces control mode is the normal operating mode of the hand reader. It is this mode that is used for identity verification and control of a door lock.

5.1 Using the Hand Reader to Gain Access

Using the hand reader is a matter of entering your ID number, placing your hand on the hand reader, and observing the results. Use the instruction sheet on the previous page as a guide to proper operation. It may be a good idea to post a copy of this guide near the hand reader(s).

Whenever **READY** is displayed on the hand reader LCD, the hand reader is ready to accept entry of an ID number. ID numbers are entered on the hand reader using the keypad or card reader. In the discussion below it is assumed that the hand reader has not been set for the account code mode of operation. If it were, the user would be prompted to enter an account code immediately after the ID number was entered.

Once the ID number has been entered, it is registered in the hand reader by pressing the # key. You may think of this as an enter key. If a mistake is made when entering a number on the keypad, the entry can be cleared by pressing the * key. Once a valid ID number has been entered, ****PLACE HAND**** will appear on the display and the four finger position indicator lamps will turn on.

If you enter your ID number and ****PLACE HAND**** does not appear, this indicates that the ID number was not accepted. This may be due to an error in entry, or because someone before you had entered a digit into the keypad. This sort of problem can be prevented by clearing the keypad with the * key prior to entering your ID number.

When ****PLACE HAND**** appears in the display, place hand as directed below. This must be done promptly as the reader will time out after several seconds and **READY** will again be displayed. If this happens, just enter your ID number again.

CORRECT HAND PLACEMENT RULES

1. **Slide your hand forward on the platen, bumping the web between the middle and index finger up against the tall web pin.**

2. **Close all fingers together so that they touch their respective guide pins. The index and middle fingers should touch the large pin and the ring and little finger the smaller pins. The finger position indicator lights will then go out.**

3. **The balls of the finger tips should be against the platen surface, and the hand should be as flat as is comfortable. Cupping of the hand should be avoided.**

4. **If large rings are worn, care should be taken to see that the ring is rotated so that the stone is up in the normal position.**

5. **The left hand may be used by placing it palm up on the platen. If this method is used, enrollment must also be done with the left hand palm up.**

If the finger position lights located at the hand outline drawing do not go out, the fingers are not properly positioned at the indicated pin. A hand reading will not be made unless the fingers are in the proper position. Remember to close all fingers on their guide pins.

The hand is to remain held on the platen for a brief moment, until the ****PLACE HAND**** message no longer is shown. The results of the verification attempt will then be indicated on the display. If the verification was successful, ****ID VERIFIED**** will be displayed and the system will take appropriate action such as unlocking the door. If it was not, ****TRY AGAIN**** will be displayed.

If ****TRY AGAIN**** is displayed, and you are in fact authorized access, it may mean that an error was made in entering your ID number or in placing your hand for measurement. In any case, re-enter your ID number and try again, taking care to achieve correct hand placement. If rings are worn, be sure that the stone is rotated up in normal position.

If after three attempts identity is not verified, that ID number will no longer be accepted, and the system will take appropriate action, such as sounding an alarm. This is called a lockout. Before the rejected number can be used again, a valid acceptance must be recorded at the hand reader.

If an ID number is entered, but the hand is not correctly placed for measurement, the unit will time out in about 25 seconds. An ID number must again be entered to initiate a new identity verification sequence.

5.2 Ready Display

When the hand reader is ready to receive an ID number for identity verification its display show **READY**. The **READY** displays for various operating modes of the reader are different. This makes it easy to determine the operating mode at a glance. The different displays are shown in the table below.

Network Master	**===READY===**
Network Remote	**---READY---**
Stand-Alone	*****READY*****

5.3 Central Printer

As described in Section four of this manual, a printer can be connected to the hand reader for the recording of system activity. The printer line format is shown below.

cnnn rrr hh:mm:ss MM-DD-YY   DLM (ID) (AC)

c	Is a * if the message is an alarm, otherwise it is a blank.
nnn	Is a sequential printer line number.
rrr	Is the reader address for the message. It will be 255 for the Network Master.
hh:mm:ss	Time in hours, minutes, and seconds.
MM-DD-YY	Date in month, day, and year.
DLM	Data Log Message. A text message that indicates the nature of the activity being printed. Eg: **ACCESS GRANTED** **ACCESS DENIED** **DOOR FORCED OPEN**
(ID)	Is the ID number which is included if appropriate.
(AC)	Is the account code which is included if appropriate.

6.0 System Operation-Command Mode

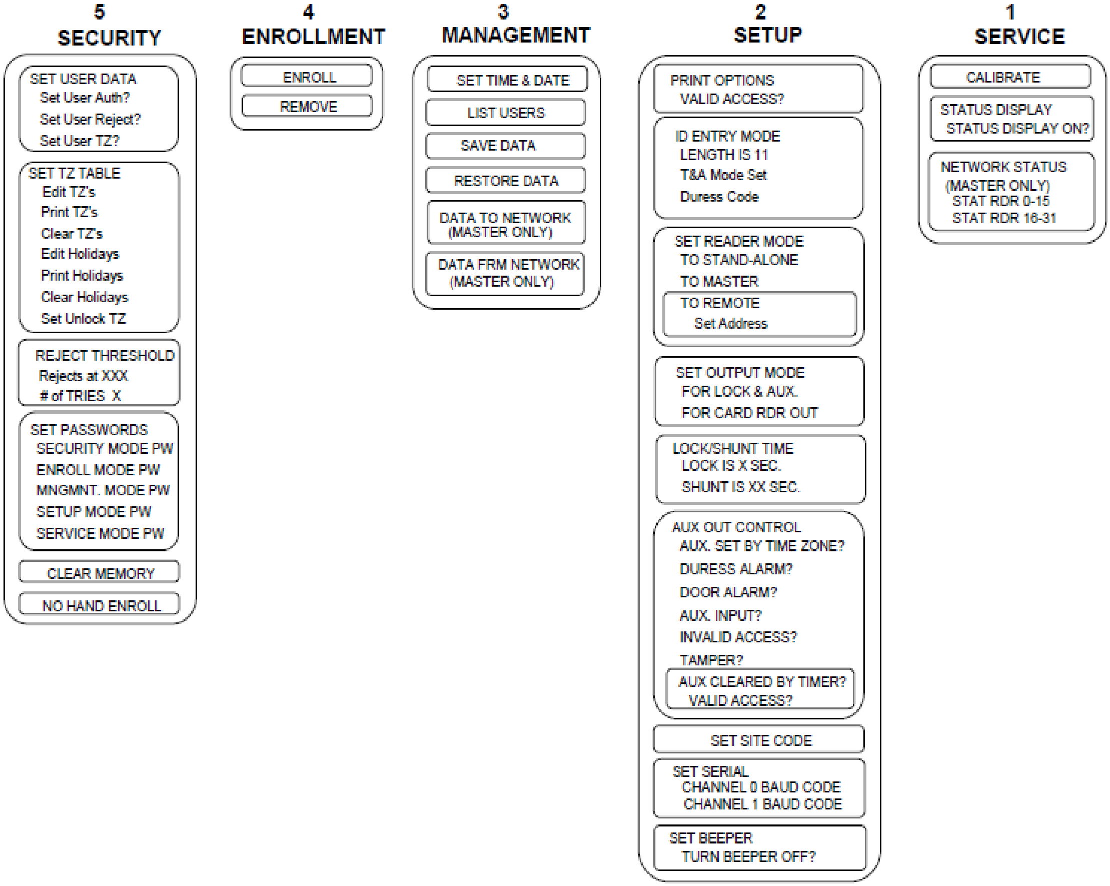
The command mode is used to add and remove users from the system and perform other important system management and service operations. This section of the manual describes the command mode, gives some important information required to use the command mode, and then gives specific instructions for use of each of the commands.

6.1 Command Mode Overview

The command mode is entered from the identity verification mode by first performing an identity verifying hand read and then entering an appropriate password. Access authorization to the command mode can be controlled on an individual enrolled user basis with five levels of authorization available.

The command mode is broken down into five different groups of commands. Access to each group is controlled by an individual password and authority level. The commands contained in each of the five groups are listed in the following:

Command Mode Structure



The drawing on the previous page depicts the structure of all of the commands which are available in the HandKey firmware version 5.07 and later. This section of the manual will present more detailed instructions for the commands shown here. The numbers directly above each of the command groups are the factory set passwords to access each group. The command mode is accessed by pressing the # key immediately after being verified, while the display shows **ID VERIFIED**. If the unit has no hand data stored, i.e. a demo unit, the command mode is accessed by pressing the # key after power up, when the display shows **READY**.

6.2 Important Background Information

This section provides information about passwords, system memory, and memory backup that is very important for a successful system configuration and operation.

6.2.1 Passwords and Authority Levels

Access to the various command mode commands is controlled by password and user authority levels. A unique password may be assigned to each of the five command groups. Only the command choices for the group whose password has been entered will be available for use. Groups can be combined by assigning them the same password. In this case, the command choices for the combined groups will be available when that password is entered.

In addition to knowing the correct password, authority levels can be assigned to restrict command mode operations to specific users. In this case, not only must the user know the required password for a command group, but must also have an authority level high enough for that group. In many cases, however, the passwords, which can be up to ten digits in length, provide adequate security, and authority levels need not be used.

Table 6.2.1 Authority Levels

	Required Authority Level
SECURITY GROUP	5 or H*
ENROLLMENT GROUP	4 or H*
MANAGEMENT GROUP	3 or H*
SETUP GROUP	2 or H*
SERVICE GROUP	1 or H*

*H is the highest authority level assigned to any user.

In the table above, note that the required authority level H is the highest level assigned to any user. Consequently, if users are enrolled, but no authority levels are assigned, then the default authority level of zero will be the highest level assigned, and any user can access any command group, provided that the appropriate password is known. Once any user is assigned an authority level greater than zero, users with authority level zero (the enrollment default) will not have access to any of the commands, and only users specifically given command level authorization will have access according to the table above.

When passwords and authority levels are set they are stored in permanent memory. Consequently, if the password for the security group is forgotten, it will not be possible to change any of the passwords, and system command mode operations may be seriously inhibited. It is recommended that procedures be put in place to prevent this. At a minimum, more than one person should be given access to the security group. If the passwords are lost or forgotten, see Section 7 of this manual for corrective action.

In many cases, all that is required during system setup is for new passwords to be assigned. For installations without complex security control requirements, there is often no need to set individual user authority levels.

When the unit is shipped from the factory the passwords are all set according to the table below.

Table 6.2.2 Factory Password Settings

SECURITY GROUP	5
ENROLLMENT GROUP	4
MANAGEMENT GROUP	3
SETUP GROUP	2
SERVICE GROUP	1

6.3 Entering and Exiting the Command Mode

If no users are enrolled on the system, simply press the # key, and you will be prompted to enter a password. If there are enrolled users, a valid hand reading must first be obtained, and then, while ****ID VERIFIED**** is displayed, press the # key to bring up the password prompt. NOTE: If the system is in the time and attendance mode, press the # key twice when the display shows **1-IN, 2-OUT, 3-BACK, 4-JOB**. Enter the password of the desired command group. This must be done promptly as there is a security time out for entering the code. Remember to once again press the **ENTER** (#) key after entering the last digit of the password. If the password is correct, and if the identified user carries an authority level high enough for the selected group, then the display will present the commands for the selected group.

Once the command mode has been entered, the display will show one command at a time in the top line. Shown in the second line will be the prompt:

*** NO YES #**

Pressing the # (Yes) key will select the displayed command. Prompts will then appear as appropriate for the selected command.

Pressing the * (No) key will cause the next command in turn to be displayed. Repeatedly pressing the * key will bring the display back to the first displayed command.

When the *** NO YES #** prompt is shown on the display, pressing any number will exit the command mode and return control to the identity verification mode. The ****READY**** display will reappear.

In the detailed descriptions of the various commands the second line *** NO YES #** will not be repeated each time the panel display is referred to.

6.4 Set User Data

The security group commands are the most sensitive commands of all. Access to these commands should, in general, be severely limited. These commands require an authority level of five.

6.4.1 Set User's Data

To change an enrolled user's authority level, reject level, or time zone data, enter the command mode security group as described in Section 6.3 of this manual, and make the **USER DATA** selection. The prompt **SET USER AUTH?** will then be displayed. If you press # (Yes), you will be prompted to change a user's authority as described below.If you press * (No), the **SET USER REJECT?** will be displayed. If you again press * (No), the **SET USERS TZ?** prompt will be displayed. Pressing * (No) one more time will take you back to the **SET USER AUTH?** prompt. If you press any key other than # or * you will leave the user data function.

6.4.1.1 Set User Authority Level

To set a user's authority level, when the **SET USER AUTH?** is displayed as described in Section 6.4.1 above, press the # (Yes) key. You will then be prompted for an ID number. Enter the ID number followed by the # key. You will then be prompted for the authority level. Enter an authority level from zero to five, followed by the # key.

If an ID number is not accepted, it means that the ID number entered was not that of an enrolled user and an authority leve cannot be set. Simply re-enter a valid ID number.

The authority level of each user can be displayed or printed using the **=LIST USERS=** command.

Mistakes in entry can be erased by pressing the * key. To leave this command, simply enter # in response to the ID number prompt.

Changes made at a network master reader using this command are transmitted to all readers on the network. Changes made using readers set as stand-alone or network remotes affect only those readers.

6.4.1.2 Set User's Reject Level

Under normal circumstances, whether a hand is accepted as valid or not is determined by the system reject threshold setting as described below. In special circumstances it may be desirable to change the reject level for a given individual. The availability of individual threshold settings allows the overall system threshold to be set to accommodate the average user, with individual threshold settings available to accommodate the exceptional case. For example, an individual with a physical impairment that finds difficulty in successfully verifying could be given a larger reject threshold. The individual would then have little problem in using the system with slight effect on system security.

To set an individual reject threshold, when the **SET USER REJECT?** is displayed as described in Section 6.4.1 above, press the # (Yes) key. You will then be prompted for an ID number. Enter the ID number followed by the # key. You will then be prompted for the reject level. Enter a threshold (see Section "6.4.3 Set Identity Reject Threshold") up to a maximum of 200, followed by the # key. Entering a threshold of zero will cause the system level threshold to be in effect for that user. To leave this command simply enter # in response to the ID number prompt. Then, to leave the command mode, press any number key.

If an ID number is not accepted it means that the ID number entered was not that of an enrolled user and a reject level cannot be set. Simply re-enter a valid ID number. Mistakes in entry can be erased by pressing the * key.

The reject level for each user can be displayed or printed using the **=LIST USERS=** command.

Changes made at a network master reader using this command are transmitted to all readers on the network. Changes made using readers set as stand-alone or network remotes affect only those readers.

6.4.1.3 Set User's Time Zone

When the prompt **SET USER TZ?** is displayed as described in Section 6.4.1, enter # (Yes). You will then be prompted to enter the user's ID number. Once this has been entered the current time zone will be displayed, and you will be prompted to enter a new time zone. Simply press # to keep the displayed value or enter a new value. Remember, time zone 0 is the special zone Always and time zone 61, the special zone, Never. The highest authority level should always be given zone 0.

6.4.2 Time Zone and Holiday Table Commands

To set, examine, print, or clear the time zone or holiday table, or to specify a time zone to automatically unlock the door, enter the command mode security group as described in Section 6.3 of the HandKey manual, and make the **TIME ZONE TABLE** selection. The prompt **EDIT TZ?** will then be displayed. If you press # (Yes) the time zone edit screen will be displayed as described below. If you press * (No), the **PRINT TZ?** option will be displayed. If you press any other key, you will leave the time zone table function. Repeatedly pressing the * (No) key will cycle you amongst the choices of **EDIT TIME ZONE**, **PRINT TIME ZONE**, **CLEAR HOLIDAY**, and **SET UNLOCK TZ**. Pressing the # key will select the displayed choice. Pressing any other key will leave the time zone table function.

6.4.2.1 Editing the TIme Zone Table

Pressing the # (Yes) key when **EDIT TZ?** is displayed as described in Section 6.4.2 above, will allow you to set, change, or view the time zone table. The prompt **ENTER TIME ZONE** will be displayed. If you just enter the # key you will leave the time zone edit function. If you enter a valid time zone and press the # key, the current setting of the selected time zone will be displayed on the HandKey display as shown below.

TZ1-1	23456 8
ON 8:00	OFF 17:00

The first line of the display shows that the information is for time zone one, time interval one, and that the valid days of the week are Monday through Friday. Note that the days of the week are numbered in sequence with Sunday=1 and Saturday=7. Day eight is the holiday specification. The second line of the display shows the start and stop times for this time zone and interval.

When the above display is first shown, the blinking cursor will be located on the top line, just before the days of the week display. When the cursor is in this position you have the following options:

1. Press any number key from one to eight to change the day of the week selection. Pressing the number of a day will reverse its selection.
2. Pressing the * key will cause the display of the next time interval for this time zone, until all intervals have been displayed.

3. Pressing the # key will move the cursor to the bottom line of the display so that you may enter the ON and OFF times. When both the ON and OFF times have been entered, the blinking cursor will disappear. Pressing any key will cause the display to show the next time interval or request another time zone when all time intervals have been shown.

On and off times are entered in 24 hour format. For example, 3:00 am is entered as 3:00, while 3:00 pm is entered as 15:00. When minutes are entered, they are rounded to the nearest six minutes. For example, if 3:14 is entered, it would be displayed as 3:12 once the # key is pressed. To enter times so that an interval is valid throughout the day, set the on time to 00:00 and the off time to 23:59. The system will round the off time up to 24:00.

Once the edit of a time zone has been completed, the display will again show **EDIT TIME ZONE #**. You can enter the number of a time zone to edit or simply press the # key to leave the time zone edit function.

6.4.2.2 Printing the Time Zone Table

Pressing the # (Yes) key when **CLEAR TIME TZ?** is displayed, as described in Section 6.4.2, will cause the complete time zone table to be printed on the HandKey printer. Only time zones that may be valid are printed. That is, if a time zone has no valid days of the week assigned, or all time intervals have the same on and off times, it will not be printed.

6.4.2.3 Clearing the Time Zone Table

Pressing the # (Yes) key when **CLEAR TIME TZ?** is displayed, as described in Section 6.4.2, will allow you to clear the time zone table. Before the table is cleared, the display will prompt to **CLEAR ENTER 123#**. In order for the table to be cleared you must enter 123#. Anything else will not clear the table.

6.4.2.4 Editing the Holiday Table

Pressing the # (Yes) key when **EDIT HOLIDAY?** is displayed, as described in Section 6.4.2, will allow you to enter or remove holidays from the holiday table. You will then be prompted to select the month. Enter a number from 1 to 12 for the desired month. The display will then show the holidays selected for that month. To change the holiday selection, enter the day of the month (1-31), followed by the # key. That will change the holiday selection for that date.

6.4.2.5 Printing the Holiday Table

Pressing the # (Yes) key when **PRINT HOLIDAY?** is displayed as described in Section 6.4.2, will cause the complete holiday table to be printed on the HandKey printer.

6.4.2.6 Clearing the Holiday Table

Pressing the # (Yes) key when **CLEAR HOLIDAY?** is displayed, as described in Section 6.4.2, will allow you to clear the holiday table. Before the table is cleared, the display will prompt **TO CLEAR ENTER 123#** In order for the table to be cleared you must enter 123#. Anything else will not clear the table.

6.4.2.7 Setting the Time Zone for Auto Unlock

Pressing the # (Yes) key when **UNLOCK TZ?** is displayed, as described in Section 6.4.2, will produce a request to enter a time zone number. The door will automatically unlock whenever the entered time zone is valid. If you do not want the door to automatically unlock, enter time zone 61(Never). You may not enter time zone 0 (Always).

6.4.3 Set Identity Reject Threshold

Upon delivery from the factory, the identity reject threshold is set to a value of 100. If the difference between the measured hand geometry and the hand template stored for an ID number differ by more than this amount, the identity is rejected. This threshold is such that an equal number of false reject and false accept errors on a single try basis can be expected.

The reject threshold can be made smaller, making it more difficult for an imposter to fool the system, but at the same time increasing the probability that a valid user will be falsely rejected. A threshold value of 60 will provide a significant increase in security with only a marginal increase in inconvenience due to false rejects. Likewise, the threshold could be made larger, increasing the false accept rate, but reducing the false reject rate.

To change the reject threshold setting, enter the command mode security group as described in Section 6.3 and make the **REJECT THRESHOLD** selection. The current reject threshold will be displayed, followed by a prompt to enter the new threshold. Enter the new threshold, or simply press the # key to leave the threshold unchanged.

6.4.4 Set Passwords

When the unit is shipped from the factory, the passwords are all set according to the table below.

Table 6.5.1 Factory Password Settings

SECURITY GROUP	5
ENROLLMENT GROUP	4
MANAGEMENT GROUP	3
SETUP GROUP	2
SERVICE GROUP	1

To change the assigned passwords, enter the command mode security group as described in Section 6.3 and select the **=SET PASSWORDS=** command. You will then be prompted to enter a new password for each of the five command groups in sequence. When prompted, you can enter a new password or simply press nothing but # to leave the password unchanged. Mistakes can be deleted by pressing the * key before the # key is pressed. Once a new password has been entered it will be permanently stored in memory until it is changed using this command. Passwords may be up to ten digits in length.

****IMPORTANT**** **Great care should be taken when the security group password is entered, as a valid security group password is required to change passwords. If this password is entered improperly or is subsequently lost, it will not be possible to gain access to the security group commands to correct the situation. In this case, consult Section 7 of this manual.**

6.4.5 Clear All Hand Data

This command will clear all hand data from the hand reader memory and should be used with great caution.

To clear memory, enter the command mode security group as described in Section 6.3 and choose the **=CLEAR MEMORY=** command. You will then be prompted to enter 123# to clear the memory. Entering anything else will cause the command to end without clearing memory. While memory is being cleared the display will show **CLEARING**.

6.4.6 Create “No Handread” ID Number

In certain rare cases a person may be unable to use the hand reader because of some severe physical deformity of the hand, for example, loss of fingers, or extreme arthritis. The “No Handread” mode allows this person to be enrolled with an ID number that grants access without a valid hand read having been obtained. For a user so enrolled, when the ID number is entered, the **PLACE HAND** prompt appears as usual. However, it is only necessary for the person to place their hand so that it is against the web pin and along at least one of the finger pins. The reader then grants access and display **ID VERIFIED** as if it were a normal hand read.

Be advised that security is totally dependent upon the ID number when a user is enrolled under the no handread mode, therefore that user should be given special instructions to keep the ID number secret. In addition it may be wise to assign a longer ID number. Since this enrollment option should be rarely used, the overall impact on system security is minimal. If possible you may wish to try increasing the reject threshold for the individual user as described in Section 6.4.1.2 to overcome problems before creating a no handread ID number. In our experience with tens of thousands of enrollments, this feature would have been useful only two or three times.

To enroll a user in this mode, enter the command mode security group as described in Section 6.3 and choose the **=NO HANDREAD=** command by pressing the # key. You will then be prompted to enter an ID number. Enter an ID number up to ten characters and press the # key when finished. If the ID number is already in use, the system will not allow the ID number to be entered and will display **SORRY, CAN’T ADD**. You will then be prompted to enter a time zone for the user. Enter an appropriate time zone (default is zero), then press the # key. No hand readings will be requested. A “no handread” user can be removed by using the standard **REMOVE USER** command described in Section 6.5.2.

6.5 Enrollment Group Commands

These commands are used to enroll and remove users. System security can be easily compromised if the enrollment process is not secure. The number of users authorized to enroll should be kept to a minimum.

****IMPORTANT**** **A new user’s first exposure to the hand reader usually occurs during the enrollment process. To ensure optimum system operation, enrollers should be well trained in hand reader operation and should take care to assure that the new users are properly indoctrinated in the proper hand placement and hand reader use.**

6.5.1 Enrolling a User

In order for a person to use the system they must first go through an enrollment process whereby a record of the identity discriminating characteristics of their hand is obtained and recorded. To accomplish this an ID number must be assigned and three hand readings taken.

To enroll a person, enter the command mode enrollment group as described in Section 6.3 and follow the operations listed in the following:

LCD DISPLAYS	ACTION REQUIRED
=ENROLL=	Press # (Yes) key
ENTER ID	Enter ID number (10 digit max.) followed by # (Ref. note 1 below).
PLACE HAND **1/3**	Place hand for reading 1. Hand must be removed to continue.
REMOVE HAND	Remove hand.

LCD DISPLAYS	ACTION REQUIRED
PLACE HAND 2/3	Place hand for reading 2.
REMOVE HAND	Remove hand.
PLACE HAND 3/3	Place hand for reading 3.
REMOVE HAND	Remove hand.
TIME ZONE (0)?	Enter the time zone for this user. Just press the # key to select the special time zone of 0.
	(ALWAYS). Otherwise enter the desired time zone from 1 to 61. Remember time zone 61 is the special zone (Never). (Ref. note 2 below).
=ENROLL=	This person is now enrolled. To enroll another person press # (Yes) and repeat the procedure. Press any numbered key to return to the ID verification mode.

NOTE 1: If an ID number is not accepted it is already in use and another number must be chosen. The display will say **SORRY, CAN'T ADD**.
NOTE 2: If the **PLACE HAND** display is shown three hand readings have been made. This means that one or more hand readings were not accepted and another hand reading is being requested to replace the rejected one. This procedure will continue until three acceptable hand readings have been enrolled. This request for additional hand readings rarely occurs.

The enrollment process can be terminated at any time by pressing the * key several times. Mistakes in entry can be erased by pressing the * key.

When all users have been enrolled, simply press any number key when the *** NO YES #** prompt is displayed and operation will revert to the identity verification mode.

Changes made at a network master reader using this command are transmitted to all readers on the network. Changes made using readers set as stand-alone or network remotes affect only those readers.

6.5.2 Remove User

To remove a user, enter the command mode enrollment group as described in Section 6.3 and choose the **=REMOVE=** command. You will then be prompted to enter the ID number of a user to be removed. If, after the ID number is entered, the number is replaced by **????**. It means that the ID number entered was not that of an enrolled user. Re-enter a valid ID number. Mistakes in entry can be erased by pressing the * key.

When the users have been removed, press any number key when the * NO YES # prompt is displayed and operation will revert to the identity verification mode.

Changes made at a network master reader using this command are transmitted to all readers on the network. Changes made using readers set as stand-alone or network remotes affect only those readers.

6.6 Management Group Commands

The management group commands are used for general system management operations.

6.6.1 Set Time and Date

The time and date is displayed in the second line of the display when the hand reader is in the identity verification mode.

To se the time and date, enter the command mode management group as described in Section 6.3 and choose the **=SET TIME & DATE=** command. Then enter the time and date when prompted.

6.6.2 List User Information

The ID numbers, individual reject thresholds, and assigned authority levels of enrolled users may be displayed on the hand reader display panel or printed

To display or print user information, enter the command mode management group as described in Section 6.3 and choose the **=LIST USERS=** command. You will then be prompted to choose the printer or hand reader display.

When user information is displayed or printed, the ID number is followed by the users reject threshold, authority level and time zone. A reject threshold of 000 means that the system reject level will be used for that user. For example:

```
1234   000   2
      01
```

is the display for user ID **1234**. The system reject threshold is used (**000**) and the user 1234's authority level is **2** and time zone is **01**.

```
4567   120   0
      00
```

is the display for user ID **4567**. An individual reject threshold level of **120** has been assigned and 4567's authority level is **0** and time zone is **0**.

6.6.3 Send Data to Network

This function is used to restore enrollment data to the network remote hand readers in the event of data loss. Data must first be restored to the network master reader using the BackHand software as described above. It is then downloaded to the network remote readers using this function. You may download to all readers at once, or to a selected reader. This command is available only for readers configured as a network master.

To send hand data to network remote readers, enter the command mode management group as described in Section 6.3 and choose the **=DATA TO NETWORK=** command. You will then be given the choice of sending the hand data to all of the readers on the network, or a selected reader.

6.6.4 Receive Data From Network

This function is used to restore the network master reader data from one of the network remote readers. When this function is selected, the user data stored in the specified reader will be transferred to the master reader. This function is available only for readers configured as a network master.

To retrieve hand data from a network remote reader, enter the command mode management group as described in Section 6.3 and choose the **=DATA FROM NETWORK=** command. You will then be asked to enter the reader number from which the hand data is to be retrieved.

6.7 Setup Group Commands

The setup group commands are used to set certain operating parameters.

6.7.1 Set Print Options

The set print option command allows you to enable or disable printing of valid accesses. If valid access printing is disabled only invalid access, alarms, and command mode operations will be printed.To enable or disable the printing of valid access messages, enter the command mode management group as described in Section 6.3 and choose the **=SET PRINT OPTIONS=** command. You will then be prompted to enable or disable the printing of valid access messages.

6.7.2 Set ID Mode

The “Set ID Mode” command is used to set the maximum length of the ID number, whether an account code will be requested, and whether a duress code can be used. To set these parameters, enter the command mode management group as described in Section 6.3 and choose the **=SET ID MODE=** command. You will then be prompted for the ID length, account code mode, and duress code mode as described in the three sections below. Simply enter the desired configuration.

6.7.2.1 ID Length

To set the ID length, enter the set ID mode as described in Section 6.7.2 above, and enter the desired length when so prompted.

The ID3D-R hand readers have a capacity for ID numbers up to ten digits long. Any number of digits from a single digit to the full capacity of ten can be used. Because of the capability to use a variable number of digits, it is in general necessary to press the # (Enter) key to indicate that the ID number has been entered. The set ID length command allows you to specify a lesser number of digits for the ID number. In this case, the # key need not be pressed to enter the ID number. After the specified number of digits have been entered, the ID number will be immediately processed. This feature is generally used when all or most of the ID numbers are of the same length. System throughput and operating convenience is then improved.

As an example, if the ID length were set to four, entering the valid ID number 1234 would cause the **PLACE HAND** prompt to appear immediately with no need to press the # key. With the ID length set to four, shorter ID numbers could be used, but the # key would have to be pressed. ID numbers longer than four digits could not be used.

6.7.2.2 Set T&A Mode (Time and Attendance)

To set the “T&A” mode and on or off, enter the set ID mode as described in Section 6.7.2 above. When the prompt **SET T&A MODE** is given, answer by pressing the # (Yes) key to enable this mode or the * (No) key to disable it.

When the “T&A” mode is enabled and a valid hand read is obtained, the hand reader display shows the following prompt:

1-IN	**2-OUT**
3-BACK	**4-JOB**

Clocking in or out is now accomplished just by pressing the one or two key. Coming back from break, lunch, or being called back can be entered by pressing the three key. In this case the following sub-menu is presented:

1-LUNCH 2-BREAK
3-CALL

Pressing the appropriate single digit logs the chosen transaction.

Job or department transfers can be recorded by pressing four at the first time and attendance menu. You will then be given the option of entering a job or department code. After selecting the desired option, you may enter any code up to nine digits long.

Time and attendance input as described above is sent to the hand reader printer and written to the hand reader datalog buffer for later retrieval by the host system. The time and attendance data is encoded as a ten digit number. The leftmost digit indicates the nature of the transaction as listed in the table below. The remainder of the digits are used for job or department numbers.

TIME AND ATTENDANCE CODES

0000000000	No T&A Data
1000000000	In
2000000000	Back From Lunch
3000000000	Out
4xxxxxxxxxx	Department Transfer
5000000000	Back From Break
6xxxxxxxxxx	Job Class Transfer
7000000000	Call Back

xxxxxxxxxx is Department or Job Code

When the time and attendance mode is enabled, the command mode can be entered by pressing the # key twice when the first time and attendance mode menu is presented. This will bring up the display of the password prompt. Entry of a valid password will access the command mode assigned that password.

6.7.2.3 Set Duress Code Mode

To set the duress code mode and duress character, enter the "Set ID" mode as described in Section 6.7.2. When the prompt **DURESS CODE** is given, enter the desired duress character as described below. If the duress code is to be disabled, press the * key. Press the # key when finished.

With the "Duress Code" mode enabled, an alarm is sounded if a user enters a prescribed single digit duress character as the first digit of the ID number. The alarm is printed and the auxiliary output can be programmed to operate in response to this alarm.

****IMPORTANT**** **The chosen duress charcter may not be used as the first digit of an assigned ID number. For example, if the chosen duress character were eight, no ID numbers beginning with eight would be permitted. Zero is a convenient duress character.**

6.7.3 Set Reader Mode

This command is used to set the operating mode of the reader to stand-alone, network master, or network remote. The functioning of each of these modes is described elsewhere in this manual.

To set the reader mode, enter the command mode management group as described in Section 6.3 and choose the **=SET READER MODE=** command. You will then be given a choice of modes. Answer # (Yes) to the desired choice, or * (No) to skip to the next choice.

If you select remote as the reader mode, you will then be prompted to set the remote address for the reader. All remote hand readers on a network must have their address set to a different number. If another hand reader is used as the network master, then the remote addresses must all be in the range 0 to 30.

The ready display is different for each of the operating modes as shown below. This makes it easy to tell at a glance the current operating mode of any reader.

Stand-Alone	***READY***
Network Master	===READY===
Network Remote	---READY---

6.7.4 Set Output Mode

The "Set Output Mode" command allows the output mode of the reader to be set for either card reader emulation or lock and auxiliary output control. When you select this option you will be asked to choose either one of these modes. Only one mode is available at a time.

If the hand reader is interfaced to a host access control system using card reader emulation, then select the card reader output mode. If the hand reader is to control a lock directly, choose the lock and auxiliary mode.

To set the output mode, enter the command mode management group as described in Section 6.3 and choose the **=SET OUTPUT MODE=** command. You will then be given a choice of modes. Answer # (Yes) to the desired choice, or * (No) to skip to the next choice.

6.7.5 Set Lock/Shunt Time

The "Lock/Shunt Time" command is used to set the unlock time and the alarm shunt time. The unlock time determines how long the door lock will remain unlocked in response to a valid access request. The door shunt time determines how long the door alarm circuits will be disabled in response to a valid access request.

To select this command, enter the command mode setup group as described in Section 6.3, and choose the lock/shunt time command. You will then be prompted to enter new unlock and alarm shunt times. The currently set times will be displayed. Simply enter the new time in seconds, or just press # for no change.

6.7.6 Auxiliary Output Setup

This command is used to specify those conditions that will cause the auxiliary output circuit to activate and clear. This command is effectively only if the output mode is set to lock and auxiliary. This command has no effect if the output mode is set for card reader emulation. The circuit can be activated by the following:

Time Zone, Duress Alarm, Door Alarm, Auxiliary Input, Activation, Invalid Access Attempt, Tamper Alarm

The circuit can be cleared by:

Timer and Valid Access

To select this command, enter the command mode setup group as described in Section 6.3, and choose the **AUX OUT CONTROL** command. Prompts which must be answered with a # (Yes) or * (No) will appear for the activation conditions. The current state of each of these will also be displayed. Simply press # (Yes) or * (No) at each prompt to select the desired activation conditions. Next you will be similarly prompted for the conditions that will reset the auxiliary output.

6.7.7 Set Site Code

This command is used to set the site (facility) code. The site code will be transmitted from the card reader emulation port when the hand reader is used in its card reader emulation mode and the ID number is entered from the keypad. In this case, the emulated card data that is transmitted includes a site code field and an ID number field. The value entered using this command is placed in the site code field and the ID number entered on the keypad is placed in the ID number field. If a card reader is used, then whatever site code is on the card is transmitted as read.

To select this command, enter the command mode setup group as described in Section 6.3, and choose the set site code command. The display will show the current site code and you will be prompted to enter a new one. To keep the site code, simply press the # (Enter) key. Enter a new site code followed by the # key.

6.7.8 Set Serial Baud Rate

This command is used to set the baud rate of the serial channels. The baud rate for Channel Zero must always be set the same for all readers on the network. Typically this is set to 9,600 baud (baud code two). The baud rate for Channel One must be set to whatever baud rate is required by the printer.

To select this command, enter the command mode setup group as described in Section 6.3 and select the set serial command. You will be prompted for the baud rate code. Enter a single digit for the desired baud rate according to the table below.

Table 6.8.4 Baud Rate Codes

BAUD RATE	CODE	BAUD RATE	CODE
38.4 K	0	19.2 K	1
9600	2	4800	3
2400	4	1200	5
600	6	300	7

6.7.9 Set Beeper Mode

The HandKey hand readers contain an audible beeper which produces a short tone whenever a key is pressed, and several different distinctive tone patterns when a hand read is complete, or a second hand read is required, or some operating error is made. If desired, this tone can be turned on or off using this command.

To select this command, enter the command mode setup group as described in Section 6.3, and choose the **==SET BEEPER==** command. You will be prompted to change the current beeper mode. Simply press # (Yes) to change the mode or * (No) to leave it the same. Changing the mode will turn the beeper off if it was on or if it was off.

6.8 Service Group Commands

The service group commands are used for service and diagnostic functions

6.8.1 Check and Calibrate

Proper camera alignment is important for accurate identification, as is proper setting of the camera exposure time. The camera exposure is automatically set when power is first applied.

The camera alignment can be checked, and the exposure time re-calibrated by entering the service mode setup group as described in Section 6.3, and choosing the **==CALIBRATE==** command. When using this command the measuring surface and mirrors should be clean and ree from foreign objects.

When the calibrate command is chosen, the row (r=) and column (c=) calibration error will be displayed, along with the exposure time (e=). The row and column error should be zero, plus or minus four or damage to the unit is indicated in which case, the factory should be consulted. The exposure should be a positive number. If the exposure is a negative number, the factory should be notified.

On the second line of the display the prompt

recal (Y#/N*)?:_

will be displayed. If the # (Yes) key is pressed, the camera exposure will be re-calibrated. Any other key will exit the command. If the re-calibrate option is chosen, the platen must be clean and free from all foreign objects.

6.8.2 System Status Display

The system status display is useful in checking out an installation. When this selection is made the status of all input monitoring circuits is shown. The systems status display can be enabled by entering the service mode setup group as described in Section 6.3 and choosing the **=STATUS DISPLAY=** command. You will then be prompted to turn the status display on or off.

With the system status display turned on, the second line of the display will show the system status code whenever

*****READY*****

is displayed in the verification mode.

```
***READY***
OCCO    14
```

The system status code indicates the status of all monitored circuits by displaying a C for closed or an O for open for each of the circuits. From left to right in the display, the circuits are:

Tamper Switch, Door Switch, Auxiliary Input, Request to Exit Switch

The numerical indication on the right is the hand measurement deviation (score) from the enrollment value for the most recent hand reading. If this number exceeds the reject threshold, the person will be denied access. Consistently high scores (greater than 50) may indicate that the enrollment was not properly performed or that the user is not following proper hand placement procedure. In this case, re-enroll the user paying particular attention to hand placement.

The status display is updated twice per second.

NOTE: Depending on firmware version, other numbers or symbols may be displayed on the status line. These should be ignored.

6.8.3 Network Status

Selecting this function will cause the display to show the status of the network. The top line of the display will indicate whether the display is for network remote readers 0-15 or readers 16-31. The bottom line of the display will show a string of 16 characters, each character either an O or a period. The 16 characters represent the state of the 16 indicated network remote readers. The leftmost character represents the first remote, the next character the second, and so on. If the remote is online, the character displayed will be an O; if it's not, the period is displayed. The display is refreshed twice per second. This display is useful during initial system setup.

When this command is selected, the first line of the display will indicate that the status is being displayed for readers 0-15. Pressing any key on the keypad will advance the display to readers 16-31. Pressing a key again will exit the network status display.

7.0 Maintenence

7.1 Cleaning

The only routine maintenence required for the ID3D-R is cleaning. The platen surface upon which the hand is placed, the side view mirror and the overhead blue window should be cleaned with reasonable frequency. As the hand reader is used, oil from hands builds up on the platen surface, and, at a certain point, becomes objectionable from the standpoint of both hygiene and function. These surfaces should be cleaned with a soft cloth moistened with a simple glass cleaner such as Windex®. Do not spray the cleaner directly on the hand reader. The hand reader should be cleaned about once a week.

7.2 Top Panel Removal

In order to replace failed parts, it is necessary to remove the top (display) panel from the hand reader. To do this, follow the steps below.

1. Remove power from the unit.
2. If a wall mount kit is used, remove unit from wall mount enclosure; otherwise, remove back cover.
3. Locate the two fastening nuts inside of the unit at the rear edge of the top panel and remove.
4. Gently pry up the rear edge of the top panel until access is gained to the printed circuit card.
5. Use the location chart at the rear of this manual to locate the desired items.

7.3 Setup and Hand Memory Reset

Most system setup values such as passwords and door unlock times are stored in a special non-volatile memory. Users' enrolled hand data is stored in battery protected memory which is retained even in the event of power loss. At certain times it may be required that the setup memory be restored to factory default conditions, or that all users hand data be cleared from memory. This is most often the case with demonstration hand readers as passwords may be inadvertently changed and forgotten, or users who are no longer present may be the only enrolled users, preventing others from using the system.

A circuit card dip switch (SW1) is provided which allows both the setup memory to be reset and the user's hand data memory to be cleared when power is applied to the hand reader. If this dip switch #4 is in the on position and the tamper switch is also depressed, the reader setup data along with the users hand data will be cleared when power is applied. This can be accomplished by holding the tamper switch closed or closing the rear door. If the tamper switch is not depressed, the hand data memory is not cleared. For demonstration systems, it is recommended that the memory reset dip switch be left in the on position so that the HandKey is always restored to the factory default conditions upon turning power on.

1. Turn off power to the unit. Remove rear door or remove from wall mount housing.
2. Locate the memory reset dip switch and move the switch to the on position. The memory reset dip switch location is shown on the “Parts Location” drawing in Appendix D of this manual.
3. Restore power to the hand reader. Hold tamper switch closed if hand memory is to be cleared.
4. When the display shows **READY**, remove power.
5. Move the SW #4 to the off position.
6. Replace the back cover or place unit into wall mount enclosure.
7. Restore power.

7.4 Memory Battery Replacement

****IMPORTANT**** **Removing the battery will cause all hand data to be erased. Be sure that the hand data is backed up on disk before removing the battery.**

Remove the top panel as described above. Locate and romove the battery. When removing the battery, **DO NOT PRY UP THE BATTERY RETAINING CLIP.** Push the battery out of its holder using a small screw driver or other object, pushing from the closed end of the retaining clip. Slide the new battery into the holder with the **+ SIDE OF THE BATTERY UP.**

****IMPORTANT**** **Do not operate the HandKey with the battery out of the battery holder on the circuit board as this will damage the circuit board and render the HandKey inoperable.**

7.5 Output Circuit Driver Replacement

In the event that the lock or auxiliary output, or the card reader emulation output does not function, the problem may be due to a bad output driver circuit. Such a failure may be caused by a short circuit or other overload of the driver circuit. This circuit consists of a single socketed integrated circuit.

To replace this circuit, first secure a suitable replacement part. The part type is shown on the parts locator chart at the rear of this manual. Locate the driver circuit, remove, and replace. Be sure that the replacement circuit is inserted in the socket in the correct orientation.

7.6 Serial Channel Driver Replacement

In the event that a serial communications channel does not work, the problem may be due to a defective serial transmitter or receiver circuit.

To replace these components, first secure suitable replacement parts. The part type is shown on the “Parts Location, Replaceable Parts, Jumper Block Location” drawing in Appedix “D” of this manual. Remove the top cover as described above, and locate the component to be replaced. Remove the defective component and replace. Be sure that the component is inserted in the socket in the correct orientation.

7.7 Power Converter Replacement

The power converter provides plus and minus voltage for the operation of the camera and serial communication circuits. A check of the functioning of the power converter can be made by measuring the voltage at the RS-232 TXD terminal five of the terminal strip. The voltage at terminal five should be about eight volts negative with respect to ground.

To replace this component, first secure a suitable replacement part.The part type is shown on the “Parts Location, Replaceable Parts, Jumper Block Location” drawing in Appendix D of this manual. Remove the top cover as described above and locate the component to be replaced. Remove the defective component and replace. Be sure that the component is inserted in the socket in the correct orientation.

7.8 Prom Chip Replacement

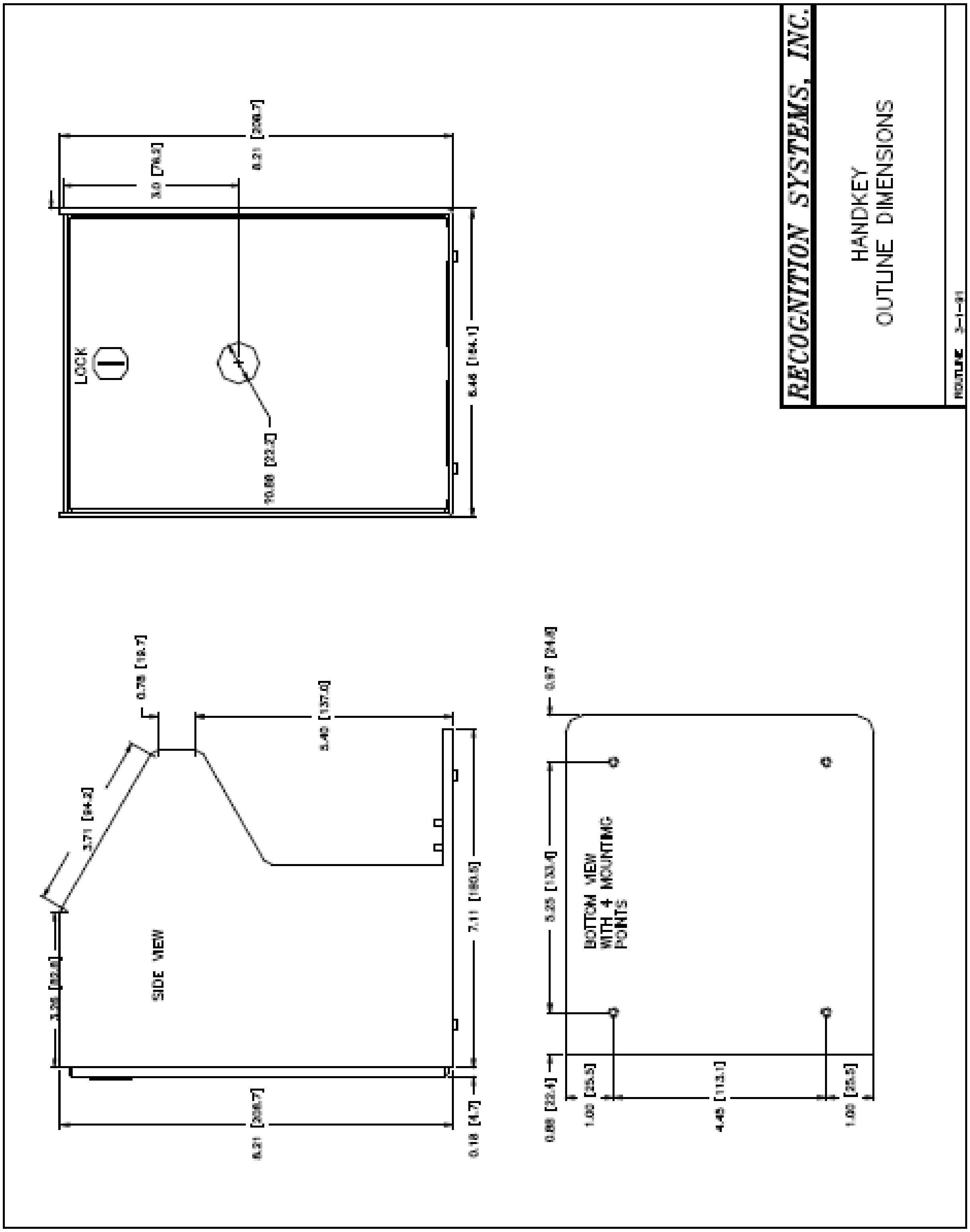
The PROM chip contains the firmware program for the hand reader and thus determines its complete function. The PROM may be changed to upgrade to a later version or a different model.

To change this component, remove the top cover as described before and locate the PROM chip using the “Parts Location, Replaceable Parts, Jumper Block Location” drawing in Appendix D of this manual. Remove the chip and replace. Be sure that the PROM is inserted in the socket in the correct orientation, exactly the same as the chip that is being removed. Before removing the chip, note that one end is notched in the middle. The notch end of the replacement chip must be positioned the same.

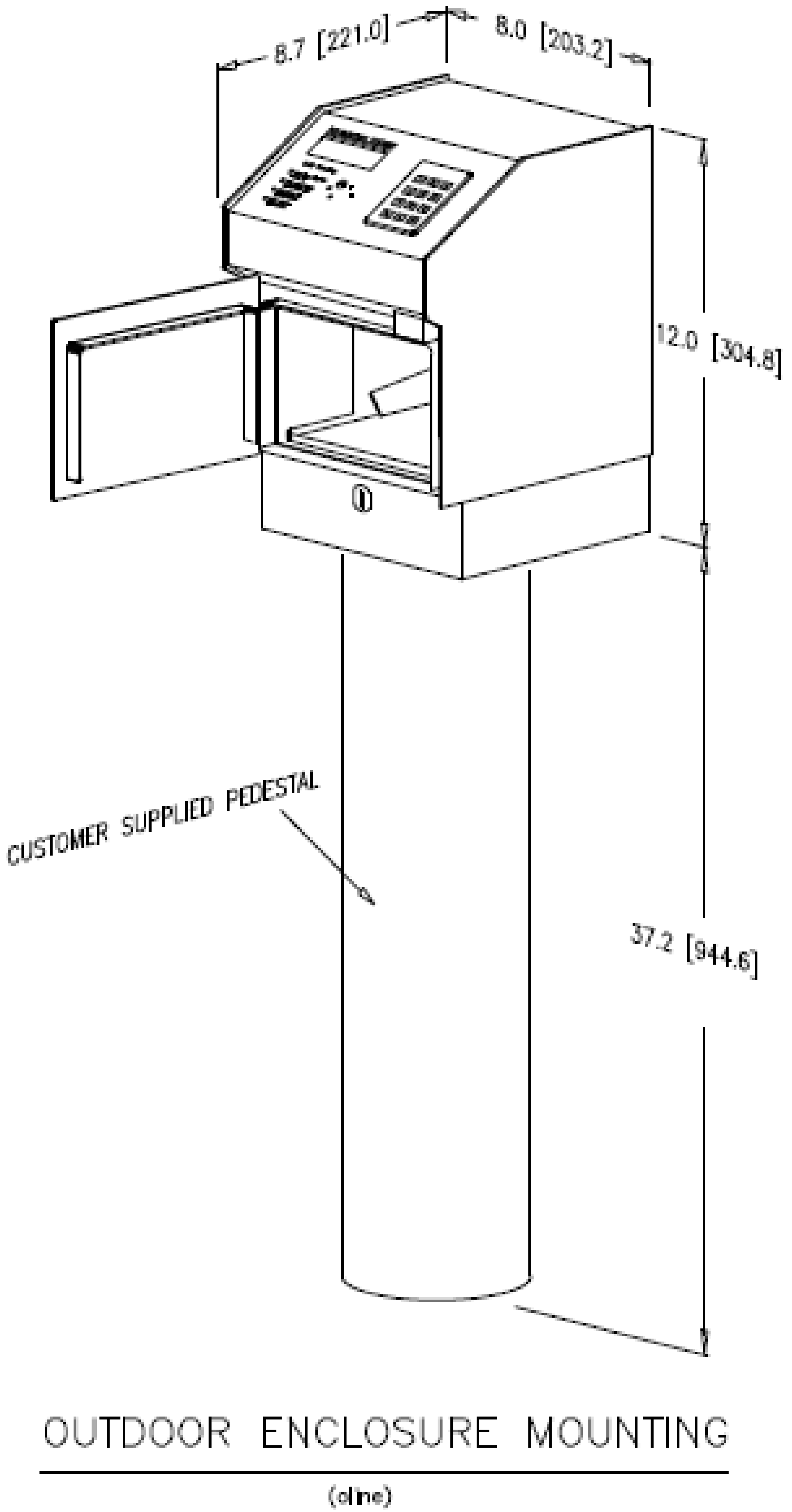
It is also necessary to reset the setup memory following the procedure given above. Once this is done, the setup values required for your installation should be re-entered.

Appendix D

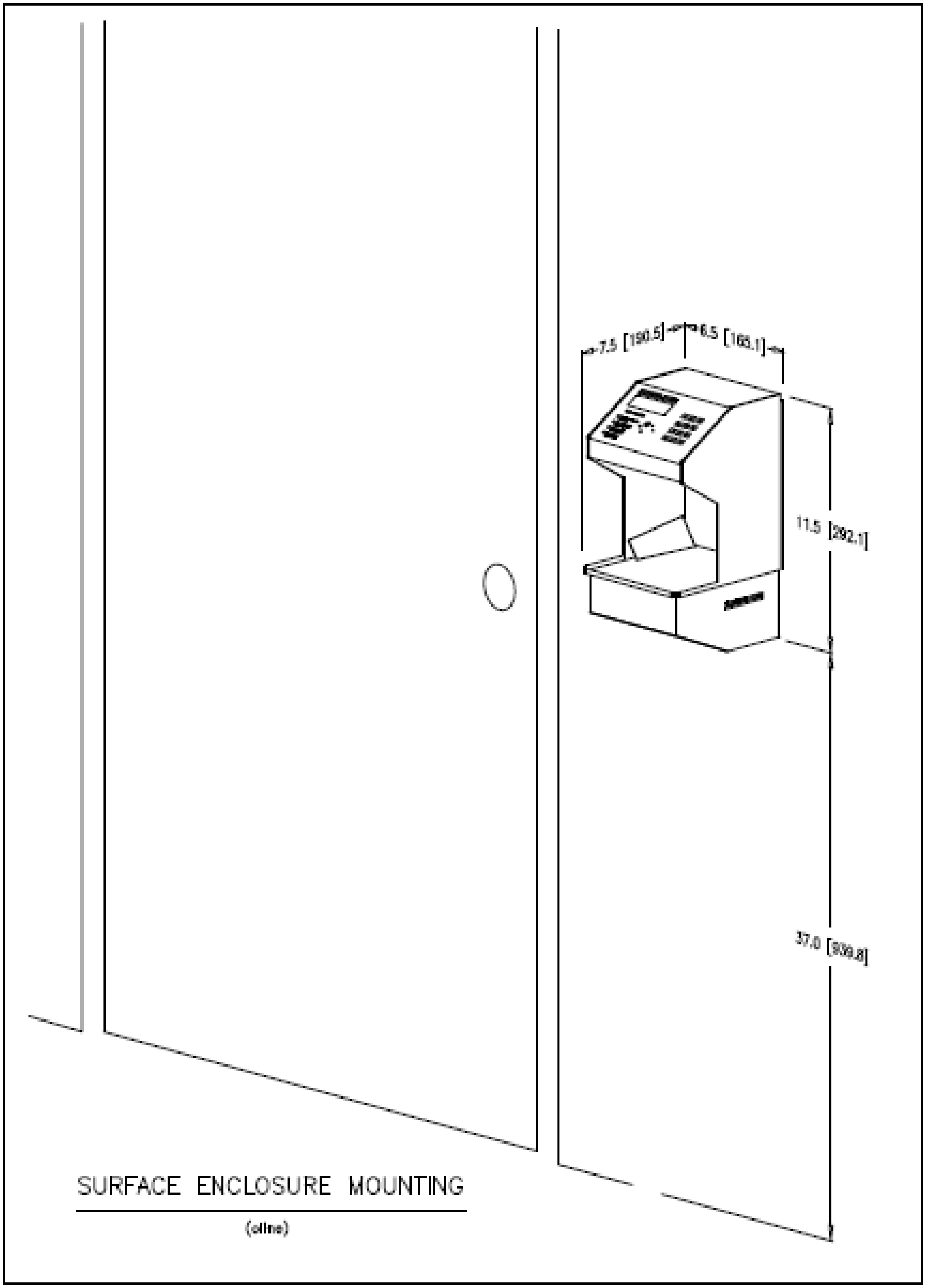
Contents:



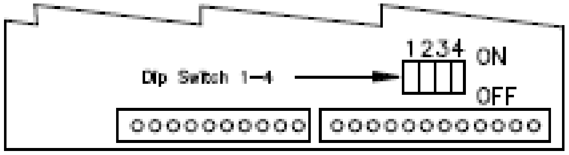
ID3D-R Outline Dimensions



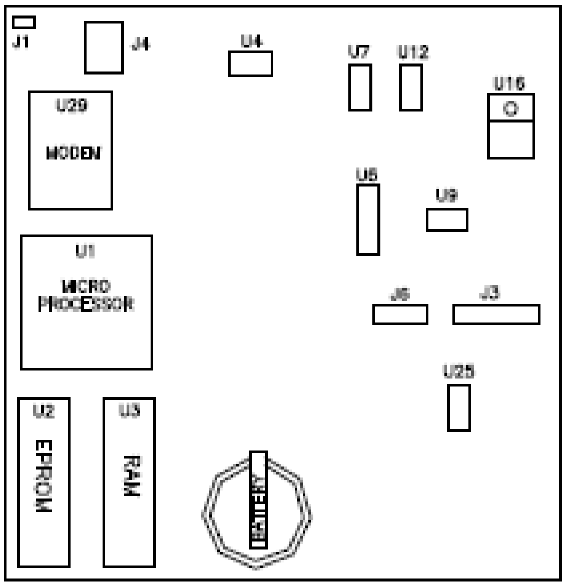
ID3D-RW Enclosure Mounting



ID3D-R/WM-201 Mounting



CIRCUIT CARD – UNDERSIDE VIEW



CIRCUIT CARD – COMPONENT SIDE

DIP SWITCH SETTINGS

SW 1: ON = RS–422(TX) END OF LINE RESISTOR FOR HAND READER LOCATED AT PHYSICAL END OF RS–422 NETWORK.
OFF = ALL OTHER HAND READERS ON THE RS–422 NETWORK.

SW 2: ON = RS–422(RX)/485 END OF LINE RESISTOR FOR HAND READER LOCATED AT PHYSICAL END OF RS–422 OR 485 NETWORK.
OFF = ALL OTHER HAND READERS ON THE RS–422 OR 485 NETWORK.

SW 3: ON = CHANNEL 0 SET FOR RS–485 COMMUNICATIONS.
OFF = CHANNEL 0 SET FOR RS–422 COMMUNICATIONS.

SW 4: ON = MEMORY WILL BE RESET WHEN POWER IS APPLIED TO HAND READER.
OFF = MEMORY IS SAVED WHEN POWER IS APPLIED TO HAND READER.

INTEGRATED CIRCUITS:

U1:	MICROPROCESSOR
U2:	EPROM/FIRMWARE
U3:	RAM
U4:	LOCK OUTPUT
U6:	CHANNEL 1 RS–232
U7:	RS–485 TRANSCEIVER/RS–422 RECEIVER
U9:	14v CAMERA POWER SUPPLY
U12:	RS–422 TRANSMIT
U16:	5v POWER SUPPLY
U25:	NVRAM
U29:	MODEM (OPTIONAL)

CIRCUIT BOARD JACKS:

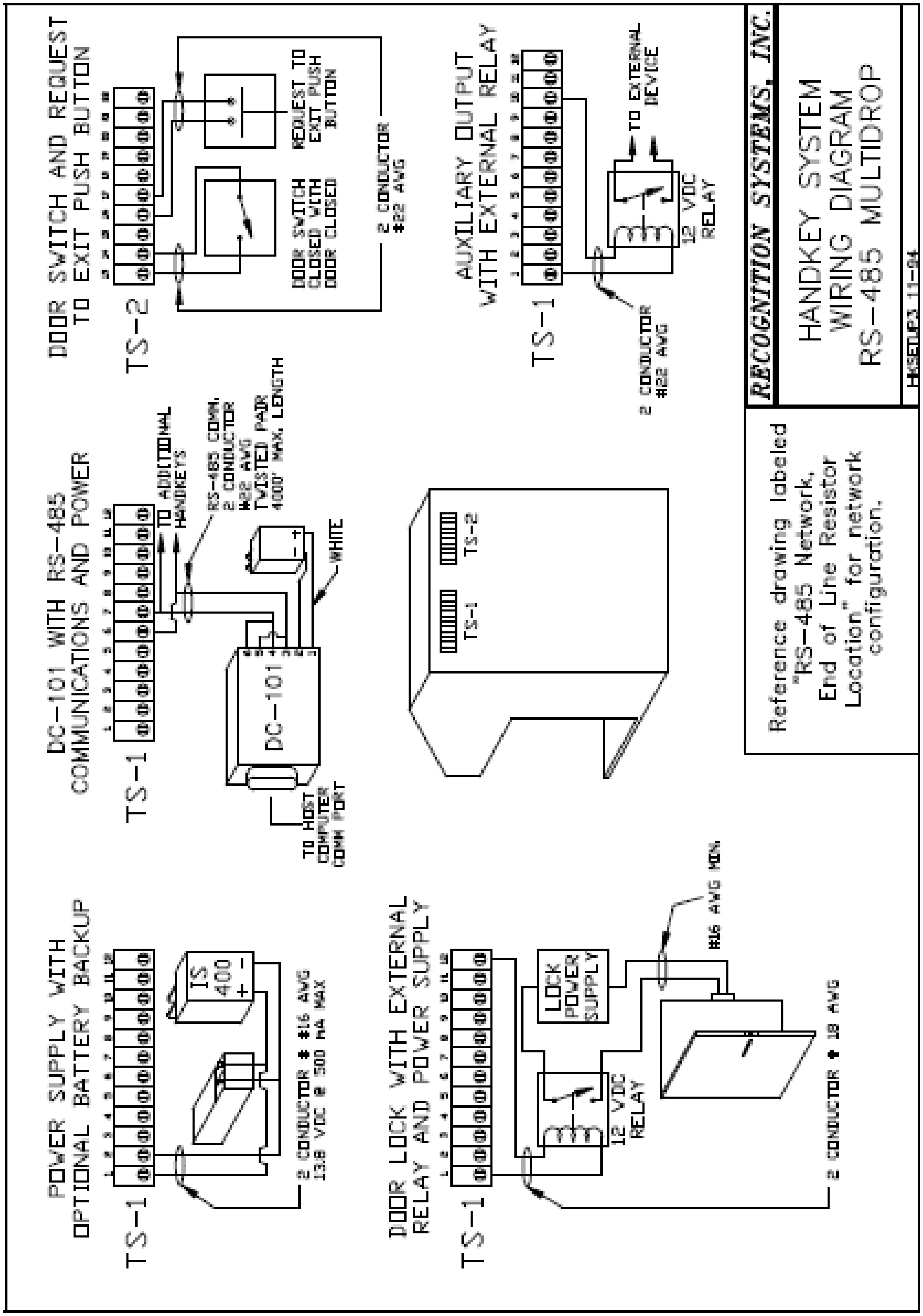
J1:	TAMPER SWITCH INPUT
J3:	LCD RIBBON CABLE
J4:	MODEM PHONE LINE
J6:	KEYPAD RIBBON CABLE

RECOGNITION SYSTEMS, I

PARTS LOCATION
REPLACEABLE PARTS
DIP SWITCH LOCATION

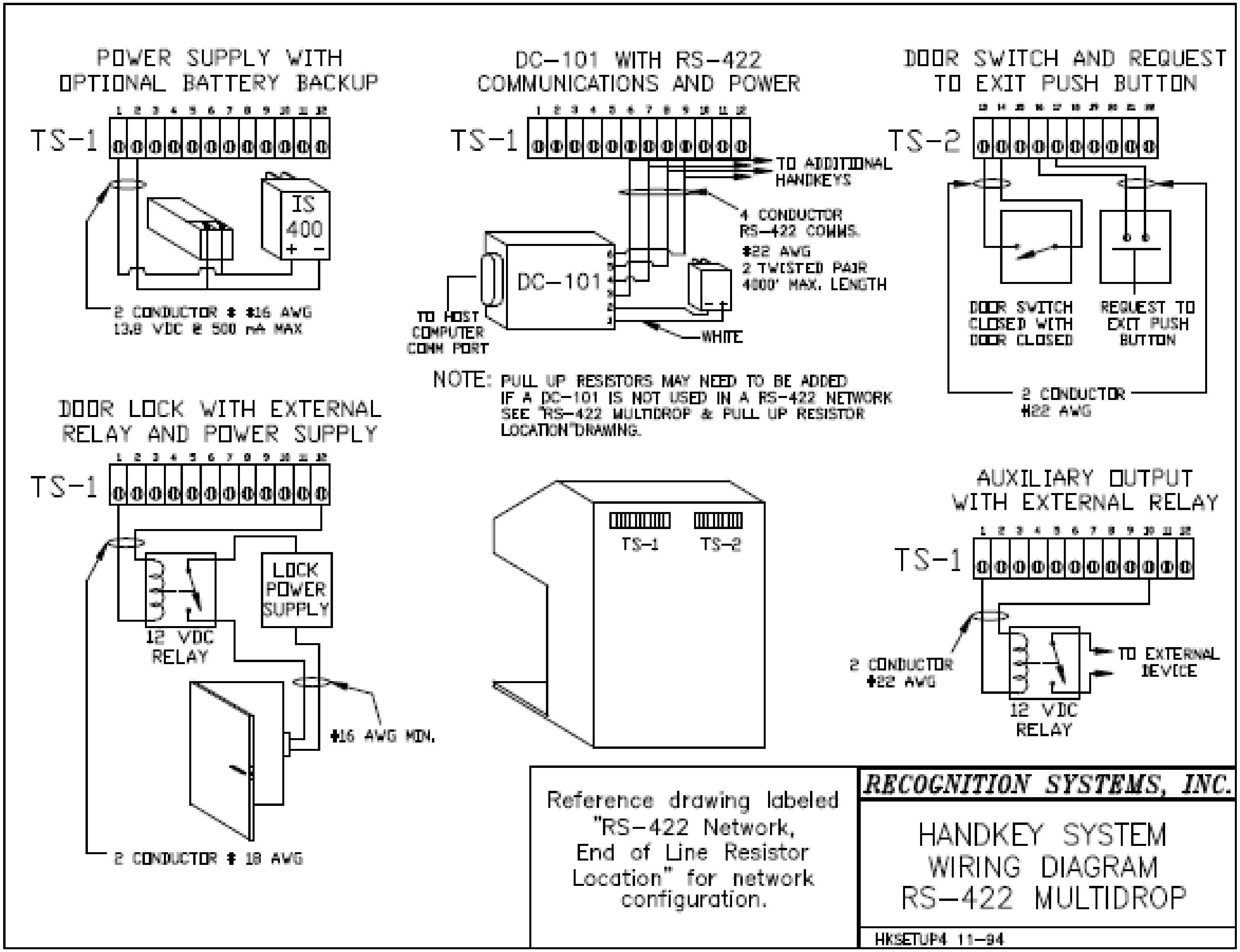
PLOCEBO 2–96

Parts Location, Replaceable Parts, Dip Switch Location

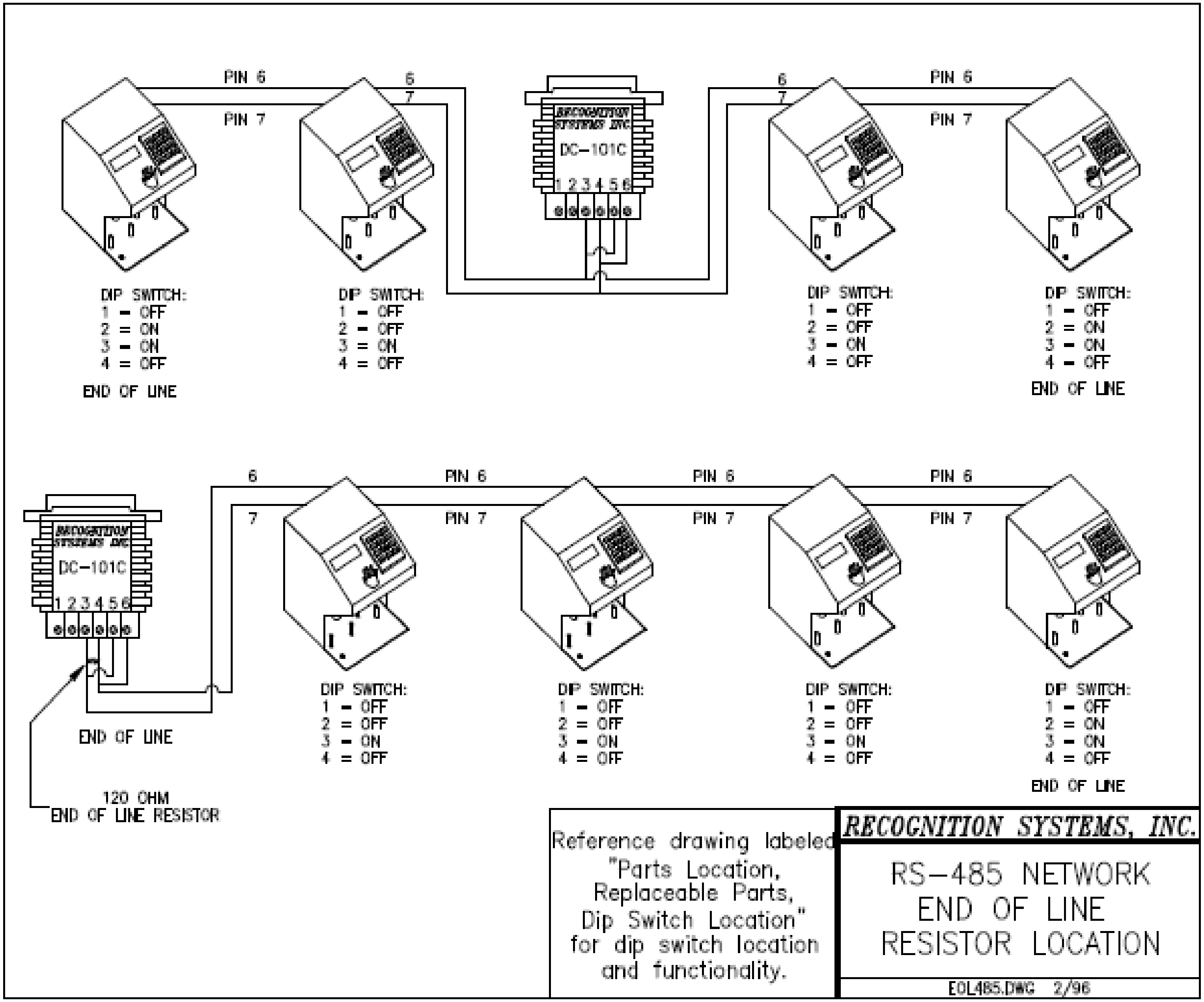

POWER SUPPLY WITH OPTIONAL BATTERY BACKUP
TS-1
IS 400
+
-
2 CONDUCTOR # #16 AWG 13.8 VDC @ 500 MA MAX
DOOR LOCK WITH EXTERNAL RELAY AND POWER SUPPLY
TS-1
LOCK POWER SUPPLY
12 VDC RELAY
#16 AWG MIN.
2 CONDUCTOR # 18 AWG
DC-101 WITH RS-485 COMMUNICATIONS AND POWER
TS-1
DC-101
TO HOST COMPUTER COMM PORT
TO ADDITIONAL HANDKEYS
RS-485 COMM, 2 CONDUCTOR #22 AWG TWISTED PAIR 4000' MAX, LENGTH
WHITE
TS-1
TS-2
DOOR SWITCH AND REQUEST TO EXIT PUSH BUTTON
TS-2
DOOR SWITCH CLOSED WITH DOOR CLOSED
REQUEST TO EXIT PUSH BUTTON
2 CONDUCTOR #22 AWG
AUXILIARY OUTPUT WITH EXTERNAL RELAY
TS-1
TO EXTERNAL DEVICE
12 VDC RELAY
2 CONDUCTOR #22 AWG
RECOGNITION SYSTEMS, INC.
HANDKEY SYSTEM WIRING DIAGRAM RS-485 MULTIDROP
HKSETUP3 11-94

Reference drawing labeled "RS-485 Network, End of Line Resistor Location" for network configuration.

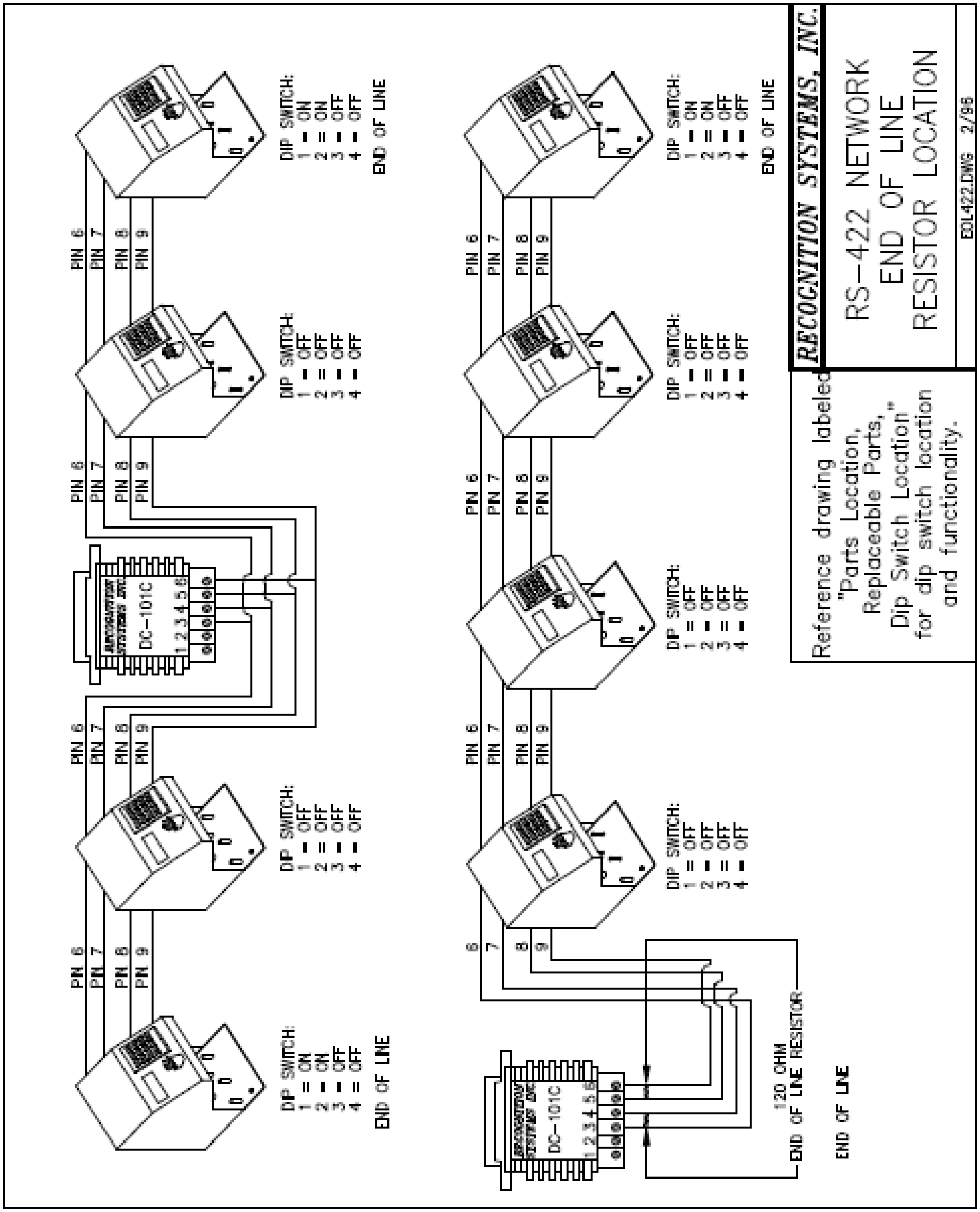
HandKey System Wiring Diagram - RS-485 Multidrop



HandKey System Wiring Diagram - RS-422 Multidrop

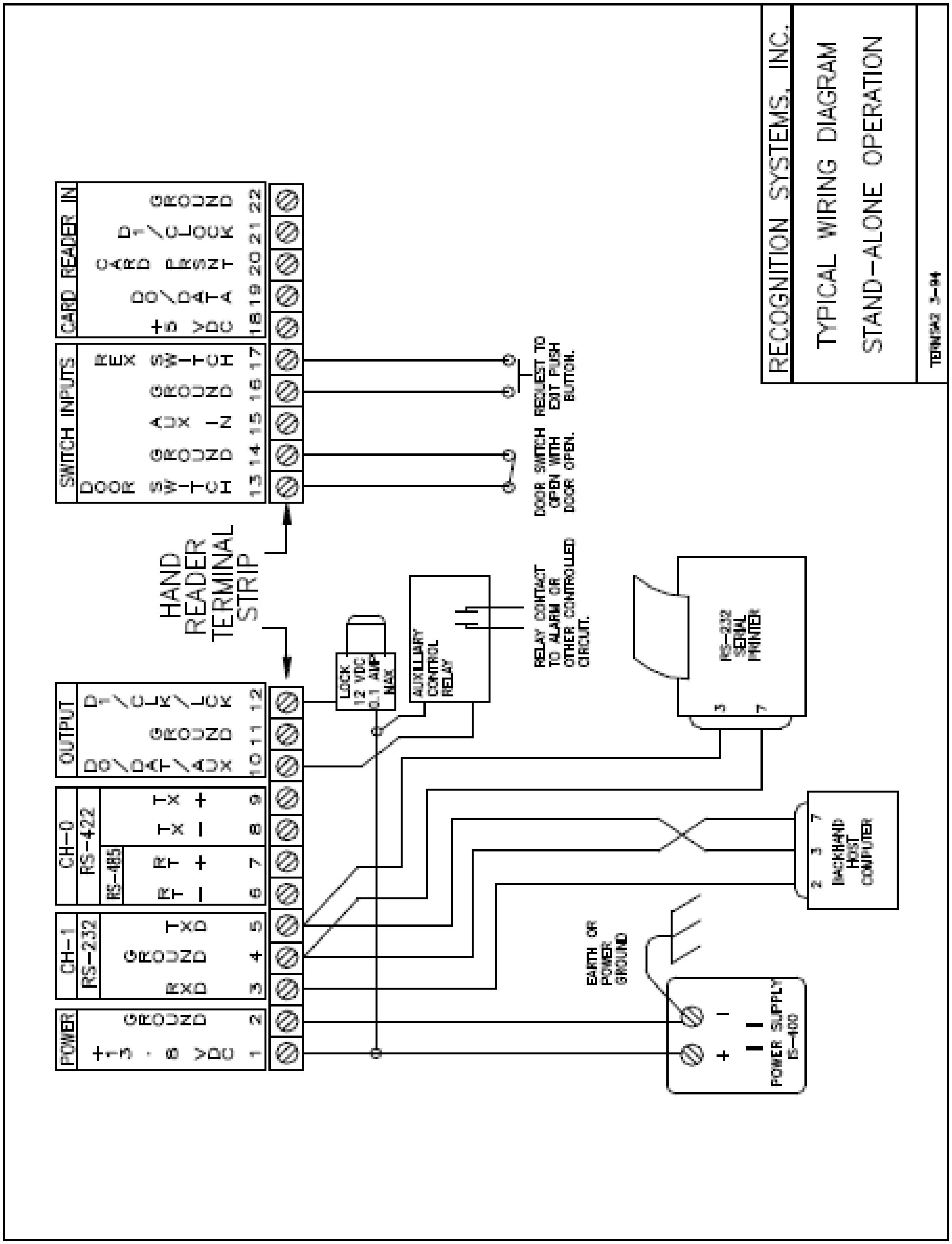


RS-485 Network, End of Line Resistor Location

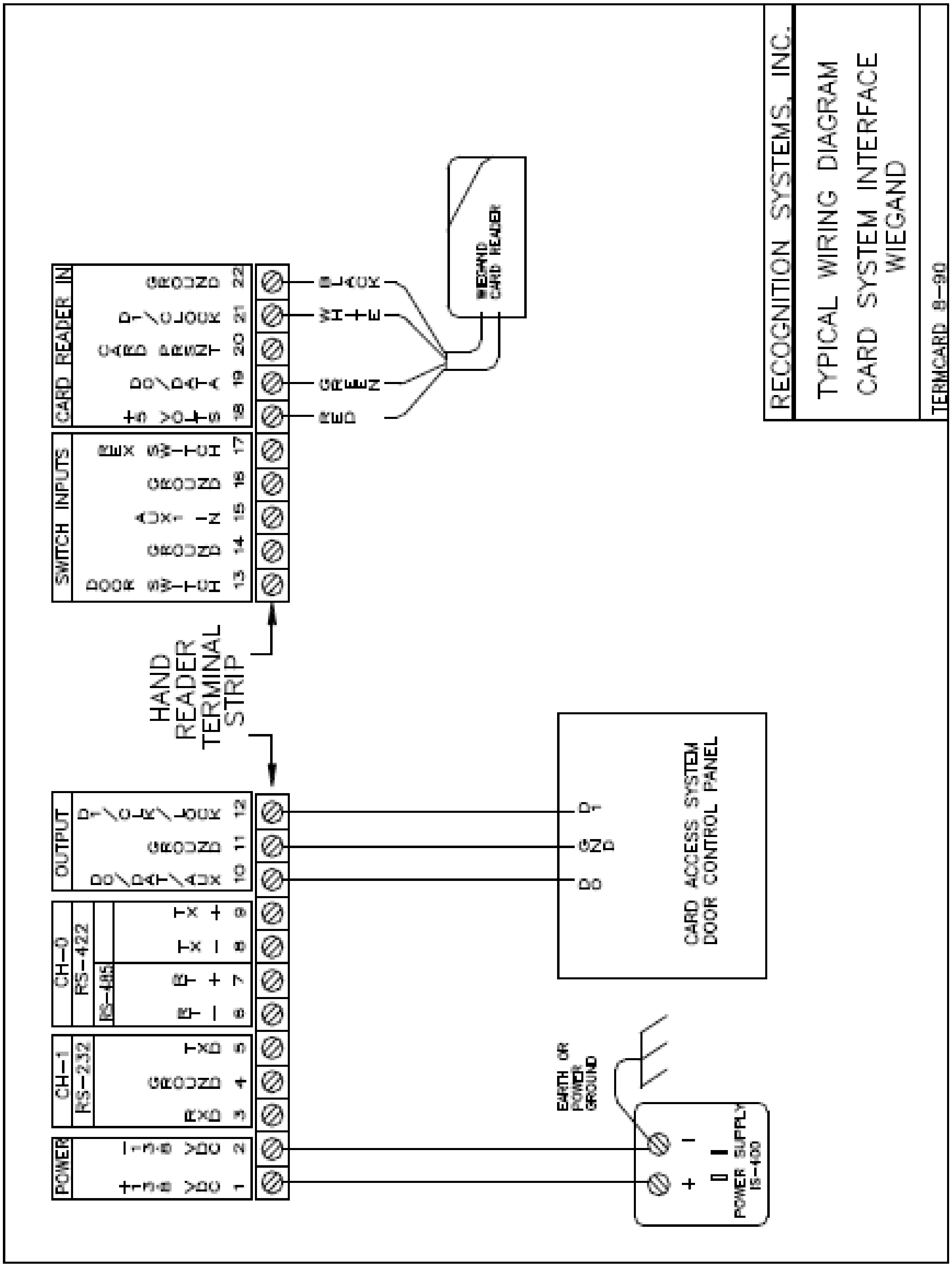


Reference drawing labeled "Parts Location, Replaceable Parts," Dip Switch Location" for dip switch location and functionality.

RS-422 Network, End of Line Resistor Location



Typical Wiring Diagram Stand-Alone



Typical Wiring Diagram Card System Interface

Index

Ingersoll Rand
Security Technologies

Ingersoll Rand's Security Technologies Sector is a leading global provider of products and services that make environments safe, secure, and productive. The Sector's market-leading products include electronic and biometric access control systems; time and attendance and personnel scheduling systems; mechanical locks and portable security, door closures and exit devices, steel doors and frames, architectural hardware and technologies and services for global security markets.

408.341.4110

www.schlage.com www.ingersollrand.com

Schlage
Biometric Solutions
Ingersoll Rand Security Technologies
1520 Dell Avenue
Campbell, CA 95008
Office: 866-861-2480/512-712-1413 (international)
Fax: 866-303-1794/408-341-4111
E-mail: sbssupport@irco.com

SCHLAGE

FingerKey

Terminal User's Guide

Ingersoll Rand
Security Technologies

Table of Contents

Using the HandNet Lite/FingerKey Product CD

Software on this CD

HandNet Lite: This program manages your users (and their biometric finger templates), and lets you set up and maintain your FingerKey network.
FingerKey Update: This utility is used to update firmware in your FingerKey reader.
FingerKey Backup/Restore: This is used to backup or restore a single FingerKey, including setup information and the user database.

Installing HandNet Lite

Important: HandNet Lite requires Windows 2000 SP4 or Windows XP SP1 to install.

Before installing, you should also install any critical Windows Updates. To do this, on your *Start* menu, pick *Programs*, and choose *Windows Update.*
HandNet Lite requires the .NET 1.1 framework to work. The installer asks you to install .NET 1.1. Always click *Yes* unless you are sure you already have it.

1. Using *My Computer* or *Windows Explorer*, find the CD Drive and double-click the CD icon.
2. Double-click the *HandNet_Lite* folder.
3. Double-click *Setup.exe.* You may wish to read the *Release Notes* files first.
4. Answer the installation questions; we recommend accepting the default settings on each screen.
   Some of the delays during the installation can seem long; please be patient as the Microsoft dotNet framework and MSDE SQL Server are installed.
5. After the installation is done, you'll be asked to restart (reboot) your computer. You must do this before you can start HandNet Lite.

Installing the FingerKey Update Utility

If you had an earlier version of this utility: Go to your *Control Panels*, choose *Add/ Remove Programs*, and remove any earlier version of this program before installing.

1. Using *My Computer* or *Windows Explorer*, find the CD and double-click the CD icon.
2. Double-click the *FK-Update* folder.
3. Double-click *Setup.exe.*
4. Follow the prompts on the screens.

The firmware on the FingerKey (v. 1.10) is on the CD in the FK-Firmware folder.

Installing the FingerKey Backup/ Restore Utility

If you had an earlier version of this utility: Go to your *Control Panels*, choose *Add/ Remove Programs*, and remove any earlier version of this program before installing.

1. Using *My Computer* or *Windows Explorer*, find the CD Drive and double-click the CD icon.
2. Double-click the *FK-BackupRestore* folder.
3. Double-click *Setup.exe* file.
4. Follow the prompts on the screens.

Documentation on this CD

- FingerKey Installation and Operation Guide
- HandNet Lite Read Me
- HandNet Lite Release Notes
- HandNet Lite User Guide

Introduction

What the FingerKey Does

The FingerKey stores a mathematical representation of the fingerprint and uses this numerical “picture” to confirm user identity. When the FingerKey recognizes a user’s fingerprint, it notifies an access control panel, which in turn sends a signal that unlocks the appropriate door. Depending on the type of access control panel, the panel may also control other systems like alarms, lights, and closed circuit cameras.

The FingerKey communicates with access control panels using Wiegand or Clock/Data.

The FingerKey initially is configured to store up to 50 users. You can purchase memory upgrades to enable it to store additional users.

How FingerKeys Recognize User Fingerprints

FingerKeys shine a light on the finger to capture a mathematical “image” of finger contours based on how the light reflects back. This numerical representation of the fingerprint, which we call a template, identifies details like bifurcations, ridge endings, and crossovers. The reader stores this template and associates it with the user’s ID number.

When a user wants to gain access, he/she enters an ID number (either by typing it in or by using a card reader). The reader asks the user to place a finger on the reader, and the reader then checks to see if the fingerprint matches the fingerprint template stored for that user. The reader notifies the access control panel about whether there was a match, and the access control panel then grants or denies access and takes other action as appropriate.

Networking Readers

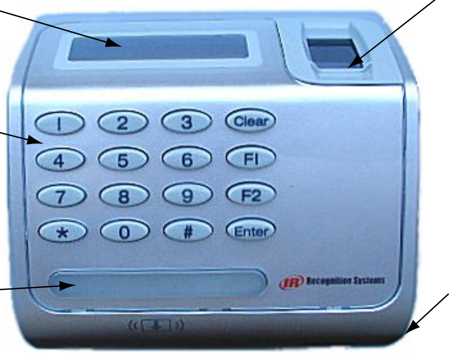
FingerKey readers can be used independently, or they can be networked with other FingerKey readers. If you network the readers, you can enroll users in one reader and then transfer those users to the other readers; this lets you enroll each user once instead of having to manually enroll each user at each reader.

FingerKey Features

The LCD display shows messages and programming menus.

The keypad allows users to enter ID numbers. It also allows for reader set-up.

Red/green/amber verifcation LEDs quickly show users if the finger was recognized, and flash other warning and status signals.



Guides help users place their fingers correctly on the sensor window.

The internal card reader provides for convenient ID entry.

An internal beeper provides audible feedback.

Figure 2-1: Finger Key Features

Setup Overview

1. If you haven't done so already, get the appropriate access control panel and electrified door hardware (lock, door position switch, request to exit, etc.).
2. Install the reader on the wall by the door; see page 6.
3. Wire the reader and connect it to your access control panel; see page 9
4. Design an ID numbering system; see page 15.
   A properly designed ID numbering system makes the reader faster and easier to use.
5. Add/enroll your supervisory staff.
   This includes users who are authorized to program the reader, users who access the reader through software, and users who will enroll new users to the reader. The process for enrolling these users is the same as for enrolling other users; see page 21.
6. Set authority levels for your supervisory staff; see page 16.
   This makes sure that these users have access to the options in the reader that they need, and it also prevents other users from being able to inappropriately access the reader menu options.
7. Customize settings in the reader as needed.
   Use the programming menus in the reader; see page 33.
8. Enroll the users who should have access through the door associated with the reader; see page 21.

Installing the FingerKey

Before You Begin

Tools You Need for the Installation

To install the reader, you need:

- a measuring tape
- a torx screwdriver
- wiring tools.

What You Need in Addition to the Reader

In addition to the FingerKey, you need:

- Electrified door hardware: Electronic lock, door position switch, request to exit, etc.
- Access control-panel: The reader can't communicate directly with a lock; it must communicate to an access control panel.

Protecting the Reader during the Installation

Protect the reader from the dust and debris generated during the wall plate installation process.

Choosing the Location for the Reader

Before you begin installation, check the site blueprints, riser diagrams, and specifications for important information about reader location. Look for any existing wall preparations and wiring that other contractors may have installed for the reader.

The reader's sensor window may be from 40–48 inches (102–122 cm) from the floor. For best performance, we recommend 48 inches. This makes reading the display, pushing buttons, and placing fingers comfortable for most people. The reader should be out of the path of traffic. It should be close to the door but not behind it. Don't put the reader where users must cross the swing path of the door.

! **NOTE** *The reader must not be exposed to airborne dust, direct sunlight, water, or chemicals.*

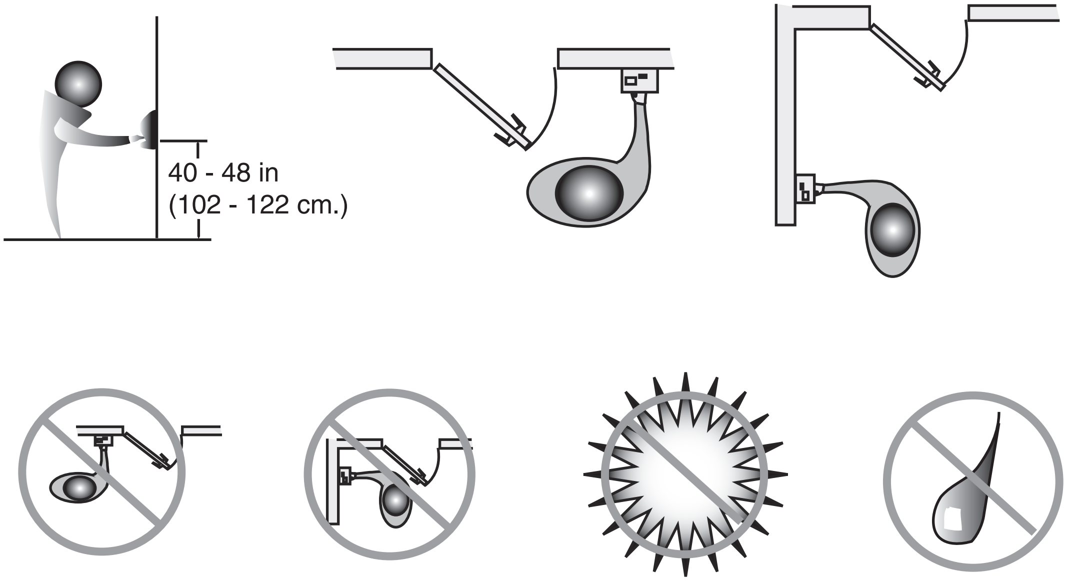


Figure 3-1: Reader Placement Rules

Fastening the Reader to the Wall

Protecting the Reader from Dust and Debris

At all times, protect the reader from excessive airborne dust and debris. This is particularly important during the installation process. For example, if you need to cut a hole in the sheetrock for the electrical box, don't place an unwrapped reader on the floor under where you are cutting; the dust would get inside the reader and affect its future use. Instead, keep the reader in its packaging until you're actually ready to fasten it to the wall. Protect the reader, just as you would any other sensitive equipment.

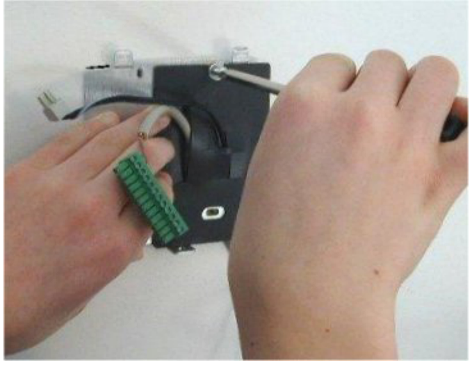
Mount All Readers at the Same Height

All readers in your facility should be mounted at the same height.

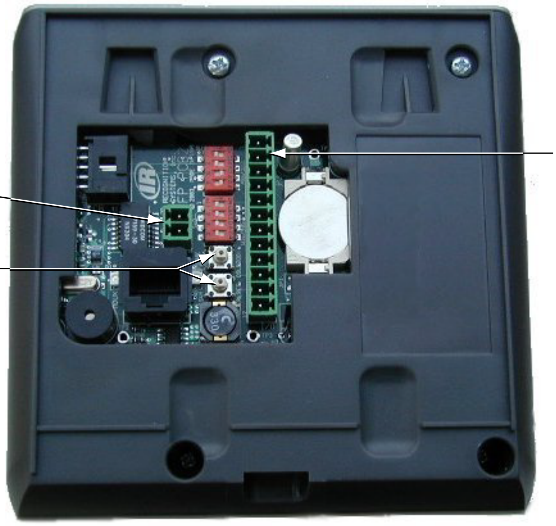
Mounting the Back Panel on the Wall

1. Have a double electrical box (double gang box) installed in or on the wall where you want to install the reader. The top of the box should be between 40 and 48 inches (102 to 122 cm) from the floor.

2. Run the wiring for the reader to this box, following local electrical code.
   - This includes the wiring from your access control panel, the power for the reader, and the network wiring if the readers are networked.
3. Run the wiring through the black gasket on the mounting plate, and then screw the reader mounting plate to the electrical box.
   - The two tabs on the mounting plate go on the top.
   - Use the screws provided with the installation kit; screws with larger heads could keep the reader from seating or closing properly.



4. Connect the wiring to the reader.



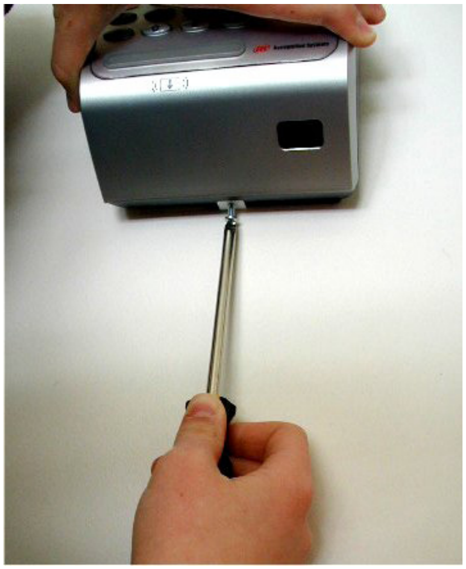
Power Connection

Make sure the wire bundles don’t press against the rest or cold boot switches.

Terminals 1-12 for reader wiring connections

- Wiring instructions begin on page 9.
- Make sure you position the wire bundles so they don’t accidentally press the reset and cold boot buttons when you close the reader. It would cause problems if the wires kept these buttons pressed when the reader was closed.

5. Hook the top of the reader on to the clips on the mounting plate, push the bottom of the reader in, and then insert the torx screw that holds the bottom of the reader to the mounting plate.



- In cold weather: Remember that all plastics are brittle when cold. If, for example, you’ve left the reader in your truck overnight on a cold winter night, you should let the reader warm up to room temperature before installing it. (If you don’t, and if you overtighten the torx screw, you could crack the plastic around the hole.)

Wiring the Reader

Always follow any electrical codes for your area.

Disclaimer

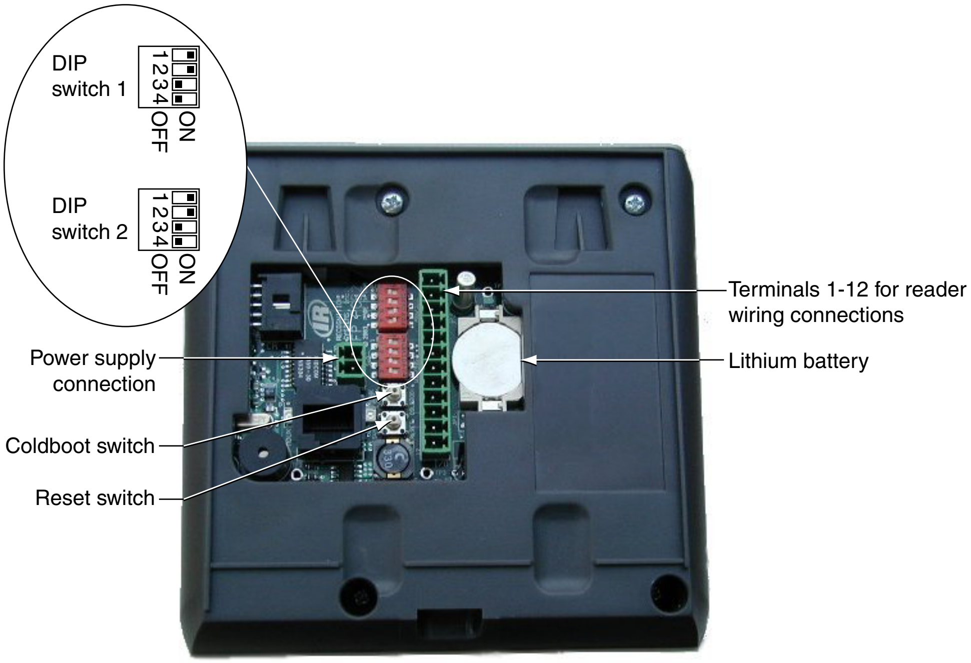
Schlage Biometrics is not responsible for readers damaged by improper wiring.

Wiring Overview

Wiring the reader involves:

- setting the reader's dip switches for your wiring configuration; see page 10.
- connecting the wires for the access control panel and for other inputs and outputs; see page11.
- connecting power input; see page 12.
- establishing a solid ground connection; see page 12.
- connecting network wiring; see page 13.

Connections on the Back of the Reader



Setting DIP Switches

Controlling how readers are networked

! NOTE *If you change DIP switch settings after the reader has power connected, you must reset the reader before the change is recognized.*

1. Switch 1 controls how readers are networked to each other.
    - To network readers (RS-485 wiring): DIP switches 1 and 2 must be on, and DIP switches 3 and 4 must be off. You will always use this configuration for networking two or more readers. Set Host Connection in the reader setup must match your setting here; see *Setting the Type of Network Connection* on page 39.
    - To use the RS-232 cable to connect to our backup utility, to upgrade the reader's firmware, or to connect a single reader to a computer host: DIP switches 3 and 4 must be on, and DIP switches 1 and 2 should be off. You'll only use RS-232 for updating the reader's firmware and for using our backup utility. For either of these purposes, you must set the DIP switch to the appropriate position, but you don't need to change Set Host Connection. If you have your readers networked and have to change the DIP switches to make a backup or to upgrade the firmware, make sure you put the DIP switches back and reset the reader when you are done.
    - If the reader isn't networked: It doesn't matter how switch 1 is set.

Identifying the type of access control panel

2. Switch 2 identifies the type of access control panel connection.
    - To connect to a panel via Wiegand/Magstripe: DIP switches 1 and 2 must be on, and DIP switches 3 and 4 should be off.
    - To connect to future Schlage Biometrics products by RS-485 wiring: This is only for future Schlage Biometrics products. There are no currently available solutions that use this option. If Schlage Biometrics offers a solution using this configuration in the future, DIP switches 3 and 4 must be on, and DIP switches 1 and 2 should be off.

If you change DIP switch settings

3. If you change any DIP switches on a reader that is already connected, you must reset the reader for the changes to take effect. To reset the reader, you can either disconnect the power and then apply power again, or you can press the Reset button.

Connecting the Reader to the Access Control Panel, to an External Card Reader, and to Other Readers

For each type of connection that you need, connect the corresponding wiring to the appropriate pins on the terminal connector block.

Table 3-1: Terminal Block Connections

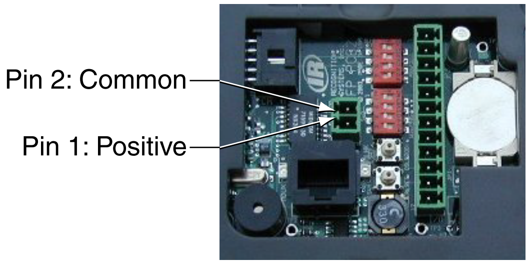
Terminal	Connection	Notes
1	Card Reader: Wiegand D0 or Magnetic Stripe Data Input	Use these terminals to connect to an external card reader to supply user IDs instead of having users enter their IDs using the reader keypad. (These terminals aren’t needed if your reader has a built-in card-reader.)
2	Card Reader: Wiegand D1 or Magstripe Clock Input	
3	Access Control Panel: Wiegand D0, Magstripe Data Output, or some other type through RS-485 wiring	Use these terminals to connect to an access control panel.
4	Ground	
5	Access Control Panel: Wiegand D1, Magstripe clock output	
6	Tamper switch output	Use this terminal to connect to a tamper alarm. A signal goes through this connection if the reader is tipped, indicating that someone may be tampering with the reader.
7	External bell input	These terminals let you connect output wires from your access control panel so your access control panel can control the bell (beeper) and red/green/amber LED’s on the reader. For input here to make a difference, the Beeper/LED settings on the Setup menu must be set to respond to external input; see page 41.
8	LED red input	
9	LED green input	
10	Reader/host network Tx: RS-485 wiring or RS-232 wiring	Use these terminals to network with other FingerKey readers through either RS-485 wiring or RS-232 wiring. (RS-232 is only used to connect a single reader to a host computer; usually you will use RS-485.)
11	Ground	
12	Reader/host network Rx: RS-485 wiring or RS-232 wiring	

Connecting Power Input

The reader requires 12 volts DC (1000 mA). Connect power to the 2-pin terminal P2.

Table 3-2: Power Supply Connections

Pin	Connection
1	Positive
2	Common (Ground)



Establishing a Solid Ground Connection

All readers should have a solid, reliable, earth ground connection. This protects internal circuit boards from electrostatic discharge and from external signal line transients (power spikes). A qualified electrician familiar with electrical code and wiring/grounding techniques should identify the earth ground source.

! NOTE *Earth Ground Connnections connect earth ground securely to the wall mount plate.*

Networking Readers

If readers are connected by RS-485, you can connect up to 32 readers to each other. This allows one reader to serve as a master; it can get users from other readers and send new users back to them; this lets you enroll a user on one reader and then give that user access at all of them. See *Getting Users from Other Readers* starting on page 43.

Networking Caution

Unless you have the appropriate networking knowledge, we don't recommend trying to set up a reader network on your own. We train our dealers to set up reader networks correctly; we recommend using their services if you are networking readers.

Designating a Master Reader

If you network a group of readers to each other and they are not managed by some software, then you must designate one of the readers as a master, and the rest must be set up as remote readers; that is, they can't be designated as master readers.

If your readers are managed by some computer software, the software is the master, so no readers would be designated as a master

See *Indicating Whether the Reader is a Master* on page 38 for help changing this setting.

Making Sure DIP Switches are Set UP Correctly

Make sure that DIP switch 1 is set to reflect the type of wiring you use; see *Controlling how readers are networked* on page 10.

Network Wiring

To create a RS-485 network, use a single twisted pair of wires (plus a ground). For each reader, connect pin 10 (Tx +/-) on the terminal block to pin 10 on the next reader, connect pin 11 (ground) to pin 11, and connect pin 12 (Rx +/-) to pin 12. You can connect up to 32 readers. You must use a daisy-chain; a star configuration will NOT work correctly.

For a RS-485 network, at 9600 baud, the maximum total line length for the network is 4000 feet. Use Belden cable 82723 or the equivalent (minimum 22 gage).

For a RS-232 network (which can only connect a single reader to a host computer), the maximum line length is 50 feet.

Secure Setup Guidelines

Secure Setup Overview

1. Design an ID numbering system; see page 15.
   A properly designed ID numbering system makes the reader faster and easier to use.
2. Add/Enroll your supervisory staff.
   This includes users who are authorized to program the reader, users who monitor the reader network, and users who will add new users to the reader. The process for adding these users is the same as for adding other users; see page 21.
3. In the reader, set authority levels for your supervisory staff; see page 16.
   This makes sure these users have access to the options in the reader that they need, and it also prevents other users from being able to inappropriately access the reader menu options. This step is critical in preventing unauthorized people from getting around your security system.
4. Customize settings in the reader as needed; see *Programming the FingerKey* starting on page 32.
   This step is listed here because you would normally complete your reader setup before adding users, but you can actually change the settings in the reader at any time.
5. Teach your users how to use the reader and then add/enroll them in the reader.
   See page 20 for more on teaching users how to use the reader; see page 21 for details on enrolling them in the reader.

Designing a User ID Numbering System

If a Card Reader Identifies Users

You don’t need to design an ID numbering system if you use a card reader to supply the ID number. The card provides all ID information.

If Users Must Type Their ID Numbers on the Reader Keypad

User ID numbers tell the reader which user is trying to gain access.

A well-designed ID number system makes it quicker for you to decide which ID to assign to a new user, and it makes ID entry faster at the reader through the use of the Set ID Length command (see page 41).

Follow these guidelines when designing an ID numbering system:

- Each user must have a unique ID number; the reader won’t accept two people with the same ID. (If you enroll people using the last four digits of their phone numbers or social security numbers, you may get duplicate numbers.)
- ID numbers may begin with 0 (zero). For example, the reader regards the ID 05 as different from the ID 5.
- ID numbers can be up to 15 digits long when entered at the reader keypad, but shorter numbers are easier to remember and easier to enter. (The reader gives you about 10 seconds to enter an ID number.) In most contexts, 4-digit numbers provide adequate security and are easy to remember and enter.
- Make all ID numbers the same length. This lets you use the Set ID Length command. If you don’t use the Set ID Length command, users must enter their ID and then press the enter key; if you use the Set ID Length command, users only have to enter the ID without needing to press enter; the reader automatically continues as soon as the appropriate number of digits are entered; see page 41 for more about this command.

Setting Authority Levels for Supervisory Staff

What Authority Levels Are For

Authority levels limit which reader programming menus the user can use. Users who need access through the door but who shouldn't be able to change the reader's settings should have an authority level of 0 (zero). This is appropriate for most users. When you add a new user, the reader automatically assigns an authority level of 0 (zero). You only need to set authority levels for users who also need to be able to change the reader's setup.

What Each Authority Level Lets You Access

Authority Level	Door Access	Access to Reader Menus				
		Service	Setup	Management	Enrollment	Security
Level 0	✓					
Level 1	✓	✓				
Level 2	✓	✓	✓			
Level 3	✓	✓	✓	✓		
Level 4	✓	✓	✓	✓	✓	
Level 5	✓	✓	✓	✓	✓	✓

See page 33 for more on what each menu in the reader contains.

Why Setting Authority Levels Is Critical

When you initially add users (including yourself and other supervisory staff), all users have an authority level of 0 (zero). When all users have equal authority levels, the reader lets every user access all of the reader menus. (This is needed so you can get to the menus during setup.) This means that initially any user that you enroll could change any setting in the reader if that user figures out how to get to the reader menus.

More critically, if an unauthorized user enters the Security menu, he can then erase all users from the reader's memory, enable unauthorized access, and change authority levels.

As soon as you set a higher authority level for any user, the reader limits access for all users with lower passwords. To prevent unauthorized users from making inappropriate changes, set the authority levels for your supervisory staff BEFORE adding other users.

Entering Users in the Appropriate Order

Because of the issues explained above, we recommend adding users and changing authority levels in this order:

1. Add your system administrators; see page 21.
   These users will oversee the security system, control all settings in the reader, and monitor activity.
   We strongly recommend having at least two system administrators. This way, if one administrator is unavailable, someone is still able to make changes if needed.
2. Change the authority level for your system administrators to 5. (See page 17.)
3. Add other users.
4. Change the authority level for other users if needed.

Changing a User's Authority Level

After you have changed authority levels and left the Security menu, you need an authority level of 5 to reenter the Security menu. You must have added a user before you can change that user's authority level.

1. On the reader keypad, press Clear and then quickly press ENTER.
   You should see:

   ```
   ENTER ID
   ```

   If you don't see this, try again. This won't work if you press Clear and ENTER at the same time; you must press Clear and then press ENTER immediately afterwards. It also doesn't work if you wait too long between pressing Clear and ENTER; after you press Clear, you must press ENTER immediately.
2. Type your user ID and press enter.
3. Place your finger when the reader asks you to. After you do this, you see:

   ```
   ENTER PASSWORD
   ```

4. Type the Security menu password and press enter.
   This password is initially set to 5. If you changed this password (see page 51), enter your password. You'll see:

   ```
   SET USER DATA
   *BACK        #NEXT
   ```

   If the reader shows the Ready display instead of this, either you entered the password incorrectly or you don't have the authority level to use this menu.
5. Press enter to indicate that you want to set user data. You'll see:

   ```
   SET USER
   AUTHORITY
   *BACK        #NEXT
   ```

6. Press enter to indicate that you want to set a user's authority level. You'll see:

   ```
   ENTER ID
   ```

7. Type the ID number for the user to set the authority level for and press enter. You'll see:

   ```
   0
   ENTER NEW VALUE
   ```

   The user's current authority level is shown on top. (The display above reflects a current authority level of 0 (zero)).

   If the reader flashes Process Fail and returns you to the Set User Authority display, you entered an ID number for a user you haven't added yet. Make sure you typed the ID correctly.

8. Type the new authority level and press enter.

```
0
ENTER NEW VALUE
5
```

The new authority level is shown on the bottom of the display. This must be a value between 0 (zero) and 5. For example, the display above shows a new authority level of 5. Make sure you enter the value for the authority level you wish to grant; see *What Each Authority Level Lets You Access* on page 16.

After you type the new authority level and press enter, the reader returns you to the Set User Authority display.

9. To change the authority level for another user, repeat the process beginning with step 6 above.
   To step back to a previous menu level, you can press the * button.
10. When done changing user authority levels, press the clear key until you are out of the reader menus.

Enrolling and Maintaining Users

Preparing to Enroll Users

These guidelines make the process of enrolling users faster and easier.

- Each user must have a unique ID number; the reader won't accept two people with the same ID. It saves time if you assign the ID numbers in advance. See page 15 for more on designing an ID numbering system.
- Determine whether you are going to collect one finger or two for each user; see *Setting Up a Duress Indicator or Alternate Finger* starting on page 40.
- Some users may have concerns about what the reader is or isn't doing; discussing the issues under *Eliminating Potential User Concerns* on page 20 helps alleviate these concerns.
- Teach users about correct finger placement before trying to enroll them. If users know how to place their fingers consistently and correctly, the enrollment process goes more quickly. See page 20 for more on teaching users how to use the reader correctly.
- You can enroll a group of people during a single enrollment session.

Teaching Users How to Use Readers

Eliminating Potential User Concerns

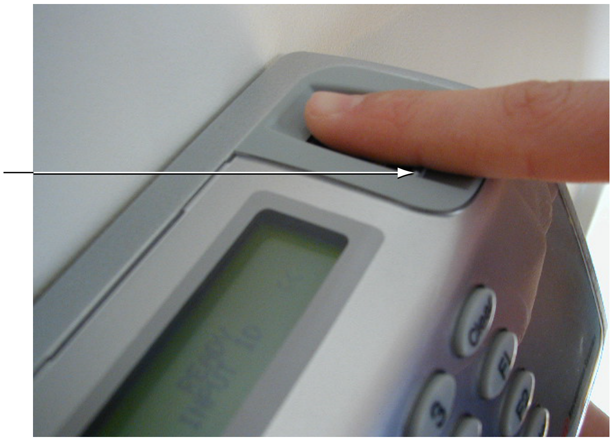
Most people have never used a fingerprint reader before, and some users will have concerns. Explaining how the reader works eliminates most fears and concerns before they occur. Inform users of these facts:

- Readers don't identify people; they just confirm identity. For example, you can't just put your finger on a reader and have it know who you are; the reader can only confirm that the finger on the reader matches the finger previously associated with a particular ID number.
- Readers do not take an actual picture of the fingerprint that could be used for general identification outside the reader network. Instead, they store a mathematical representation of the print that confirms that the same finger is present as when the entered ID number was enrolled. Readers don't invade privacy; they guarantee it.
- Readers shine an ordinary red light, generated by a red LED, on the finger.
- Readers are as sanitary as doorknobs.

Correct Finger Placement

Because the reader measures the fingerprint, it's important to place your finger on the reader the same way every time. When you put your finger on the reader, do this:

- Place the end of your finger gently and comfortably onto the plastic window to the right of the display; there's no need to apply pressure.
- The first finger crease below your fingertip should rest on the ridge below the window; don't slide your finger forward to fit your fingertip into the groove above the window. Use that groove only as a guide to keep your finger parallel to the window.



The first finger crease below your fingertip should rest on the ridge below the window.

Figure 5-1: Finger Placement

- Keep your finger flat. You should feel the plastic across the bottom of your finger.

Choosing a Finger

The reader accepts the index, middle, or ring fingers or the thumb from either hand. (Don't use the pinky, though; the reader may appear to enroll it, but it will generally cause verification errors afterwards.) Since you must use this same finger for access later on, choose a finger that is easy to place correctly; see *If Users Have Trouble Gaining Access* on page 24.

If you are using a secondary finger, the user must choose a different finger for the secondary finger.

Enrolling Users

Before a user can have access, you must take the user to a reader and have the reader create a template or mathematical representation of the user's fingerprint (we call this enrolling the user). Before you enroll a user, teach the user about correct finger placement (see page 20).

Use the Enrollment menu in the reader to enroll users.

You must have an Authority Level of 4 or higher to enroll users (see page 16 for more about authority levels).

1. On the reader keypad, press Clear and then quickly press ENTER.

   You should see:

   ```
   ENTER ID
   ```

   If the reader doesn't have users yet, you go directly to the Enter Password display shown below; in that case, skip to step 4.

   If you don't see either Enter ID or Enter Password, try again. Don't press Clear and ENTER at the same time; you must press Clear and then press ENTER immediately afterwards. Also don't wait too long between pressing Clear and ENTER; after you press Clear, you must press ENTER immediately.
2. Type your user ID and press enter.
3. Place your finger when the reader asks you to. After you do this, you see:

   ```
   ENTER PASSWORD
   ```
4. Type 4 and press enter.

   This is the standard password for the Enrollment menu; if you have changed this password (see page 51), enter your password instead. You should see:

   ```
   ADD USERS
   *BACK      #NEXT
   ```

   If the reader shows the Ready display instead of this, either you entered the password incorrectly or you don't have the authority level to use this menu.
5. Press ENTER to indicate that you want to add users. You'll see:

   ```
   ENTER ID
   ```

6. Type the ID number of the user to enroll and press enter.

   You'll now see:

```
PLACE PRIMARY FINGER
```

7. Have the user place and remove his/her finger on the reader each time when asked.

   The reader should ask the user to place his/her finger twice; if it asks for the finger more than twice, the user isn't placing his/her finger consistently; go over the instructions for correct finger placement.

   Once the user places the finger correctly two times consecutively, the reader asks the user to place the alternate finger if the Set Secondary Finger setting in the Setup menu requires this (see page 40):

```
PLACE ALTERNATE
FINGER
```

   Follow the same procedure as with the first finger. The reader accepts any finger as the alternate finger (including the primary finger).

   If the alternate finger is being used for duress, make sure the user places a different finger for the alternate finger.

8. Once the user has successfully placed the required finger(s), the reader briefly flashes the message User Enrollment Successful and then displays:

```
ADD USERS
*BACK     #NEXT
```

   Press ENTER to enroll another user if needed, or press clear until you are out of the reader menus.

For DX-2200 Readers (iCLASS)

If you have a DX-2200 reader, that is, a reader that supports iCLASS cards, your enrollment options will be slightly different; see *Adding Users on a DX-2200 (iCLASS)* on page 45 for more details).

Maintaining Users

You can remove users with the Remove Users command on the Enrollment menu; see page 46.

You can set or change user authority levels and reject levels with Set User Data on the Security menu; see page 47.

If Users Have Trouble Gaining Access

If Many Users Are Having Access Problems

The reader probably needs to be cleaned; see page 25.

If cleaning the reader doesn't help, try raising the reader's reject threshold; see *Controlling How Sensitive the Reader Is When Verifying Fingerprints and How Many Tries a User Gets* starting on page 51.

If a Particular User Is Having Access Problems

Try each of these steps; stop as soon as you find a solution that works.

1. The user might have placed the finger badly during the initial enrollment. Remove the user from the reader, go over correct finger placement, and then add the user again. This creates a new fingerprint template for the user. Make sure the user is placing the right finger.
2. Remove the user, and enroll the user again using different fingers.
   Try the thumb if other fingers don't work.
3. Increase the reject threshold, that is, how closely the fingerprint must match the stored template.
   Some users have fingerprints that scan badly. Other users have physical conditions that make it impossible to place the finger consistently. For these users, increasing the reject threshold may solve the problem; see page 49.
4. If all of the above has failed, enroll the user as a special user.
   This type of enrollment reduces security because it doesn't require finger recognition; only do this as a last resort. See *Enrolling Users Who Don't Need Finger Recognition to Gain Access* on page 49.

Ongoing Reader Maintenance

Cleaning Readers

Why Readers Need to Be Cleaned

FingerKeys recognize a user's fingerprint by reflecting light off the finger. The reader forms a mathematical "image" of the user's fingerprint based on how the light reflects back. If the sensor window is dirty, the light won't correctly reflect back so the image generated won't match the user's fingerprint. When this happens, the image the reader sees is different from the fingerprint template stored in the reader. This causes the reader to not recognize the user's finger. The solution is simple: regularly clean the window. This enables a clear image of the fingerprint that the reader can recognize.

How to Clean a Reader

Spray any ordinary, non-abrasive window cleaner on a clean soft cloth. The cloth should be damp but not wet or dripping. Use the damp cloth to wipe the plastic window to the right of the display. Pay special attention to the corners and edges of the window where dust may collect. Wipe the rest of the reader when done.

- Never spray cleaning fluid directly onto the reader! Always spray a cloth and then wipe the reader with the cloth. If you spray the cleaner directly on the reader, the cleaning fluid can drip on the main circuit board; this could cause a short and ruin the board.
- Make the cleaning cloth damp but not wet! If the cloth is wet, this can cause the same problems as if you spray the cleaner right on the reader.
- Never use an abrasive or gritty cleaner! An abrasive cleaner could scratch the surfaces.

How Often Readers Should Be Cleaned

A reader in a clean environment with light usage might only need to be cleaned once a month.

A reader in a dirty environment or a reader with heavy use should be cleaned once a week.

If a reader is having problems recognizing users, cleaning the reader usually eliminates the problem.

Clearing or Resetting the Reader

Reset Options

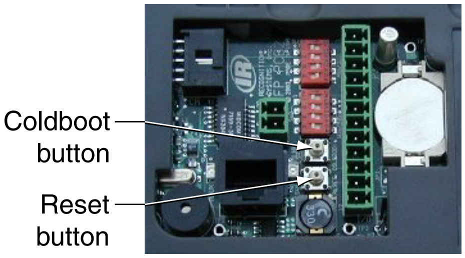
- If you’ve changed network related settings (address, master/remote status, etc.) through the reader menus: The reader automatically resets itself when you leave the menus. You’ll see a message that tells you that the reader is resetting if this is needed.
- If you’ve changed DIP switches: You must reset the reader for the changes to take effect. Just press the Reset button on the back of the reader. (Disconnecting the power and then connecting it again would do the same thing.)
- To erase the users in a reader while keeping its settings: Use the Clear Memory option on the Security menu.
- To erase the reader’s settings while keeping the users in the reader: Do a warm boot; this is explained below.
- To erase the reader’s settings and also erase all users: Do a cold boot; this is explained below.

Erasing Only the Users

To erase all users from the reader while leaving the reader’s settings unchanged, use Clear Memory on the Security menu; see *Erasing All Users from the Reader* starting on page 52. To keep unauthorized people from erasing users, this option requires you to have an authority level of 5 and to know the Security menu password; see *Why Setting Authority Levels Is Critical* on page 16. If you don’t have access to the Security menu, you can’t erase the users.

Erasing the Setup or the Setup & Users & Passwords

1. Remove the torx screw on the bottom of the reader and remove the reader from the wall mount.
   The reader is held closed with a with a tamper resistant screw; you must use a torx screwdriver to remove it.
2. On the back of the reader, find the RESET and COLDBOOT buttons.
   When the reader is upright, the COLDBOOT button is the top button and the Reset button is the bottom button. (If you look carefully at the labels on the board, you will see that these buttons are labeled there.)



3. Press and release the RESET button.
   This clears the display on the front of the reader.
4. While the display is clear, press the COLDBOOT button and hold it in until the reader display shows:

```
SELECT BOOT RESET
1=WARM    2=COLD
```

5. Let go of the COLDBOOT button and indicate what to erase:
    - To erase only the reader's setup: Press 1 for Warm boot. This resets the reader's setup to the factory default settings, but it keeps all users. (If you have upgraded the reader's memory so the reader can store more users, erasing the reader's setup does not affect this; you will still have the expanded user memory.)
    - To erase the reader's setup and all users and passwords: Press 2 for Cold boot. This resets the reader to the factory default settings, and it permanently erases all users in the reader.

    After the process is done, you see a message that the tells you that the process is complete, and then you see the Ready display.

Upgrading the Reader's Firmware

Periodically, Schlage Biometrics, Inc. will release upgrades to the reader's firmware; these upgrades may add new features or correct minor problems.

To upgrade the reader, you must first install the FingerKey Update Utility on your computer, and then, whenever you have an upgrade, you must connect the reader and install it in the reader.

System Requirements

To install and run the FingerKey Update Utility, your computer must meet these requirements:

- a PC with a CD-ROM drive and a serial port.
- Windows 2000 or Windows XP.

Making Sure You Have the .NET Framework

The FingerKey Update Utility requires the .NET framework to run. It is included on the CD for your convenience. If you don't have it, you must install it before you install the FingerKey Update Utility. To see if your computer has the .NET framework installed:

1. Click the Start menu, highlight Settings, and click Control Panel.
2. Double-click Add/Remove Programs.
3. In the Add/Remove Programs window, scroll down and look for MicroSoft .NET Framework 1.1.
   - Programs are listed in alphabetical order.
   - If your computer has the .NET Framework installed, proceed to Installing the FingerKey Update Utility below. If your computer doesn't have the .NET Framework, you must install it.

Installing the .NET Framework

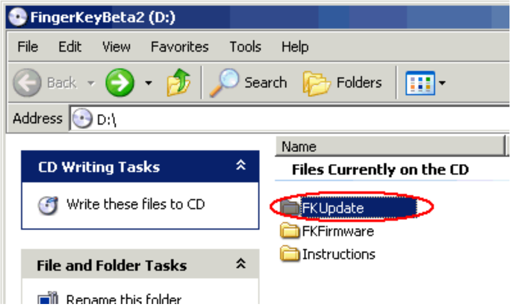
If you don't have the .NET Framework, you must install it.

1. Insert the FingerKey CD (included with the FingerKey reader) into your CD-ROM drive.
2. Double-click the My Computer icon on your desktop, and then browse to the CD contents.
3. Open the FK-Update folder on the CD.
4. Double-click 1033dotnetfx.exe to start the installation.
   Follow the instructions on the screen. You may have to restart your computer at the end of the process.

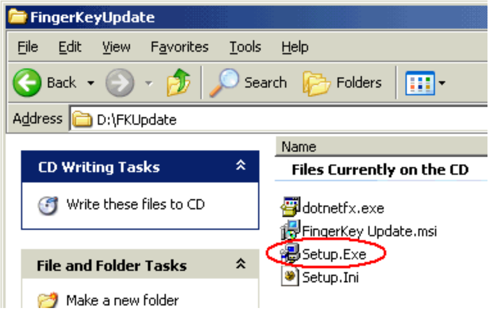
Once the .NET Framework is installed, you are ready to install the FingerKey Update Utility.

Installing the FingerKey Update Utility

1. Insert the FingerKey CD into your CD-ROM drive.
2. Double-click the My Computer icon on your desktop and browse to the CD contents.
3. Double-click the FKUpdate folder on the CD-ROM drive.



4. Double-click Setup.exe.



5. Click Next on each screen in the installation process.
   - While we don’t recommend it, you can change the location where the utility is installed if you need to.
6. On the final screen, click Close to close the installation window.

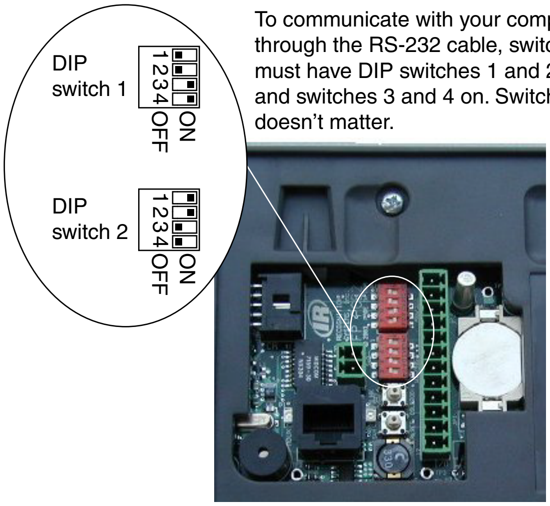
Upgrading the FingerKey or Sensor Firmware

Once you have installed the FingerKey Update Utility, you can then use it to upgrade the reader whenever we provide an update. There are three basic steps:

1. Establish communication between the FingerKey reader and the update utility.
2. Update the reader’s application firmware or sensor firmware.
3. Reset the FingerKey to initialize the new firmware.

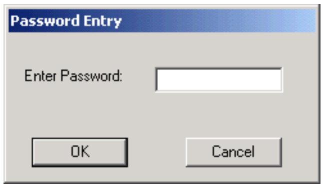
Establishing Communication Between the Reader and the Update Utility

1. Disconnect power from the FingerKey.
2. On the back of the reader, for switch 1, move DIP switches 1 & 2 to the off position, and turn switches 3 & 4 on.



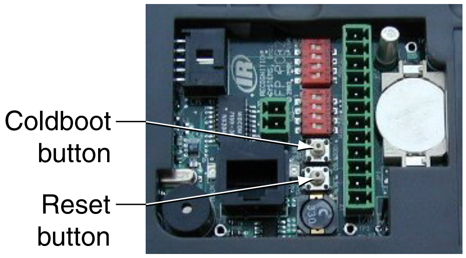
To communicate with your computer through the RS-232 cable, switch 1 must have DIP switches 1 and 2 off, and switches 3 and 4 on. Switch 2 doesn't matter.

3. Connect the RS-232 cable to a serial port on your computer and to the connector terminal on the back of the reader.
4. Connect power to the reader.
5. Start the FingerKey Update Utility.
   - The installation puts a FingerKey Update icon on your desktop.
   - You can also click your Start menu, highlight Programs, highlight Schlage Biometrics, and click FingerKey Update.
6. Enter the password for the FingerKey Update Utility.



   - The initial passwords are 1234NEW for the regular password and ADMIN for the administrative password. These passwords are case sensitive.
   - The administrative password lets you change passwords and erase memory blocks (something you don't generally need to do).
   - To change these passwords, log in with the ADMIN password, click File, click Change Passwords, enter the ADMIN password again, enter the new passwords, and click OK.
7. Click the File menu, click Select Communications Port, and select the serial port you've connected the reader to.
   - Once you've selected the appropriate port, the program remembers the port you chose; you only need to do this the first time you use the utility.
8. Click the Identify button.

9. On the reader, press the Reset button, and press and hold the Cold boot button until the reader display shows the message Download Mode.



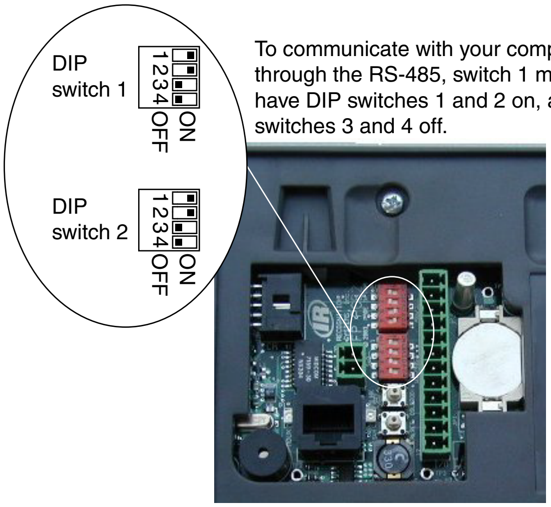
10. Confirm that the reader and update utility are communicating by looking at Bootloader Version, Firmware Version, and Program Checksum displayed in the lower-left corner of the utility.

Updating the FingerKey's Application Firmware

1. Click the Download button.
2. Browse to the location of the FingerKey application firmware file, and click Open. The update should take about six minutes.
3. When you see the message Device Programmed Successfully, click OK.

Resetting the FingerKey

1. Disconnect the RS-232 cable from the FingerKey.
2. Reset the reader's DIP switches to the original position.



To communicate with your computer through the RS-485, switch 1 must have DIP switches 1 and 2 on, and switches 3 and 4 off.

- For a Schlage Biometrics-485 connection (the usual setup), for switch 1, move DIP switches 1 & 2 must be on, and switches 3 & 4 must be off.

3. Press the Reset button on the back of the FingerKey.
4. Verify that the new firmware has been successfully initialized by observing the FingerKey start-up screens for the firmware version(s).

Programming the FingerKey

Which Settings You Should Change in the Reader

If you have software like HandNet Lite that manages your readers, you would typically only change the reader address and communication type using the reader menus; you would change all other settings through the software; changes made through the reader menus would typically be overwritten by the software.

If you are not using software to control and monitor the readers, then you would change all settings through the reader menus.

Menus in the Reader

You program the reader through these five menus:

- **Service Menu:** This lets the master reader display the status of all readers on the network. (Readers that aren't configured as a master don't currently have any options on this menu.)
- **Setup Menu:** This lets you control the reader's network address, the maximum user ID length, settings for auxiliary output devices, facility codes, the network master, network connection interface, network configuration, a duress indicator using a secondary finger, and whether or not the reader beeps when you press the keys. The Setup menu also includes a command that lets you upgrade the reader's memory, that is, that expands the number of users the reader can store.
- **Management Menu:** This lets you list all of the users in the reader and lets the master reader send/acquire user databases to/from readers in a network.
- **Enrollment Menu:** This lets you enroll (add) or remove users.
- **Security Menu:** This lets you customize user settings (how closely the user's fingerprint must match the template and whether the user can use these command menus). It also lets you control the standard reject threshold (how closely all users' fingerprints must match templates), set the passwords needed to get to these menus, clear all the users from reader, and give a user access without fingerprint recognition. If you use Smart Cards (HID iCLASS cards), the security menu also lets you do the needed setup.

The following page lists each option on each menu.

Summary of menu options

Table 7-3: Summary of Menu Options

Service Menu	Setup Menu	Management Menu	Enrollment Menu	Security Menu
Network Status	Set Reader Mode	List Users	Add Users	Set User Data
	Set Address	Data from Network	Remove Users	Set Passwords
	Set Host Connection	Data to Network		Clear Memory
	Set Secondary Finger	Verify Reader		Set Credential Formats
	Set LED/Beeper			Reboot Reader
	Set ID Length			Smart Card Options
	Set Language			
	Memory Upgrade			
	Ethernet Upgrade			

Getting to the Menus in the Reader

1. **On the reader keypad, press Clear and then quickly press ENTER.**
   If the reader already has users in it, you see:

   ENTER ID

   If you see this, type your user ID and press enter. The reader asks you to place your finger. Once you place your finger and it has been verified, you should then see the Enter Password display shown below.

   If the reader doesn't have any users yet: You go directly to the Enter Password display:

   ENTER PASSWORD

   If you don't see the Enter ID or the Enter Password display: If you don't see either Enter ID or Enter Password, try again. Don't press Clear and ENTER at the same time; you must press Clear and then press ENTER immediately afterwards. Also don't wait too long between pressing Clear and ENTER; after you press Clear, you must press ENTER immediately.
2. **Type the password for the menu you want and press enter.**

   The initial passwords are listed below; your passwords will be different if you changed them. (See *Setting Passwords for the Reader Menus* on page 51.)

Table 7-4: Command Menu Passwords

	Initial Password
Service Menu:	1
Setup Menu:	2
Management Menu:	3
Enrollment Menu:	4
Security Menu:	5

If you are authorized to use the menu you picked (and if you entered the correct password), the first command on the menu appears.

If you are returned to the Ready prompt, then either you entered the password incorrectly or you aren't authorized to use that menu. See page 16 for more about authority levels.

Navigating the Menus

Once you enter a menu, you can:

Change the settings for the command shown: Press Enter.

Go to the next or previous option on a menu: Press # for Next. If you accidentally pass the option you need, press * for Back or keep pressing # (Next). From the last option on the menu, # (Next) cycles you back to the first option again; * (Back) cycles you around in reverse.

Go to a different menu: Press clear until you get back to the Enter Password. display. From there, type the password for the menu you want to go to, and then press enter.

Backspace while entering numbers: Press * to backspace one character at a time at displays where numbers can be entered.

Leave the menus: Press clear until you get back to the Ready prompt. You will have to press clear more than once.

Once in any menu, you can change multiple settings within that menu; you don't have to leave the menu after changing any individual setting. To change settings in a different menu, press CLEAR until you return to the Enter Password display, and then type the password for the menu you want to go to.

Service Menu

What You Can See with This Menu

The Service menu lets the master reader display the status of all readers on the network.

If the reader isn't set up as a master, there are no available commands on this menu.

How to Get to This Menu

See *Getting to the Menus in the Reader* on page 34 and *Navigating the Menus* on page 35 for help getting to or moving around this menu.

Network Status

Network Status lets the master reader display the status of all reader addresses (0-31). The first line reflects reader addresses 0-15; the second line reflects addresses 16-31. If there is a connected reader at an address, the display shows a 1 (one) in the corresponding position; if there is no reader at a given address, the display shows a 0 (zero).

Unless you have used Verify Reader for each address (see page 44), it make take up to five minutes from the time that all readers are turned on before the Network Status command gives accurate results; it can take up to five minutes to check the status of each connected reader. If you use Network Status sooner than this, you may see some 0's where there really are connected readers; to check individual readers more quickly than this, use Verify Reader instead (see page 44).

The Network Status command is available only in the master reader; see *Setting the Type of Network Connection* on page 39.

NETWORK STATUS
***BACK #NEXT**

To display network status, press ENTER.

You see two lines of 16 characters each (corresponding to reader addresses 0-31), where 1 indicated a connected reader and 0 (zero) indicates no reader.

For instance, if your network had readers at all addresses except 1, 14, 15 and 18, you'd see:

1011111111111100
1101111111111111

Setup Menu

What You Can Change with This Menu

The setup menu lets you change these settings:

Set Reader Mode: This lets you choose the network master. Only one device in a network can be a master.

Set Address: This controls the reader's network address. There may be up to 32 readers in a network, each with a different address number (0-31).

Set Host Connection: This sets the network connection interface, such as Ethernet or serial (RS-485, RS-232).

Set Secondary Finger: This lets you set an alternate finger as a duress signal, which indicates that the user is in danger or being forced to give someone access.

Set LED/Beeper: This controls whether the reader beeps when you press the keys and when the reader recognizes or fails to recognize the user. It also controls whether the reader or an external device (typically an access panel) controls the reader's LED and beeper.

Set ID Length: If user IDs are all the same length, this lets the reader automatically continue without the users pressing enter after typing the ID.

Set Language: This lets you change the language used for the reader's display.

Memory Upgrade: This lets you increase the number of users the reader can store.

Getting to This Menu

See *Getting to the Menus in the Reader* on page 34 and *Navigating the Menus* on page 35 for help getting to or moving around this menu.

The commands are in the order listed above. To get to any command after you get to the menu, keep pressing # (Next) until you get to the command you want.

Indicating Whether the Reader is a Master

Set Reader Mode lets you indicate whether the reader is a master or remote reader. If your readers are networked, the master reader can transfer users to or from other readers; see *Getting Users from Other Readers* on page 43 and *Sending User Information to Other Readers* on page 44.

Only one reader in a network can be the master.

If your readers are managed by software, the software is the master so no reader should be designated as a master.

SET READER MODE
***BACK #NEXT**

To choose the network master, press ENTER. You see:

SET TO MASTER
***NO #YES**

Type * for No or # for Yes.

Setting the Reader's Address

Set Address lets you assign the reader's network address. Each networked reader requires a number; you may have up to 32 readers in a network, each with a different address (0-31).

The default address is 32, indicating a stand-alone reader. To connect the reader to a network, assign an address that doesn't conflict with any other reader on the network.

Connecting the reader to a network does not automatically transfer users to or from the master reader; to transfer users see *Getting Users from Other Readers* on page 43 and *Sending User Information to Other Readers* on page 44.

SET ADDRESS
***BACK #NEXT**

To choose the address, press ENTER. You'll see:

INPUT ADDRESS

Enter a number from 0 to 31 on the keypad. Press ENTER. The display returns to Set Address. Press # (Next) to go on to the next option.

There's no way to set this back to 32 after you change it, but there's no need to; a stand alone reader can have any address; we just start at 32 so you won't have a conflict at initial setup.

If you change the reader's address or network connection (or if you've changed DIP switches), you must leave the command menus (which will reset the reader) before the change takes effect.

Setting the Type of Network Connection

Serial Connection

Set Host Connection controls how networked readers communicate with each other. The reader may be set to stand alone, to RS-485, to RS-232, or to TCP/IP.

For a serial connection with more than two readers or a line length greater than 50 feet, you must choose RS-485; RS-232 is only useful for connecting a single reader to a computer's serial port.

If you choose RS-485 or RS-232, the reader asks for a baud rate. We recommend starting at 9600. Once your network is working correctly, try increasing this speed at each to see if communication still works; the length of the wiring in your network affects the maximum workable baud rate. All readers in the network must be set to the same baud rate.

If you choose RS-485 or RS-232, you must set DIP switch 1 to correspond to your choice; see *Controlling how readers are networked* on page 10.

If you change the reader's address or network connection (or if you've changed DIP switches), you must leave the command menus (which resets the reader) before the change takes effect.

TCP/IP Connection

If the reader is connected to the host computer through a TCP/IP (Ethernet) connection, then you must first upgrade your reader using the Ethernet Upgrade option; see page 42.

Once you've used the Ethernet Upgrade option, you can then use Set TCP/IP to enter the IP address supplied by your network administrator.

When asked for IP Address, use # for the period. For example, to enter 192.168.0.55, you would type 192#168#0#55.

From Set IP Address, press * (Back) or # (Next) to get to Set Subnet Mask and Set Gateway Address. You'll enter those values just as you did the IP address. Contact your network administrator if you aren't sure what to enter.

The reader will reboot when you leave the command menus. Once the reader is done rebooting, it is ready to communicate with the new address.

```
SET HOST CONNECTION
*BACK        #NEXT
```

To set the connection, press enter. You'll see:

```
SET STAND ALONE
*BACK        #NEXT
```

Press # (Next) until you see:

```
SET TCP/IP
*BACK        #NEXT
```

Press ENTER. You'll see:

```
SET IP ADDRESS
*BACK        #NEXT
```

Press ENTER. You'll see:

```
INPUT IP ADDRESS
```

Type the IP address, using # for the period. Press ENTER when done.

Enter the subnet mask and gateway in the same way.

Setting Up a Duress Indicator or Alternate Finger

Set Secondary Finger lets you control whether users can verify with a different finger then they usually use, and if yes, what it means if they do.

Administrators should decide which of these options that plan to use BEFORE they start enrolling users.

You have three possibilities:

- **The reader collects only one finger for each user.** To set this up, choose # (Yes) for the Disable option. This makes enrolling new users slightly faster.
- **The reader collects two fingers for each user and either finger gives normal access.** This way, if a user has a band-aid or cut on one finger, the user could use the other finger. To set this up, choose * (No) for the Disable option, and then choose # (Yes) for the Alternate option.
- **The reader collects two fingers for each user, with the second finger indicating duress or danger.** If you are concerned about possible situations where a user is in danger or is being forced to give access to someone else, you can set the secondary finger as a duress indicator. When the secondary finger indicates duress, access is granted if the secondary finger is used, but the access control panel also triggers a silent alarm. (It does this by either sending an alternate facility code or with reverse parity; which depends on how your access control panel is set up.) To set this up, choose * (No) for the Disable option, choose * (No) for the Alternate option, and then choose # (Yes) for the Duress option. (Your access panel must support this feature for this to make any difference.)

```
SET SECONDARY
FINGER
*BACK        #NEXT
```

To change this setting, press enter. You'll see:

```
DISABLE
*NO        #YES
```

Press # (Yes) to use the reader without the secondary finger option. Press * (No) to set this option. You'll see:

```
SET ALTERNATE
FINGER
*NO        #YES
```

Press # (Yes) to set the alternate finger option. Press * (No) if you do not want to set this. You'll see:

```
SET DURESS FINGER
*NO        #YES
```

Press # (Yes) to set the duress finger option. Press * (no) to return to the Disable prompt or CLEAR to go to the Setup menu.

If you enroll users without a secondary finger (that is, with this Disabled), and later turn the secondary finger for an alternate or for duress, those users will continue to have access using the primary finger, but they won't have a template of the secondary finger and so won't be able to take advantage of the added functionality. To collect the secondary finger so those users can use the duress or alternate finger feature, delete those users (see *Removing Users* on page 46) and enroll them again; when you re-enroll them, the reader will collect the secondary finger.

When an alternate or duress finger is placed on the reader

When a user places an alternate finger, the reader display indicates that the alternate finger was recognized. However, if the user places a duress finger, the reader display does not give any indication that the duress finger was used; the display looks exactly as it does when the primary finger is used. This is because the duress signal is supposed to be invisible to the person who is forcing the user to give them access; it should look exactly the same as a normal access.

Controlling the Beeper and LEDs

Set LED/Beeper lets you control the beeper and LEDs.

- **Enable Beeper:** When on, the reader beeps once when you press a key, once when a user is granted access, and twice when access is denied.
- **External LED Control** determines what controls reader's LED display. If this is set to No, the LED is normally red, turns amber when user input is required, and turns green when an ID is verified. If this is set to Yes, the LEDs are controlled by input from your access control panel; the red LED is on when input is received through the terminal connector block (P3) pin 8, green is on when input is received through pin 9, and amber is on when input is received through both 8 and 9. See page 11 for more on what each terminal connector block pin is for.
- **External Bell Control:** If this is set to Yes, the beeper sounds when input is received from your access control panel through terminal connector block (P3) pin 7. See page 11 for more on what each terminal connector block pin is for.

SET BEEPER
***BACK #NEXT**

To change this setting, press enter. You'll see:

ENABLE BEEPER
***NO #YES**

Type * (No) to disable the beeper. Type # (Yes) to enable the beeper. You'll see:

EXTERNAL LED CONTROL
***NO #YES**

Type * for No or # for Yes. You'll see:

EXTERNAL BELL CNTRL
***NO #YES**

Type * for No or # for Yes. To return to the Setup menu, press CLEAR.

Setting the ID Length

If all of your users have the same length ID: Set ID Length lets users type ID numbers without having to press enter at the end. For example, if all user IDs were four digits long, you could set the ID length to 4 and the reader would automatically continue when the user enters the fourth digit.

If your IDs are different lengths: Set the ID length to the length of the longest ID. Users with the longest IDs won't have to press enter; users with shorter IDs will.

If IDs are entered from a card reader: What you enter here doesn't matter; Set ID Length doesn't affect what length IDs are accepted from a card reader; that is determined by the input formats you select; see page 53.

The length is initially set to 25 digits (the longest possible Wiegand ID). Valid values are from 1 to 25 digits.

SET ID LENGTH
***BACK #NEXT**

To change this setting, press enter. You see:

INPUT LENGTH

Type the length of the longest ID you will use (valid lengths: 1-15) and press enter. To leave the length unchanged, press enter without typing anything.

Setting the Language for the Reader's Display

Set Language lets you change the language used for the reader's display. This is initially set to English. Other languages will be supported in the future.

SET LANGUAGE
***BACK #NEXT**

To change this setting, press enter. You see:

SET ENGLISH
***NO #YES**

You currently can't choose any other option.

Increasing the Maximum Number of Users Readers Can Accept

Memory Upgrade lets you increase reader memory to handle more users. The reader initially stores 50 users. You can purchase a code to upgrade the reader so it can store additional users.

To upgrade, contact your dealer or systems integrator.

If you upgrade the memory in one reader, we recommend upgrading all readers in the network at the same time. Otherwise, if you transfer users from one reader to another, you could transfer more users than another reader can hold. (If you do this, the reader would just transfer as many users as it could; you would not receive any indication that all users weren't transferred).

```
MEMORY UPGRADE
*BACK       #NEXT
```

To upgrade memory, press enter. You see:

```
ENTER CODE
```

Enter your code on the keypad and press ENTER.

If you don't press the correct code, the display flashes Wrong Code and returns you to the Memory Upgrade prompt.

Enabling the Reader to Communicate with a Host Computer by Ethernet

Ethernet Upgrade lets you enable a reader to communicate with a host computer through TCP/IP. The reader is initially not configured to be able to communicate through TCP/IP.

To upgrade, contact your dealer or systems integrator.

```
ETHERNET UPGRADE
*BACK       #NEXT
```

To upgrade memory, press enter. You see:

```
ENTER CODE
```

Enter your code on the keypad and press ENTER.

If you don't press the correct code, the display flashes Wrong Code and returns you to the Ethernet Upgrade prompt.

Management Menu

What You Can Do with This Menu

This menu lets you list all of the users in the reader. If the reader is a master reader, it also lets you send/receive user databases to/from readers in a network and check to see if a particular reader on the network is communicating.

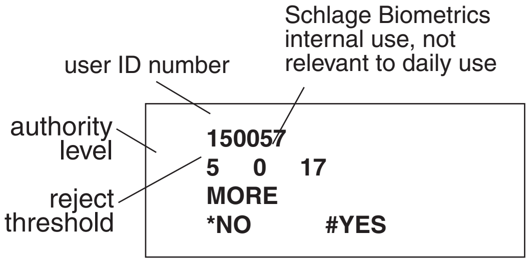
Getting to This Menu

See *Getting to the Menus in the Reader* on page 34 and *Navigating the Menus* on page 35 for help getting to or moving around this menu.

Listing Users

List Users lets you navigate and display the list of enrolled users in the reader.

The display shows something like this:



```
150057
5   0   17
MORE
*NO        #YES
```

Press * (No) if you don’t want to look at any more users; press # (Yes) to show another record.

```
LIST USERS
*BACK        #NEXT
```

To change this setting, press enter. You see:

```
USERS ENROLLED
12
MORE
*NO        #YES
```

In this example, 12 users are enrolled in the reader.

To learn about each user, press # for Yes. The display shows something like what’s shown on the left.

Getting Users from Other Readers

Data from Network lets the master reader get the entire user set from any reader on the network. Users enrolled at the remote reader whose IDs aren’t in the master reader are added to the master set. If a user ID is already in the master, the information for the user in the master reader is replaced by the information from the remote reader.

Used with Data to Network (explained below), Data from Network lets you enroll users in one reader then transfer them to other readers. This command is available only in the master reader.

This option assumes that you have enough memory in the reader for all of the users. If you try to transfer users from one reader to another when one of the readers doesn’t have enough memory to store all of the users, the reader simply transfers as many users as it can. You would not get any warning that some users were not transferred. If you need to, you can upgrade the reader’s memory so that it can hold more users; see page 42.

```
DATA FROM NETWORK
*BACK        #NEXT
```

To get the user database from another networked reader, press enter. You’ll see:

```
INPUT ADDRESS
```

Type the address (0-31) of the reader to get users from and press enter. You’ll see:

```
NETWORK DB UPLOAD
PLEASE WAIT . . .
```

Sending User Information to Other Readers

Data to Network lets the network master send its entire set of users to all readers on the network or to specified readers. This lets you give users access through multiple readers without enrolling them separately in each reader. This command erases the users in the remote reader and then sends all of the users from the master reader. This means that if you have a user in the remote reader that isn't in the master reader, that user will be deleted.

This command is available only in the master reader. To send users that are in another reader, first use Data from Network (see above) to bring the users from that reader into the master, and then use Data to Network to send the users from the master to the other readers.

```
DATA TO NETWORK
*BACK      #NEXT
```

To send a user list, press enter. You see:

```
SEND DB TO ALL
*NO      #YES
```

If you type # (Yes), the reader sends its database to all other readers; if you type * (No), you see:

```
INPUT ADDRESS
```

Type the address (0-31) of the reader to send the users to and press enter.

This option assumes that you have enough memory in the reader for all of the users. If you try to transfer users from one reader to another when one of the readers doesn't have enough memory to store all of the users, the reader simply transfers as many users as it can. You would not get any warning that some users were not transferred. If you need to, you can upgrade the reader's memory so that it can hold more users; see page 42.

Checking to See if a Particular Networked Reader is Connected

Verify Reader lets the network master check to see if a particular reader is communicating. When asked to Input Address, type the address of the reader to check. After a few second delay, the reader's display lets you know whether a reader with that address is connected to the network. Watch the display closely since the message disappears after about two seconds.

```
VERIFY READER
*BACK      #NEXT
```

To see if a particular reader is communicating, press enter. You see:

```
INPUT ADDRESS
```

Type the address (0-31) and press enter. After a moment, the reader will tell you whether that reader is in the network.

You can also use the Network Status command (see page 36) to check the connection status of all readers at once, but if you haven't used Verify Reader for each connected reader first, then Network Status can take up to five minutes from the time all of the networked readers were powered up. If you've just powered the readers up, Verify Reader is a faster way to check the status of individual readers and to cause those readers to appear under Network Status.

Enrollment Menu

What You Can Change with This Menu

The Enrollment menu lets you add users to the reader and remove users from the reader.

Getting to This Menu

See *Getting to the Menus in the Reader* on page 34 and *Navigating the Menus* on page 35 for help getting to or moving around this menu.

Adding Users

Add Users lets you enroll a new user in the reader. Adding users is explained in detail starting on page 21.

If your reader is a master reader, adding a user to that reader automatically sends the user to all readers on the network.

ADD USERS
***BACK #NEXT**

To add a user, press ENTER. See page 21 for an explanation of the rest of the process.

If you've added the user on a reader that isn't the master, or if the network wasn't connected to the network when you added the user, see *Sending User Information to Other Readers* on page 44 for help sending the user to other readers.

Adding Users on a DX-2200 (iCLASS)

The Schlage Biometrics DX-2200 fingerprint reader lets you store fingerprint templates on an HID iCLASS card. If you have this model fingerprint reader, Add Users still lets you enroll new users, but it has additional underlying menu choices that let you control whether the user's fingerprint template is stored on the card, in the reader, or both.

ENROLL TO DATABASE: This does a standard enrollment where the user is added only to the reader's database; the fingerprint template is not stored on an iCLASS card. The rest of the process is the same as for a standard reader; see page 21 for complete detail. If you want the user's template stored on the card, choose "No" here and choose "Yes" for one of the next two questions.

ENROLL TO SMART CARD: This stores the user's ID and fingerprint template only on the iCLASS card; it does not store it in the reader's database. If you want the user's template both on the card and in the reader, choose No here and choose Yes for the next question.

If you choose "Yes" here, you'll be asked whether to enter an ID or whether to get the ID from the card. These options are explained below.

ENROLL TO BOTH: This stores the user's ID and fingerprint template both on the iCLASS card and in the reader's database.

If you choose "Yes" here, you'll be asked whether to enter an ID or whether to get the ID from the card. These options are explained below.

ADD USERS
***BACK #NEXT**

To add a user, press ENTER.
You'll see:

ENROLL TO DATABASE
***NO #YES**

If you type # (Yes), the user will only be enrolled in the reader and not on an iCLASS card. If you type *(No), you'll see:

ENROLL TO SMART CARD
***NO #YES**

If you type # (Yes), the user will only be added to the card and not stored in the reader's database and not on an iCLASS card. If you type * (No), you'll see:

ENROLL TO BOTH
***NO #YES**

If you type # (Yes), the user will be added to both the card and also stored in the reader's database.
If you type * (No), you'll be returned to the ENROLL TO DATABASE display shown above.

Choosing Where to enter the User's ID

If you choose either Enroll to Smart Card or Enroll to Both above, then the reader asks whether you want to manually enter the user's ID number through the reader's keypad or whether the card's serial number should be used as the user ID.

SET ID FROM KEYPAD: This lets you manually enter a user ID on the reader's keypad.

SET ID FROM CARD CSN: This asks you to present a card to the reader and uses the card's serial number as the user's ID number.

SET ID FROM KEYPAD
*** NO # YES**

Type # (Yes) to manually enter the ID with the reader's keypad; type * (No) to go to the next screen where you can choose to use the card's serial number (CSN) as the user ID. If you type * (No), you'll see:

SET ID FROM CARD CSN
*** NO # YES**

If you type # (Yes), the card's serial number will become the user's ID. The reader will ask you to present the card so it can get the serial number:

PRESENT SMART CARD TO READER

If you typed * (No), you'd be returned to the SET ID FROM KEYPAD display shown above.
See page 21 for an explanation of the rest of the process of enrolling a user.

Completing the Enrollment Process

The rest of the enrollment process—placing the primary and secondary fingers—is described starting on page 21.

Removing Users

Remove User lets you delete a user from the reader. Once you remove the user, the user can no longer open the door controlled by reader. If the user needs access again, you would have to re-enroll the user.

REMOVE USERS
*** BACK #NEXT**

To remove a user, press ENTER. You'll see:

ENTER ID

Type the ID number of the user you want to remove and press ENTER. When the user is removed, the display returns to REMOVE USERS. Press ENTER to remove another user.
If you type an unused ID number, the display flashes PROCESS FAIL and returns to REMOVE USERS.

Security Menu

What You Can Change with This Menu

The Security menu lets you change each of these settings:

SET USER DATA: This lets you control:

- which reader menus the user may access
- how closely the user's fingerprint must match the stored fingerprint template.
- enroll a user who doesn't require fingerprint recognition to gain access.
- whether the secondary finger is used for duress or merely as an alternate.

SET REJECT THRESHOLD: This controls how sensitive the reader is in general to differences in user fingerprints and how many tries a user has to gain access before the reader locks the user out.

SET PASSWORDS: This lets you change the passwords for the menus in the reader.

CLEAR MEMORY: This erases all of the users in the reader.

SET CREDENTIAL FORMATS: This lets you set the input and output card formats for the reader and controls what the reader sends the access panel for invalid ids, rejected users, and so on.

Getting to This Menu

See *Getting to the Menus in the Reader* on page 34 and *Navigating the Menus* on page 35 for help getting to or moving around this menu.

The commands are in the order listed above. To get to any command, once you get to the menu, keep pressing # (Next) until you get to the command you want.

Customizing a User's Settings

Set User Data lets you control:

- which reader menus a user may access
- how closely a user's fingerprint must match the stored fingerprint template

You must enroll the user before you can customize that user's settings; see page 21 for help enrolling users.

SET USER DATA
***BACK # NEXT**

To customize settings for users, press ENTER. You'll see:

SET USER AUTHORITY
*** BACK # NEXT**

Press ENTER to give a user authority to access reader menus. You'll see:

ENTER ID

Type the ID of the user to give a higher authority level to the user and press ENTER. You'll see:

0
ENTER NEW VALUE

The user's current authority level is shown on top. Type the new authority level and press ENTER. You'll return to the SET USER AUTHORITY display. From here, you can change authority for another user, or press # (Next) to continue to the SET USER THRESHOLD display, or press CLEAR to return to the Security Menu.

Which reader menus a user may access

When you enroll users, the reader assigns an authority level of 0 (zero); this gives the user access through the door, but, as long as you have set your supervisors to a higher security level, it doesn't let the user change reader settings; this is appropriate for most users. Change authority for supervisory personnel who are responsible for adding other users or maintaining the security system.

The authority levels give this access:

Authority Level	Door Access	Access to Reader Menus				
		Service	Setup	Management	Enrollment	Security
Level 0	√					
Level 1	√	√				
Level 2	√	√	√			
Level 3	√	√	√	√		
Level 4	√	√	√	√	√	
Level 5	√	√	√	√	√	√

See page 16 for more about authority levels. See page 32 for more on what each menu contains.

Setting Supervisory Passwords First

Until you set higher authority levels for your supervisory users, the highest security level assigned gives full access to all of the reader menus. This means that if every user in the reader has an authority level of 0 (zero), then every user will be able to use the reader's command menus because they all have the highest level assigned. Only when you've created users with higher authority levels does the authority level of 0 prevent users from accessing the reader's menus.

Enrolling Users Who Don’t Need Finger Recognition to Gain Access

If a user has very severe arthritis or very unreadable fingerprints, Set Special User gives the user access without fingerprint recognition. (If you choose this, the reader still asks the user to place a finger on the reader so it won’t be apparent to others that fingerprint recognition isn’t required, but the reader doesn’t check the image of the fingerprint; it gives access regardless of whose finger is placed.)

Set No Bio Data lets you specify a user ID that should have access without fingerprint recognition; if you’ve previously given a user that has a finger template access without fingerprint recognition, Clear No Bio Data takes this special access away so the user’s finger template is used again. (If you created the user without a template initially, then Clear No Bio Data will fail; you must delete the user and enroll the user again with a finger template if you want the reader to start recognizing the user’s finger.)

Security Risk!!!

Bypassing fingerprint recognition significantly reduces security; anyone can get access with that ID if they discover that the reader isn’t looking at the fingerprint. Only use this as a last resort. Try these options first:

Review correct finger placement; see *If a Particular User Is Having Access Problems* on page 24.

Delete the user and then try enrolling the user again using a different finger.

Raise the user’s reject threshold. Under Set User Data on the Security menu, use Set User Threshold to raise the user’s reject level; see page 50 both for help changing that setting and for help determining the appropriate level.

```
SET SPECIAL USER
* BACK       # NEXT
```

To add a user who doesn’t need finger print recognition to gain access, press ENTER. You’ll see:

```
SET NO BIO DATA
* NO        # YES
```

Press # (Yes) to add the user who doesn’t need finger recognition. Press * (No) to go to the CLEAR NO BIO DATA display (see below):

```
ENTER ID
```

Type the ID number to be given access without fingerprint recognition and press ENTER. If you enter an ID that’s not already in the reader, you see:

```
ENROLL NO BIO DATA
* NO        # YES
```

Press # (Yes) to enroll the ID number without finger recognition. The display flashes USER ENROLLMENT SUCCESSFUL. If you press * (No), that ID isn’t enrolled. If you choose * (No) for SET NO BIO DATA, you see:

```
CLEAR NO BIO DATA
* NO        # YES
```

Press # (Yes) to eliminate no fingerprint access for a user that currently has access without a fingerprint being recognized. Press * (No) to return to the SET SPECIAL USER display.

Set Facility: This lets you control facility addresses. There may be up to 256 facilities serviced in a network, each with a different address number (0-255).

Set Site ID: If the card format you use includes a Site ID and if users manually enter an ID with the keypad, this lets you set what value is passed to the access panel.

Set Company ID: If the card format you use includes a Company ID and if users manually enter an ID with the keypad, this lets you set what value is passed to the access panel.

Set Issue Code: If the card format you use includes an Issue Code and if users manually enter an ID with the keypad, this lets you set what value is passed to the access panel.

Set Expiration: If the card format you use includes an expiration date and if users manually enter an ID with the keypad, this lets you set what date is passed to the access panel.

How Closely the User’s Fingerprint Must Match the Stored Template

When a user places a finger on the reader, slight differences in finger placement cause the fingerprint image to be nearly but not exactly identical to the template stored for the user. The reader compensates for these minor differences. This setting controls how exact the fingerprint match must be.

For most users, the standard setting that applies to all users (see page 47) is appropriate. Only change the reject threshold here if the reader should be more or less sensitive with specific users. For example, a user with arthritis (or other condition that affects finger movement) might find it hard to place the finger consistently. This setting lets you make the reader less sensitive for this user. Or, for users with access to the reader menus, you might use this setting to make the reader more sensitive to increase security.

You can enter 0 (zero) or a value from 30 to 250. 0 indicates that the user should use the default value for all users. (This default is set with Set Reject Threshold; see page 51). Other values cause the reader to be more or less stringent for this user that for others. Thirty (30) is the most secure and allows only very minor variations; 250 is the most tolerant of differences; only use this setting for users with very serious finger conditions. When the user enrolls, the reject threshold is initially set to 0 (zero).

To get to this option, answer # to SET USER AUTHORITY.

```
SET USER THRESHOLD
* BACK       # NEXT
```

Press ENTER to make the reader more or less sensitive for a user. You’ll see:

```
ENTER ID
```

Type the user ID to change the reject level for and press ENTER. You’ll see:

```
0
INPUT THRESHOLD
```

The user’s current reject level is shown on top. Type the new reject level and press ENTER. You’ll return to the SET USER THRESHOLD display. You can then change the reject level for another user, press # (Next) to continue to the SET USER AUTHORITY display, or press CLEAR to return to the Security Menu.

Figuring Out What to Set The Reject Level To

Setting a user’s reject threshold too high reduces the security of your system. For users having trouble gaining access at the standard setting, first try the solutions suggested in the section *If a Particular User Is Having Access Problems* on page 24. If you find that the only solution is to increase the users reject threshold, set the level to a value no higher than what the user needs.

To figure this out, temporarily increase the user’s reject threshold to 250 and have the user try to gain access. When the user gains access, the display flashes ID Verified along with the user’s score (how close the finger was to the stored template). For example, after verifying the user, the display shows something like this:

```
ID VERIFIED          140
PRIMARY FINGER
```

The score here indicates how closely the fingerprint matched the stored template.

Set the user’s reject threshold slightly higher than the score.

If the user can’t gain access even with a reject threshold of 250, delete the user and add the user again using a different finger.If that doesn’t work, you may need to give the user access that doesn’t require finger recognition; see page 51. If even this doesn’t work, you may have to use the Set Special User feature (page 51) to give the user access without finger recognition.

Controlling How Sensitive the Reader is When Verifying Fingerprints and How Many Tries a User Gets

Set Retry Limit controls how sensitive the reader is to differences in user fingerprints and how many tries the user has to gain access before the reader locks the user out.

This setting applies to all users who don't have a different reject level set under Set User Data (see page 50). If a particular user is having trouble gaining access, change that setting rather than this one.

INPUT THRESHOLD: Enter from 30 to 250. (This is initially set at 63, a good setting for most contexts.) The lower the number, the more closely the user's fingerprint must match the stored template; the higher the number, the more variation that the reader will tolerate. Lowering this number creates a more secure system, but some users have fingerprints that don't scan well; it might cause these users to be rejected more often.

SET NUMBER OF TRIES: If the reader doesn't recognize the user's fingerprint on the first try, this indicates how many times the user can reenter an ID before the reader locks out that ID out. For example, if this is set to 3 (the initial setting), and the user's fingerprint is not recognized after reentering the ID three times, the reader won't let that ID try to gain access again until another user is successfully recognized. This prevents someone from making repeated attempts to gain access with someone else's ID.

SET REJ THRESHOLD
*** BACK # NEXT**

To change this setting, press ENTER. You'll see:

63
INPUT THRESHOLD

The current reject threshold is shown on top. Enter a number (30-250) that reflects how close the fingerprint match must be for the typical user. Press ENTER. You'll see:

SET RETRY LIMIT
*** NO #YES**

Press * (No) and then # (Next) to continue to the Set Passwords display. To change this setting press ENTER. You'll see:

5
INPUT # OF TRIES

The current number of thries is shown. Type the number of tries (1-5) the user will have to gain access, and press ENTER.

Setting Passwords for the Reader Menus

Set Passwords changes the passwords assigned to the five reader menus. To increase the reader's security, you can change the password for any or all menus. However, if you use authority levels (which we very strongly recommend), you don't generally need to change the passwords (see page 16 for more about authority levels.)

Menu passwords can be up to 10 digits long. When you type the new password on the keypad, do so carefully; the display doesn't show the number you pressed but instead confirms each entry with an *. If you accidentally set this password to something other than what you want, you could lock yourself out of the menu.

SET PASSWORDS
*** BACK # NEXT**

To change passwords for the reader menus, press ENTER. You'll see:

SERVICE MENU PSWD
*** NO # YES**

Press # (Yes) to change the Service menu password. Type the new password for that menu and press ENTER. Press * (No) to continue to the password for the next menu.

If you think you might have typed a digit incorrectly, press CLEAR and start over. The password isn't be changed until you press ENTER.

Do NOT Lose Your Security Menu Password

If you forget the password that you set for the Security menu, you won't be able to access that menu to change certain settings in the reader. If you forget this password, the only way to get back to the Security menu is to reset the reader to the factory settings; see page 26. Doing so clears all settings and passwords (and users).

Erasing All Users from the Reader

Clear Memory erases all users from the reader but keeps the reader setup. Typically you'd only do this if you were moving the reader to a new location with different users but the same setup requirements.

Be sure this is what you want before you continue. Once you clear users from the reader's memory, there's no way to get them back unless you have a backup or unless the reader is connected to a network and the master reader can resend the user database; see *Sending User Information to Other Readers* on page 44.

CLEAR MEMORY
*** BACK # NEXT**

To erase all users from the reader, press ENTER. You'll see:

CONFIRM: DELETEDB
*** NO # YES**

Press * (No) if you don't want to erase the users. To erase all users from the reader, press # (Yes). The reader displays DELETING USER DB and returns to the Security Menu after the users have been erased.

Controlling How the Secondary Finger is Used for Individual Users

Set Duress User changes the use of the secondary finger for individual users.

Once you press enter when Set Duress User is shown, you can choose Set Duress Action to mark the secondary finger as being used to indicate duress, or, if you say not to Set Duress Action, you can choose Clear Duress Action to mark that user's secondary finger to be used as an alternate and not as a duress indicator.

To change how the secondary finger is used for all users, see *Setting Up a Duress Indicator or Alternate Finger* on page 47.

SET DURESS USER
*** BACK # NEXT**

To change the use of the secondary finger for a particular user, press ENTER when SET DURESS USER is shown. You'll see:

SET DURESS ACTION
*** NO # YES**

Press # (Yes) to indicate you want to use a particular user's finger to indicate duress. After you press #, you see:

ENTER ID

Type the userID number; if the user has a secondary finger enrolled, the reader will use that finger to indicate duress. If you pressed * (No) for SET DURESS ACTION, the reader instead shows:

CLEAR DURESS ACTION
*** NO # YES**

Press # (Yes) toindicate that you no longer wish to use the secondary finger to indicate duress; the secondary finger for the user ID yo enter wil now be merely an alternate.

Setting Input and Output Card Formats

SET CREDENTIAL FORMATS lets you set the reader's card format (input and output), keypad output format, and output for special situations.

Pressing enter on Set Credential Formats takes you to a set of four sub options:

SET INPUT FORMATS: This controls which card formats the reader will accept. You can choose up to five Wiegand or two Magstripe card formats. You must choose either Wiegand or Magstripe formats; you can't use both. Most companies only use one format.

SET OUTPUT FORMAT: When an ID is received from an external card reader, this controls the format of the ID the reader sends to the access panel. Usually the format you enter here matches the main input format you expect to receive.

SET KEYPAD FORMAT: When a user manually enters an ID through the reader keypad or uses the built-in card reader, this controls the format of the ID the reader sends to the access panel. Usually the format you enter here matches the main input format you expect to receive. If you use HID iCLASS cards (Smart Cards), choose this option; iCLASS cards don't store formatted ID's.

SET CREDENTIAL FRMTS
*** BACK # NEXT**

To set input and output formats, press ENTER. You'll see:

SET INPUT FORMATS
*** BACK # NEXT**

* (Back) and # (Next) cycle you through these options:

CLEAR DURESS ACTION
*** BACK # NEXT**

CLEAR DURESS ACTION
*** BACK # NEXT**

CLEAR DURESS ACTION
*** BACK # NEXT**

ENTER for any of these options lets you make changes. These options are explained in more detail on the following pages.

SET GLOBAL OPTIONS: This controls what the reader passes on to the access panel when the reader rejects a user, encounters an unknown user ID, or has a user indicate duress. It also controls what happens if an ID from a card runs over the allowed length (for example, if you indicate that input should be 16-bit Wiegand format and someone uses and card with 20-bit Wiegand format).

Interpreting the Format Detail Below

The following subsections elaborate on these options.

In the discussion of the format detail in the table below, you will see an elaboration on the format that looks like this:

```
         1         2
12345678901234567890123456
PFFFFFFFFIIIIIIIIIIIIIIIIP
EXXXXXXXXXXXX.............
.............XXXXXXXXXXXXX
```

The numbers at the top: Identify the bit numbers; this example has 26 bits.

F: Indicates which bits contain the facility code; in this example, bits 2-9 have the facility code.

I: Indicates which bits contain the ID; in this example, bits 10-25 contain the ID.

P/E/O/X/.: P indicates a parity bit; the E under the first parity bit here indicates that this parity is even. The X's following indicate which bits are used to determine that parity bit; the periods following indicate that those bits are not used in determining that parity bit; in this example, bits 2-13 are used to determine parity bit 1, and bits 14-26 do not affect this parity bit. The O under the second parity bit (bit 26) indicates this parity bit is odd; the preceding X's indicate that bits 14-25 are used to determine this parity bit.

Available Card Formats

	Format	Description	Format Detail
	0	None	
Wiegand formats	1	WC01=26BIT:16BIT ID	Facility code: 8 bits, bit 2-9 ID: 16 bits, bit 10-25
			1 2
			12345678901234567890123456 PFFFFFFFFIIIIIIIIIIIIIIIIP EXXXXXXXXXXXX............. .............XXXXXXXXXXXXO
	2	WC02=32BIT:22BIT ID	Facility code: 8 bits, bit 2-9 ID: 22 bits, bit 10-31
			1 2 3
			12345678901234567890123546789012 PFFFFFFFFIIIIIIIIIIIIIIIIIIIIIIP EXXXXXXXXXXXXXXX................ ................XXXXXXXXXXXXXXXA
	3	WC03=34BIT:16BIT ID	Facility code: 16 bits, bit 2-17 ID: 16 bits, bit 18-33
			1 2 3
			1234567890123456789012345678901234 PFFFFFFFFFFFFFFFFIIIIIIIIIIIIIIIIP EXXXXXXXXXXXXXXXX................. .................XXXXXXXXXXXXXXXXA
	4	WC04=26BIT:20BIT ID	Facility code: 12 bits, bit 2-13 ID: 20 bits, bit 14-33
			1 2 3
			1234567890123456789012345678901234 PFFFFFFFFFFFFIIIIIIIIIIIIIIIIIIIIP EXXXXXXXXXXXXXXXX................. .................XXXXXXXXXXXXXXXXO
	5	WC05=34BIT:32BIT ID	ID: 32 bits, bit 2-33
			1 2 3
			1234567890123456789012345678901234 PIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIP EXXXXXXXXXXXXXXXX................. .................XXXXXXXXXXXXXXXXO
	6	WC06=35BIT:20BIT ID	Facility code: 12 bits, bit 3-14 ID: 20 bits, bit 15-34
			1 2 3
			12345678901234567890123546789012345 PPFFFFFFFFFFFFIIIIIIIIIIIIIIIIIIIIP .EXX.XX.XX.XX.XX.XX.XX.XX.XX.XX.XX. .XX.XX.XX.XX.XX.XX.XX.XX.XX.XX.XX.O OXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
	7	WC07=37BIT:19BIT ID	Facility code: 16 bits, bit 2-17 ID: 19 bits, bit 18-36
			1 2 3
			1234567890123456789012345678901234567 PFFFFFFFFFFFFFFFFIIIIIIIIIIIIIIIIIIIP EXXXXXXXXXXXXXXXXXX.................. ..................XXXXXXXXXXXXXXXXXXO
	8	WC08=37BIT:35BIT ID	ID: 35 bits, bit 2-36
			1 2 3
			1234567890123456789012345678901234567 PIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIP EXXXXXXXXXXXXXXXXXX.................. ..................XXXXXXXXXXXXXXXXXXO

Assigning the Facility Code

If the card format you use includes a Site ID and if users manually enter an ID with the keypad, Set Facility lets you provide the facility code expected by your access control panel. Valid values are from 0 to 255.

If users are using cards instead of manually entering their IDs, the facility code is taken from the card and the value here is ignored.

SET SITE ID
***BACK #NEXT**

To assign a facility number, press ENTER. You see:

INPUT FACILITY

Type the number (0-65535) of the facility code expected by your access panel and press ENTER. Press ENTER without typing anything to leave the number unchanged.

Setting the Site ID

If the card format you use includes a site ID and if users manually enter an ID with the keypad, Set Site ID lets you set what value is passed to the access panel.

If users are using cards instead of manually entering their IDs, the site ID is taken from the card and the value here is ignored.

SET SITE ID
***BACK #NEXT**

To assign a site ID, press ENTER. You see:

INPUT SITE ID

Type the number (0-65535) of the site ID expected by your access panel and press ENTER. Press ENTER without typing anything to leave the number unchanged.

Set Company ID

If the card format you use includes a company ID and if users manually enter an ID with the keypad, Set Company ID lets you set what value is passed to the access panel.

If users are using cards instead of manually entering their IDs, the company ID is taken from the card and the value here is ignored.

SET COMPANY ID
***BACK #NEXT**

To assign a company ID, press ENTER. You see:

INPUT COMPANY ID

Type the number (0-65535) of the company ID expected by your access panel and press ENTER. Press ENTER without typing anything to leave the number unchanged.

Set Issue Code

If the card format you use includes an issue code and if users manually enter an ID with the keypad, Set Issue Code lets you set what value is passed to the access panel.

If users are using cards instead of manually entering their IDs, the issue code is taken from the card and the value here is ignored.

SET ISSUE CODE
***BACK #NEXT**

To assign a site ID, press ENTER. You see:

INPUT ISSUE CODE

Type the number (0-65535) of the issue code expected by your access panel and press ENTER. Press ENTER without typing anything to leave the number unchanged.

Set Expiration

If the card format you use includes an expiration date and if users manually enter an ID with the keypad, Set Expiration lets you set what date is passed to the access panel.

If users are using cards instead of manually entering their IDs, the expiration date is taken from the card and the value here is ignored.

SET EXPIRATION
***BACK #NEXT**

To assign a facility number, press ENTER. You see:

INPUT MONTH

Type the number (1-12) that corresponds to the month and press ENTER. You see:

INPUT DAY

Type the number (1-31) that corresponds to the day of the month and press ENTER. You see:

INPUT 2-DIGIT YEAR

Type the last two digits of the expiration year and press ENTER.

	Format	Description	Format Detail
MagStripe formats	9	MS09=MAG1	ABA Track 2 Input ID len 25 Output min len 1 Output max len 25 Do trim leading zeroes Oriented right, no offset
	10	MS10=MAG2	ABA Track 2 Input ID len 25 Output min len 1 Output max len 25 Do trim leading zeroes Oriented right, no offset
	11	MS11=MAG3 Octal 7	ABA Track 2 Input ID len 7 Output min len 1 Output max len 25 Do trim leading zeroes Oriented right, no offset MS11=MAG3 Octal 7 is the format used for FingerKeys with a ProxIF reader.

Setting Input Formats

Set Input Formats, the first sub-option under Set Credential Formats, controls which card formats the reader will accept at either an internal or external card reader. You can choose up to five Wiegand or two Magstripe card formats. You must choose either Wiegand or Magstripe formats; you can't use both. Most companies use only one format.

The possible formats are shown under Available Card Formats on page 54; the reader is initially set to accept input in formats 7, 6, 4, 2, and 1; you only need to use this option if you use some format other than one of these or if you want to prevent some of these formats.

Enter formats in descending order; if you set more than one input format, the reader sorts them in descending order from the largest bit format to the smallest, with None having the lowest value. For example, if the reader is set to:

Input Format 1: WC08
Input Format 2: WC07
Input Format 3: WC06
Input Format 4: WC05
Input Format 5: WC04

and you change Format 1 to None, the formats adjust to:

Input Format 1: WC08
Input Format 2: WC07
Input Format 3: WC06
Input Format 4: WC05
Input Format 5: NONE

SET INPUT FORMATS
*** BACK # NEXT**

Press ENTER to set the card formats the reader will accept. You'll see:

SET INPUT FORMAT1
*** BACK # NEXT**

Press ENTER to set Input Format 1. Press # (Next) to go to Input Format 2. When you press ENTER to change any input format, you see something like:

WC07=07=37BIT:19BIT ID

SET TO NONE
*** NO # YES**

Line 1 shows the card format that is currently selected. Line 3 shows the format that will be chosen if you press # (Yes). Press * (No) to cycle to the next available format; press # (Yes) to choose the format.
After you set Input Format 1, follow the same procedure for Input Formats 2-5.

Setting Output Formats

Set Output Format, the second sub-option under Set Credential Formats, controls the card format the reader sends to the access control panel if you use an internal or external card reader.

For the output format, you can choose:

Use Input Format: Doesn't change the formatting; passes through whatever card format is received. This is the default setting.

Set to None: Sends no output to the access panel; don't use this option if you want people to have access through the door.

Formats 1-10: See the list of Available Card Formats on page 54.

```
SET OUTPUT FORMATS
* BACK        # NEXT
```

Ress ENTER to set the card format(s) the reader passes on to the access panel. You'll see something like:

```
INPUT FORMAT/S

USE INPUT FORMAT/S
* BACK        # NEXT
```

Line 1 shows the card output format that is currently selected. Line 3 shows the format that will be chosen if you press # (Yes). Press * (No) to cycle to the next available format; press # (Yes) to choose the format.

Setting the Keypad Format

Set Keypad Format, the second sub-option under Set Credential Formats, controls the format of the ID the reader sends to the access panel when a user manually enters an ID through the reader keypad or uses the built-in card reader (rather than using an external card reader). Choose from:

Set to None: Prevents users from entering IDs from the reader keypad; users must use a card reader (either the built-in card reader or an external one). If you choose Set to None, you can still use the reader keypad to program the reader.

Formats 1-10: See the list of Available Card Formats on page 61. Format 1 is the default.

```
SET KEYPAD FORMAT
* BACK        # NEXT
```

Press ENTER to set the card format to use for keypad-entered IDs. When you press ENTER to change the keypad format, you see something like:

```
WC01=26BIT:16BIT ID

SET TO NONE
* NO       # YES
```

Line1 shows the card format that is currently selected. Line 3 shows the format that will be chosen if you press # (Yes). Press * (No) to cycle to the next available format; press # (Yes) to choose the format.

Modifying Output for Specific Reader Situations

Set Global Options lets you control what the reader sends to the access panel for these conditions:

Set ID Overflow: If the ID on the card is longer than the maximum length permitted by the formats you selected, this indicates what the reader should send to the access panel:

Suppress Output: The reader won't send anything.
Substitute 1 Bits: Instead of the ID that was entered, substitute all 1 bits.
Substitute Zero: Instead of the ID that was entered, send 0 (zero).

Set ID Unknown: This controls what the reader sends the access panel when it doesn't recognize the ID.

```
SET GLOBAL OPTIONS
* BACK        # NEXT
```

Press ENTER to control what gets sent to the access panel for any of the conditions listed. You see:

```
SET ID OVERFLOW
* BACK        # NEXT
```

* (Back) and # (Next) cycle you through these options:

```
SET ID UNKNOWN
* BACK        # NEXT
```

```
SET BIO REJECT
* BACK        # NEXT
```

```
SET DURESS ACTION
* BACK        # NEXT
```

ENTER for any of these options lets you make changes.

Set Bio Reject: This controls what the reader sends the access panel when a valid ID is entered but the user's finger is rejected because it doesn't match the template.

Set Duress Action: This controls what the reader sends the access panel when a user places a duress finger.

For each of these three situations, you have these four options:

Suppress Output: The reader won't send anything.
Alt Facility Code: Instead of the normal facility code, the reader sends the facility code you choose.
Incr/Decr Facility: The reader increases or decreases the facility code by the increment you choose.
Toggle Parity Bits: The reader toggles the output parity bits, that is, if the parity bits are even, it makes them odd, and if they are odd, it makes them even.

Resetting the Reader

Reboot Reader resets the reader. It does the same thing as if you disconnected the power and then powered up the reader again. Changing the reader's DIP switches require that you reset the reader for the changes to be accepted. This is probably the only time you would use this option. (Certain changes to the reader's configuration also require the reader to be reset, but if you make those changes, the reader automatically reboots when you leave the reader's command menus.)

REBOOT READER
*** BACK # NEXT**

To reboot the reader, press ENTER. You'll see:

ARE YOU SURE?
*** NO # YES**

Press # (Yes) to confirm that you want to do this.

Configuring the Reader for Smart/ HID iCLASS Cards

Smart Card Options takes you to a group of settings for configuring and maintaining HID iCLASS cards. This menu only appears if you have an iCLASS reader. (iCLASS readers are marked with DX-2200 on the back.) If you have any other type of card and reader, this section doesn't apply to you.

iCLASS cards can store the user's biometric fingerprint template directly on the card instead of in the reader; see *Adding Users on a DX-2200 (iCLASS)* starting on page 45 for help enrolling users so their information is stored on the cards.

SMART CARD OPTIONS
*** BACK # NEXT**

Press ENTER. You'll see:

SET ICLASS OPTIONS
*** BACK # NEXT**

Press ENTER to go to the first of the iCLASS settings: # (Next) or * (Back) moves to the other options on that menu; ENTER changes the settings for the option you are on.

Supported Cards

FingerKeys work with HID iCLASS 16K cards in the 16 application format. FingerKey readers convert unprogrammed 16K 2 application cards to the 16 application format if they can be converted; otherwise, the card can't be used. 2K cards aren't supported in the DX-2200 because they don't have enough space to store FingerKey user records.

Warning: Do NOT Lose or Forget the Card Key(s)

The card's key enables FingerKeys to access information on the card; the key is stored on both the card and the reader; the key must match in the reader and card for information to be shared. If you were to lose or forget the key (and if it were no longer in the reader), the card would become useless; there's no way to figure out what a card's key is, even for the manufacturer. (This doesn't affect the Schlage Biometrics fingerprint reader; it can always be reset to the default key.) However, if you know that one of several old keys was used but aren't sure which, you can recover the card by trying the various old keys: see *Setting the Old Key in the Reader* on page 62 for detail.

Setting a New Key in the Reader

Set New Reader Key lets you provide a security password that encrypts the areas that Schlage Biometrics fingerprint readers use on your iCLASS cards; this makes your cards distinct from other people's cards and also protect each user's fingerprint data from being read if you use the same cards with other devices.

You don't have to define a key: Schlage Biometrics fingerprint readers have a built-in, unique, secure key that is used by default if you don't provide a different one.

If you do enter a new key, make sure that you record it or find some way to remember it; if you forget the key, you can make the card unusable.

The key is a 64 bit value. This is entered in the reader with 8 sets of numbers from 0–255. For example:

240 10 240 34 77 255 1 19

is a valid key since there are 8 numbers, each of which fall between 0 and 255.

Generally you shouldn't change a key unless there's a specific security reason to do so. For example, you might change the key if a disgruntled employee left and failed to return a card; that employee could still gain access if you didn't change the key (and limit automatic updates). Apart from some specific situation like this, one can continue to use the same key for an indefinite period.

```
SET NEW READER KEY
 * BACK      # NEXT
```

Press ENTER. You'll see:

```
ENTER NEW READER KEY
      (0 - 255)

 * BACK      # NEXT
```

Enter the first of your 8 numbers and press ENTER. Repeat this for the remaining numbers. When done, you'll see a screen like this:

```
 CONFIRM KEY VALUES
240    10     240    34
 77   255       1    19
     * NO     # YES
```

Press # (Yes) to confirm and save the new key. The reader saves the prior key as the old key; the options following control whether the key is automatically updated on cards.
As noted previously, make sure you don't lose or forget the key.

Determining Whether Keys Get Automatically Updated on Cards

When you create a new reader key, Enable Auto Updates controls when/if the new key gets put on the iCLASS cards used with your system.

Enable Auto Update: Choose Yes if you want keys automatically updated the next time users present their cards; choose No if you want to manually update the cards or if you only want the cards updated at some other reader. (For help manually updating keys, see *Manually Updating a Key on a Card* on page 63.)

Set Update Limits: Choose No if you want the reader to automatically update all cards with the old key for an unlimited number of cards and an unlimited time period. Choose Yes if you want to limit the number of cards that get updated.

Input Maximum Cards: If you've chosen to Set Update Limits above, then enter the number of cards to update. For example, if you have 20 employees, you might want to limit the reader to updating 20 cards. You can enter a number from 0–500. (If you have more than 500 cards, you can either manually update the additional cards, or you can allow an unlimited number of cards. 0 (zero) here lets the reader update an unlimited number of cards.

```
ENABLE AUTO UPDATES?
   * NO     # YES
```

If you want the reader to automatically update keys on cards, press # (Yes). You'll see:

```
SET UPDATE LIMITS
  * NO     # YES
```

Choose * (No) if you want all cards updated for an indefinite period; if you choose * (No), this is the final screen in this process. To limit the number of cards or the number of days during which automatic updates can occur, choose # (Yes). You'll see:

```
INPUT MAXIMUM CARDS
```

Enter the maximum number of cards to automatically update and press ENTER. You'll see:

```
INPUT MAXIMUM DAYS
```

Enter the maximum number of days to automatically update and press ENTER.

Input Maximum Days: If you've chosen to Set Update Limits above, enter the number of days during which automatic updates are allowed. You can enter a number from 0–60. (To update cards after 60 days, you can either manually update the cards, or you can allow an unlimited number of cards. 0 (zero) here lets the reader update keys for an unlimited number of days.

Converting a Reader Key for HandNet Lite

If you enter a key in the reader and later need to enter it in HandNet Lite, you must convert these 8 numbers to 8 pairs of hex digits so you end up with a 16 digit hex number. Use this table to convert keys if needed:

#	Hex	#	Hex	#	Hex	#	Hex	#	Hex	#	Hex	#	Hex	#	Hex
0	00	32	20	64	40	96	60	128	80	160	A0	192	C0	224	E0
1	01	33	21	65	41	97	61	129	81	161	A1	193	C1	225	E1
2	02	34	22	66	42	98	62	130	82	162	A2	194	C2	226	E2
3	03	35	23	67	43	99	63	131	83	163	A3	195	C3	227	E3
4	04	36	24	68	44	100	64	132	84	164	A4	196	C4	228	E4
5	05	37	25	69	45	101	65	133	85	165	A5	197	C5	229	E5
6	06	38	26	70	46	102	66	134	86	166	A6	198	C6	230	E6
7	07	39	27	71	47	103	67	135	87	167	A7	199	C7	231	E7
8	08	40	28	72	48	104	68	136	88	168	A8	200	C8	232	E8
9	09	41	29	73	49	105	69	137	89	169	A9	201	C9	233	E9
10	0A	42	2A	74	4A	106	6A	138	8A	170	AA	202	CA	234	EA
11	0B	43	2B	75	4B	107	6B	139	8B	171	AB	203	CB	235	EB
12	0C	44	2C	76	4C	108	6C	140	8C	172	AC	204	CC	236	EC
13	0D	45	2D	77	4D	109	6D	141	8D	173	AD	205	CD	237	ED
14	0E	46	2E	78	4E	110	6E	142	8E	174	AE	206	CE	238	EE
15	0F	47	2F	79	4F	111	6F	143	8F	175	AF	207	CF	239	EF
16	10	48	30	80	50	112	70	144	90	176	B0	208	D0	240	F0
17	11	49	31	81	51	113	71	145	91	177	B1	209	D1	241	F1
18	12	50	32	82	52	114	72	146	92	178	B2	210	D2	242	F2
19	13	51	33	83	53	115	73	147	93	179	B3	211	D3	243	F3
20	14	52	34	84	54	116	74	148	94	180	B4	212	D4	244	F4
21	15	53	35	85	55	117	75	149	95	181	B5	213	D5	245	F5
22	16	54	36	86	56	118	76	150	96	182	B6	214	D6	246	F6
23	17	55	37	87	57	119	77	151	97	183	B7	215	D7	247	F7
24	18	56	38	88	58	120	78	152	98	184	B8	216	D8	248	F8
25	19	57	39	89	59	121	79	153	99	185	B9	217	D9	249	F9
26	1A	58	3A	90	5A	122	7A	154	9A	186	BA	218	DA	250	FA
27	1B	59	3B	91	5B	123	7B	155	9B	187	BB	219	DB	251	FB
28	1C	60	3C	92	5C	124	7C	156	9C	188	BC	220	DC	252	FC
29	1D	61	3D	93	5D	125	7D	157	9D	189	BD	221	DD	253	FD
30	1E	62	3E	94	5E	126	7E	158	9E	190	BE	222	DE	254	FE
31	1F	63	3F	95	5F	127	7F	159	9F	191	BF	223	DF	255	FF

For example, this key entered in the reader: 240 10 240 34 77 255 1 19
would be entered as this key in HandNet Lite: F00AF0224DFF0113

If you're starting with a key from HandNet Lite you can do the same thing in reverse: convert each two hex digits to a decimal number and enter each number in turn in the 8 entries in the reader.

Setting the Old Key in the Reader

Set Old Reader Key lets you override the previous key if needed. The entries here are like those for a new key; see the discussion above for more about the key format or how to convert a HandNet Lite key to a reader key.

To change the key for a previously used iCLASS card, the reader must know what the old key is—this prevents unauthorized people from converting other cards to work with your system. Whenever you enter a new key, the reader automatically remembers what your last key was, so most of the time, you don't need to change this value. For example, suppose you originally set the key to 11 22 11 22 11 22 11 22 and then you used Set New Reader Key to change the key to 33 44 33 44 33 44 33 44. The reader remembers the old key, and it would automatically change cards to the new key if you set it to automatically update keys (see *Controlling If/ When Card Keys Are Automatically Updated* below). It would also remember the old key if you manually updated cards.

However, suppose in January you set the key to 11 22 11 22 11 22 11 22, in February change it to 33 44 33 44 33 44 33 44, and in March change it again to 55 66 55 66 55 66 55 66. Cards that got used during February would have been updated to 33 44 33 44 33 44 33 44; cards that didn't get used during February would still have January's key of 11 22 11 22 11 22 11 22. The reader can automatically update those cards with the most recent old key (55 66 55 66 55 66 55 66), but it would no longer recognize the prior old key of 11 22 11 22 11 22 11 22. If you have a situation like this, to update the older cards, you must manually enter the old key to use. You can avoid ever having to do this if you make sure that all cards get updated each time you change your key.

```
SET OLD READER KEY
* BACK       # NEXT
```

Press ENTER. You'll see:

```
ENTER OLD READER KEY
      (0 - 255)
       1 OF 8
```

Enter the first of your 8 numbers and press ENTER. Repeat this for the rest of your 8 numbers. When you are done, you'll see a screen like this that confirms the key:

```
  CONFIRM KEY VALUES
240     10      240    34
 77    255        1    19
      * NO     # YES
```

Press # (Yes) to confirm and save the old key. The reader will now ask about automatic updates; these entries are the same as those described under Determining Whether Keys Get Automatically Updated on Cards on page 60.

If you have an older card and know that one of several keys was used on it but aren't sure which one, enter the various old keys in turn here, trying to update the card each time.

New Cards Automatically are Handled

The reader automatically knows how to set the key for blank manufacturer cards; an old key isn't needed if a card's key has never been set.

Controlling If/ When Card Keys are Automatically Updated

When you enter a new key, the reader lets you indicate if/when keys get automatically updated. Set Auto Updates lets you change that setting if you need to. The options you have here are exactly the same as the ones you see when you enter a new key; for details, see *Determining Whether Keys Get Automatically Updated on Cards* on page 60.

```
  SET AUTO UPDATES
  * BACK  # NEXT
```

Press ENTER. You'll see:

```
ENABLE AUTO UPDATES?
   * NO      # YES
```

These options are exactly like what you see when adding a new key; see Determining Whether Keys Get Automatically Updated on Cards on page 61.

Manually Updating a Key on a Card

Update a Card lets you manually update any card that currently contains the old key stored in the reader or that contains either of HID's default keys. You would need to manually update cards if you had reached the limits of the number of cards/days for automatic updates, or if you chose to disable automatic updates.

To update a card with a key that isn't the most recent old key, see *Setting the Old Key in the Reader* on page 62 for help and for further discussion of when you might need to do this.

You won't generally need to use this option if you set the reader to automatically update cards.

UPDATE A CARD
*** BACK # NEXT**

Press ENTER. You'll see:

PRESENT SMART CARD
TO READER

Present the card to the reader. You'll see a message that tells you whether the reader was able to update the card.

Controlling Fingerprint Template Compression

Set Record Type controls how much the user's fingerprint template is compressed before writing it to the card.

We recommend Maximum Compression: it gives the fastest read/write times. If you use (or plan to use) your iCLASS cards with other devices, Maximum Compression also leaves the most space for the other devices. Programmed iClass cards require a compressed format if users enroll two fingers: programmed cards only have 1568 bytes available, so two uncompressed finger templates won't fit. To help you figure out whether you can use your cards with both FingerKeys and some other device, here's the exact number of bytes used be different configurations:

SET RECORD TYPE
*** BACK # NEXT**

Press ENTER. You'll see:

NO COMPRESSION
*** NO # YES**

Press * (No) until you see the level of compression you want; when the appropriate level of compression is shown, press # (Yes):

MAXIMUM COMPRESSION
*** NO # YES**

	Number of Enrolled Fingers	
	1	**2**
No Compression	854 bytes	1654 bytes
Minimum Compression	566	1078
Medium Compression	454	854
Maximum Compression	310	566

Erasing Cards

Erase Card clears all areas that the FingerKey has secured on the card, removes user identification and fingerprint templates, and resets the card's key for these areas to the HID default key so the card is ready to be used by another user or even another application. If you're also using this card with other applications/devices, this command does not erase or affect the areas of the card controlled by those applications or devices as long as they use a different key.

The key in the reader and the card must match to erase the card; you can't erase a card with an unknown key.

ERASE CARD
*** BACK # NEXT**

Press ENTER. You'll see:

ERASE USER DATA
*** NO # YES**

Press # (Yes) to confirm that you want to erase the card. You'll see:

PRESENT SMART CARD
TO READER

Present the card to get information about the user on the card.

Listing Info about the Card User

List Card User lets you get the user ID, authority level, reject threshold, flag information (Schlage Biometrics internal use), and iCLASS serial number (as a hex value) from any card that you present. This information is shown over three screens.

The key in the reader and the card must match to list information from the card; you can't list information from a card with an unknown key.

LIST CARD USER
*** BACK # NEXT**

Press ENTER. You'll see:

PRESENT SMART CARD
TO READER

Present the card to get information about the user on the card.

Appendices

FingerKey Specifications

Size:	width: 5.31 in (13.49 cm)
	height: 5.03 in. (12.78 cm)
	depth: 2.98 in. (7.75 cm)
Power:	12 VDC
Weight:	less than 1.5 lbs (.68 kg)
Wiring:	Belden cable 82723 or the equivalent (minimum 22 gage); maximum total line length for RS-485 network: 4000 ft. Maximum total line length to connect RS-232 reder to host computer: 50 ft.
Temperature:	Operating: 0C to 45 C (32F to 113F)
	Non-operating (storage): -10C to +60C (14F to 140F)
Relative Humidity Non-Condensing:	Operating: 0% to 80%
	Non-operating (storage): 0% to 85%
Memory Retention:	5 years using a standard internal lithium battery
Communications:	RS-485 2-wire; RS-232
Baud Rate:	4800, 9600, 19200, 28800, 38400, 57600
User Capacity:	50 users, expandable
Card Reader Input:	Proximity, Wiegand, Magnetic Strip
Card Reader Output:	Wiegand (8 configurations), Magnetic Strip (2 Configurations)
Duress Code:	Second finger can be used to indicate duress

Limited Warranty

Schlage Biometrics, Inc. warrants to the original user that Schlage Biometrics products will be free of defects in material and workmanship for one year from the user's purchase date or 15 months from the date the reader was shipped from the factory, whichever is sooner, provided:

1. Schlage Biometrics has been notified within such period by return of any alleged defective product, free and clear of all liens and encumbrances, to Schlage Biometrics or its authorized dealer, transportation prepaid; and
2. The product has not been abused, misused, or improperly maintained and/or repaired during such period; and
3. The defect wasn't caused by ordinary wear and tear; and
4. The defect isn't the result of voltage surges/brownouts, lightning, water damage/flooding, fire, explosion, earthquakes, tornadoes, acts of aggression/war, or similar phenomenon; and
5. Schlage Biometrics has approved accessories used as integral to the product.

If Schlage Biometrics inspects the product and finds that it is defective, Schlage Biometrics will, at its option, either repair or replace the product, or if agreed upon, refund the purchase price, less a reasonable allowance for depreciation, in exchange for the returned product.

Schlage Biometrics makes no other warranty and all implied warranties including any warranty of merchantability or fitness for a particular purpose are limited to the warranty period set forth above.

Schlage Biometrics' maximum liability is limited to the purchase price of the product. In no event shall Schlage Biometrics be liable for any consequential, indirect, incidental, or special damages of any nature arising from the product or its use.

Schlage Biometrics may change the design of any of its products without incurring any obligation to make the same change on units previously purchased.

Index

Ingersoll Rand
Security Technologies

Ingersoll Rand's Security Technologies Sector is a leading global provider of products and services that make environments safe, secure, and productive. The Sector's market-leading products include electronic and biometric access control systems; time and attendance and personnel scheduling systems; mechanical locks and portable security, door closures and exit devices, steel doors and frames, architectural hardware and technologies and services for global security markets.

408.341.4110

www.schlage.com

www.ingersollrand.com

Schlage
Biometric Solutions
Ingersoll Rand Security Technologies
1520 Dell Avenue
Campbell, CA 95008
Office: 866-861-2480/512-712-1413 (international)
Fax: 866-303-1794/408-341-4111
E-mail: sbssupport@irco.com

SCHLAGE

HandNet for Windows

Terminal User's Guide

Ingersoll Rand
Security Technologies

Table of Contents

Getting Started

Introduction

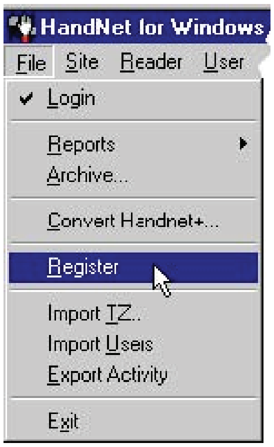
What HandNet Does

HandNet for Windows lets you control and monitor many connected HandKey readers. In this one program, you can control who can use each reader and when. You can also monitor activity and alarms for all readers at once.

Registering HandNet

After the first time you use this Version of HandNet, you have fourteen days to register it. You must register it even if you registered your previous Version of HandNet. If you do not register it within fourteen days, you will not be able to log into the program. The process should only take a minute.

1. If you have not logged into HandNet yet, log in; see page 4.
2. If the registration screen is not shown, pick *Register* from the *File* menu, and click the *Print the registration form* button on that screen.
3. Fill the form out and fax it to the number at the top of the form. Once we receive your completed form, we will fax an activation code back to you within two business days (since it could take two days for us to send your code back, please print and send the registration form now; do not wait until day fourteen).
4. Pick *Register* from the *File* menu, enter the activation code we sent, and click the *Activate* button. Once you do this, HandNet is permanently functional.



New Features in Version 2.0

HandNet for Windows Version 2.0 provides a number of new features, but these are only available to you if you purchased the upgrade to the full feature set. If you did not purchase this upgrade and you would like to, please contact your dealer; once you pay for the upgrade, we will send you a new access code to enter on the *Registration* screen. Once you enter this code, all the new features are immediately available to you.

How to tell if I have access to the new features

1. From the main menu bar, click the *Help* menu, and then click *About HandNet for Windows*.
2. Check the bottom of the box that pops up. To be able to use the new features, the last line must say *You may use all features of this software*. If this line says *Your current license does not let you use the enroll*..., you must contact your dealer and upgrade your license before you can use the new features (once you upgrade, we willsend you an access code that makes these feature available).

The new features

Enrolling Users from HandNet: Previously, to enroll a user you had to go to a features reader, enter command mode on the reader, and enroll the user. Now, if you have a reader that is near the computer, you can add the user in HandNet, select the reader to enroll at, and pick *Enroll* from the *Reader* menu without ever having to deal with command mode on the reader; see page 87.

User Access for a Limited Time Period: HandNet now lets you specify that a user's access should start and stop at certain days or times. For example, if a contractor needs access to your facility, you can now set the access to expire on the day that the contract ends. This gives you more complete control of who can access readers and when; see page 93.

Import/Export Users: If you have more than one computer system running HandNet and you want users added on one system to be available to the others, HandNet now lets you export user information from one program and import it into another; see page 99.

Exporting Activity for External Report Generation: If you want to create custom activity reports using some external report tool, *Export Activity* on the *File* menu sends all of your current activity to an access database file called expactvt.mdb; see page 116. While the main HandNet database files are password protected for security reasons, this file is not so you can open it and access any information in it at will. You can also set HandNet up to automatically export activity whenever you archive activity.

* * * * *

Getting Help in HandNet

The online help has the same information that is in this manual. To get help in HandNet, press F1. This brings up help for the screen you are on. From there, you can use the contents, index, or search tabs at the left of the help window to find any topic.

For Basic Topics

Click the *Contents* tab at the top of the left pane, click a book to open and click a topic. Not every topic is in the *Contents* tab, so if you do not find what you need, try the *Index* or *Search* tabs.

For Groups of Topics on a Single Theme

In addition to the contents you can also click on the pull-down list right under the *Previous/Next* buttons (in the bottom middle of the header). This list contains a number of important groups of topics. Once you are on one of these topics, the *Next* and *Previous* buttons work as well.

Screens and Menus

On menus and screens in this help, click any option on the screen to jump to help on that item.

When to Use the Index and When to Search

Use the index for main themes like adding a reader or enrolling a user. Use the search for minor points. For example, if you type *enroll* on the *Index* tab, you get three main topics that deal with enrolling users. On the *Search* tab, *enroll* gets you nearly thirty topics where *enroll* appears somewhere in the text. For main topics, the index gets you to what you want more directly. On the other hand, if you remembered that a screen somewhere said something about the number of tries a user gets before having access denied, the *Search* tab would check the entire text and find this detail for you. Use the *Index* tab to find items that are likely to be a main topic; use the search tab to find minor points.

Marking a Topic to Return to

To mark a topic in the help that you want to come back to:

1. Go to the topic that you want to mark.
2. Click the *Favorites* tab at the top of the left pane.
3. Click the *Add* button at the bottom of the pane. This adds the topic to your favorites list.

To get back to any marked topic later:

1. Click the *Favorites* tab at the top of the left pane of the help window.
2. Double-click the topic.

Getting In and Getting Out

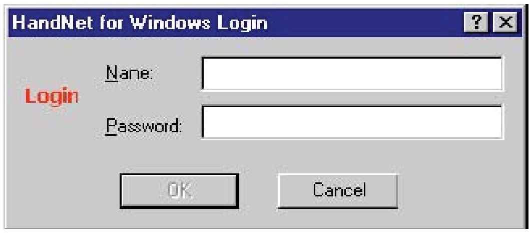
Starting HandNet

To start HandNet, either click the HandNet icon on your Windows desktop, or click the *Start* menu on your Windows taskbar, highlight *Programs*, and highlight and click *HandNet for Windows*.

Logging into HandNet

HandNet requires you to log in before you can make any changes; this prevents unauthorized people from changing information. If you are not logged in, you can look at the lists of activity, users, and readers (network), but you cannot change any information and cannot use any other options.

1. Click *Login* on the *Toolbar,* or pick *Login* from the *File* menu. The program brings up this box:



2. Type your name and password, and click *OK*.

If this is a new system: Use a name of *1234* and a password of *new* (change this name and password immediately so unauthorized people cannot user the program).

After initial setup: If you forget your name or password, see your supervisor or security administrator.

Passwords are NOT case sensitive. For example, if your password is *narnia*, then *Narnia* and *NARNIA* would also work.

After you are done using HandNet, be sure to log out again so unauthorized operators will not be able to use the program.

Changing the Initial Login Name and Password

HandNet comes set up with a login name of *1234* with a password of *NEW*. This lets you get into HandNet when you first start using it, but this is not secure; anyone may read this manual and find this name and password. To keep unauthorized users from using HandNet, change this password before you add any other information.

1. Click the *View* menu.
2. Click *Settings*.
3. Click the *Operators* tab.
4. Click the operator named *1234* and then click *Edit*. This takes you to the *Operator Definition* screen, which has settings for this user.
5. Change the *Name* to your name, and change the *Password* to something you will remember but that no one else will be able to guess. Click *OK* to return to the list of operators.

Remember the name and password you enter; if you forget it, you will not be able to get into HandNet. Do not change any other settings; this user is set up to use any option in HandNet; if you uncheck any boxes, you will not be able to use the corresponding options.

6. Click the *Close* button at the bottom of the box to close *System Settings*.

Logging out of HandNet

Log out of HandNet when you are done using it. This prevents unauthorized people from changing information. Someone who is not logged in can look at the lists of activity (including alarms), users, and readers, but cannot change any information or use any other options.

To log out, click the *Logout* button on the *Toolbar* or pick *Login* again from the *File* menu to uncheck it.

Exiting HandNet

For security purposes, you should generally log out of HandNet when you are done making changes so unauthorized people cannot add users or make changes. However, unless you are going to install a new Version of the HandNet software, or you need to restart the computer HandNet is running on, you do not typically want to exit from the HandNet program. If you exit (that is, shut down the program), you disconnect it from all readers. While all readers will continue to record activity and give access as appropriate, the program will not receive any information from the readers or process any alarms during the time that HandNet is not running. Because of this, you would usually leave HandNet running all the time.

* * * * *

Getting Started Overview

Procedure for Getting Started and Setting Up

QUICK STEPS

Getting Started with HandNet for Windows

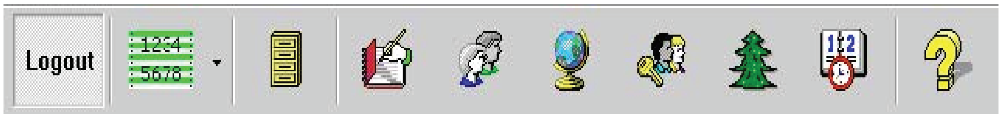
1. Log in; see page 4.
2. If you have not done so yet, register HandNet. HandNet will not let you log in after fourteen days if you do not register it; see page 1.
3. Change the initial password so unauthorized users will not be able to use the program; see page 4.
4. If you have been using readers without HandNet and you want to get the users from the reader(s):
    1. Pick *Settings* from the *View* menu.
    2. Click the *Security* tab.
    3. Check the box by *Do not delete unauthorized enrollments.*

   This prevents HandNet from deleting the users from the readers when you enable them (you will import the users from the reader later, after setting up the readers and sites). If you did not change this setting, when you enabled the site and reader, HandNet would regard all of the users in the reader as unauthorized (because they were not in HandNet yet), and it would delete them from the reader.
5. Set up site(s), that is, groups of connected readers; see page 33.
6. Set up readers; see page 42.
7. If you want to control which days and times users can access readers, set up time zones (see page 61) and holidays (see page 65).
8. If you have set up time zones and holidays, or if you want to give some users access through some readers but not others, set up access profiles; see page 67.
9. If you have previously been using one of our older MS-DOS products (HandNet Plus or HandNet), convert the users; see page 98 (if you have been using HandNet for Windows 1.09 or later, you do not need to convert anything; this Version of HandNet automatically updates information for the new Version).
10. If you have been previously using readers without one of the HandNet products and you need to get users from the reader(s), upload users from the reader(s); see *Getting User Information from a Reader* on page 99.
11. Add users; see page 74.
12. Enroll the users; see page 87.
13. When you are done using HandNet, be sure to log out so unauthorized people will not be able to add or change anything; see page 5.

Menus and Navigation

Toolbar

The toolbar looks like this:



If you are not logged in yet, the first button will be a login button and a number of the other will be disabled.

Turning the Toolbar On and Off

Toolbar on the *View* menu turns it on or off.

Options on the Toolbar

Login	You see this button if you are not logged in yet. Click this button to login to HandNet; see page 4. Without logging in, you cannot make any changes or do anything other than look at basic information.
Logout	Once you log in, the first button changes to the *Logout* button. If you are going away from the computer, logging out prevents making unauthorized changes. If anyone could possibly get access to the computer in your absence, logging out is an important security precaution.
1234 5678 ▾	The main button lets you generate a custom activity report; see *Creating a Custom Activity Report from the Reports* Menu on page 105. The small arrow to the right pulls down the *Reports* menu; see page 13.
🗄	This lets you archive older activity; see page 113.
📓	This opens the *Activity* window; see page 101. The *Activity* window lists all actions you take in HandNet, and actions or alarms from each reader. If the *Activity* window is already open and behind another window, this brings it to the front.
👥	This opens the *Users* window; see page 71. This lists everyone who is potentially able to access readers. If the *Users* window is already open and behind another window, this brings it to the front.
🌐	This opens the *Network* window; see page 31. The *Network* window lists all of your sites, readers, and their current status. If the network window is already open and behind another window, this brings it to the front.

🔑	This takes you to the access profile settings; see page 67. Access profiles let you control which readers different types of users have access to and when.
🎄	This takes you to the holidays settings; see page 65. If users have different access on holidays than on other days, the holidays settings identify when those days are.
1 2	This takes you to the settings that let you define different periods of time when users can have access; see page 61 (in HandNet, we call these time zones, but there is no connection to the time zones we usually think of that have to do with different times around the world).
?	This pops up the online help for HandNet. The help contains the same information as this manual but arranged in a slightly different format. To get help for the screen you are on, you can also press F1 anywhere in HandNet. The help has a complete index and also lets you search for specific text; see page 3.

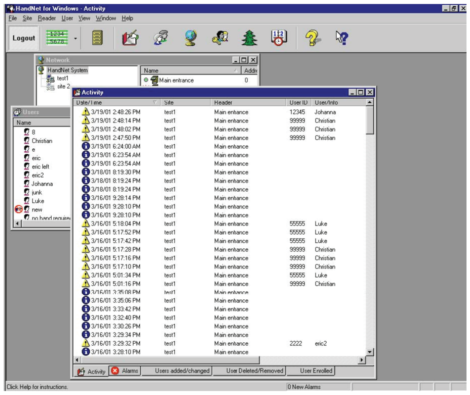
* * * * *

Tiling the Display Windows

HandNet lets you keep open the *Activity* window, the *Users* window, and the *Network* window (which shows sites and readers). If you have more than one window open, *Tile Horizontally* on the *Window* menu adjusts the open windows so they fill the Handnet window from side to side, and so they do not overlap and cover each other up.

Example of Windows that are NOT Tiled

Notice that the front windows cover up parts of the windows behind them and that the windows do not fill up the screen from side to side.



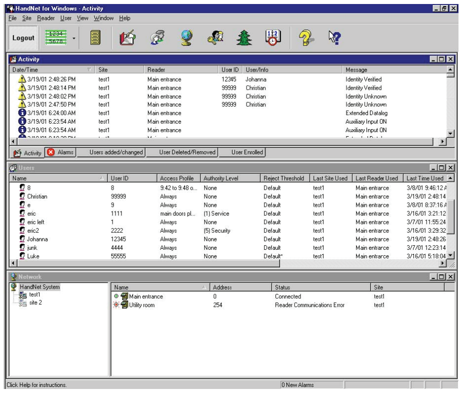
Name	Addr
Main entrance	0

Name
8
Christian
e
eric
eric left
eric2
Johanna
junk
Luke
new
no hand require

Date/Time	Site	Reader	User ID	User/Info
3/19/01 2:48:26 PM	test1	Main entrance	12345	Johanna
3/19/01 2:48:14 PM	test1	Main entrance	99999	Christian
3/19/01 2:48:02 PM	test1	Main entrance	99999	Christian
3/19/01 2:47:50 PM	test1	Main entrance	99999	Christian
3/19/01 6:24:00 AM	test1	Main entrance		
3/19/01 6:23:54 AM	test1	Main entrance		
3/19/01 6:23:54 AM	test1	Main entrance		
3/18/01 8:19:30 PM	test1	Main entrance		
3/18/01 8:19:24 PM	test1	Main entrance		
3/18/01 8:19:24 PM	test1	Main entrance		
3/16/01 9:28:14 PM	test1	Main entrance		
3/16/01 9:28:10 PM	test1	Main entrance		
3/16/01 9:28:10 PM	test1	Main entrance		
3/16/01 5:18:04 PM	test1	Main entrance	55555	Luke
3/16/01 5:17:52 PM	test1	Main entrance	55555	Luke
3/16/01 5:17:42 PM	test1	Main entrance	55555	Luke
3/16/01 5:17:28 PM	test1	Main entrance	99999	Christian
3/16/01 5:17:16 PM	test1	Main entrance	99999	Christian
3/16/01 5:17:10 PM	test1	Main entrance	99999	Christian
3/16/01 5:01:34 PM	test1	Main entrance	55555	Luke
3/16/01 5:01:16 PM	test1	Main entrance	99999	Christian
3/16/01 3:35:08 PM	test1	Main entrance		
3/16/01 3:35:06 PM	test1	Main entrance		
3/16/01 3:33:42 PM	test1	Main entrance		
3/16/01 3:32:40 PM	test1	Main entrance		
3/16/01 3:30:26 PM	test1	Main entrance		
3/16/01 3:29:34 PM	test1	Main entrance		
3/16/01 3:29:32 PM	test1	Main entrance	2222	eric2
3/16/01 3:28:10 PM	test1	Main entrance		

Example of Windows that ARE Tiled

Notice that none of these windows cover any parts of the other, and that the windows now fill up the screen from side to side.



Date/Time	Site	Reader	User ID	User/Info	Message
3/19/01 2:48:26 PM	test1	Main entrance	12345	Johanna	Identity Verified
3/19/01 2:48:14 PM	test1	Main entrance	99999	Christian	Identity Verified
3/19/01 2:48:02 PM	test1	Main entrance	99999	Christian	Identity Unknown
3/19/01 2:47:50 PM	test1	Main entrance	99999	Christian	Identity Unknown
3/19/01 6:24:00 AM	test1	Main entrance			Extended Datalog
3/19/01 6:23:54 AM	test1	Main entrance			Auxiliary Input ON
3/19/01 6:23:54 AM	test1	Main entrance			Auxiliary Input ON

Name	User ID	Access Profile	Authority Level	Reject Threshold	Last Site Used	Last Reader Used	Last Time Used
8	8	9:42 to 9:48 o...	None	Default	test1	Main entrance	3/8/01 9:46:12 A
Christian	99999	Always	None	Default	test1	Main entrance	3/19/01 2:48:14
e	9	Always	None	Default	test1	Main entrance	3/8/01 8:37:16 A
eric	1111	main doors pl...	(1) Service	Default	test1	Main entrance	3/16/01 3:21:12
eric left	1	Always	None	Default	test1	Main entrance	3/7/01 11:55:24
eric2	2222	Always	(5) Security	Default	test1	Main entrance	3/16/01 3:29:32
Johanna	12345	Always	None	Default	test1	Main entrance	3/19/01 2:48:26
junk	4444	Always	None	Default	test1	Main entrance	3/7/01 12:23:14
Luke	55555	Always	None	Default*	test1	Main entrance	3/16/01 5:18:04

Name	Address	Status	Site
Main entrance	0	Connected	test1
Utility room	254	Reader Communications Error	test1

* * * * *

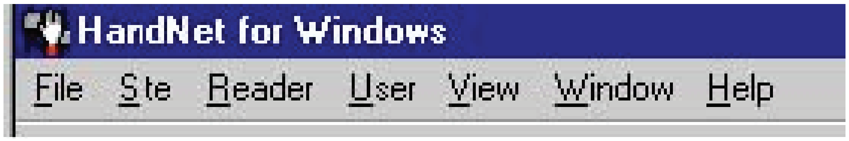
Menu Overviews

Pulling Down Menus with the Keyboard instead of the Mouse

If you prefer working from the keyboard rather than clicking with the mouse, you can hold the *ALT* key down and then type the underlined letter in the choice. For example, to open the *View* menu, you would hold *ALT* down and type *V* (this is often the first letter in the option, but not always).

Main Menu Bar

The main menu bar looks like this:



These menu options are briefly summarized below. The following pages contain more detail on the options on these menus.

File: The *File* menu lets you log in and out, generate reports, archive older activity, import setup information, and shut the program down; see page 11.

Site: The *Site* menu lets you add and change settings for sites (groups of connected readers); see page 14.

Reader: The *Reader* menu lets you add new readers, delete readers, and rename readers in the HandNet network. You can also unlock, relock, and lockup the selected reader, enroll a user at the selected reader, activate and deactivate an auxiliary device, and send (download) time, time zones, users, and setup configuration to selected readers; see page 15.

User: The *User* menu lets you add users, delete users, rename users, change information for a selected user, and create custom entries to collect additional information about users; see page 17.

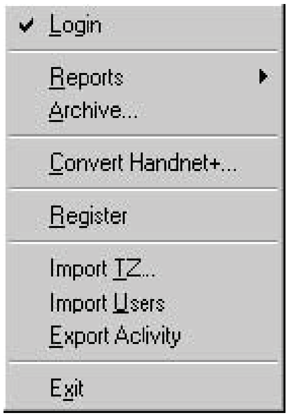
View: The *View* menu lets you open the *Users, Activity, and Network* windows (the *Activity* window lists both activity and alarms; the *Network* window lists all of your sites and readers). The *View* menu also lets you turn the toolbar on or off. And it lets you get to access profiles, holidays, activity filters, time zones, and system settings (you do not need these options on an ongoing basis; these are normally only used when setting the program up); see page 18.

Window: The *Window* menu lets you switch between open windows, tile open windows horizontally on the screen, or switch panes within the *Network* window; see page 20.

Help: The *Help* menu lets you pop up the help system you are looking at now (you can also press F1 to pop up *Help*); see page 21.

File Menu

The *File* menu lets you log in and out, generate reports, archive older activity, import setup information, and shut the program down.



Login: You must log in to HandNet before you can do anything other than look at information; see page 4. You must log in to acknowledge alarms, add sites and readers, add or change users. When you are done using the program, click this same option again to log out so unauthorized operators cannot use the program.

Reports: This brings up another menu that lists several standard reports, and that lets you create custom reports based on the activity that you see in the *Activity* window; see page 13.

Archive: This takes older information from the current activity file and stores it in a separate file. Once you archive information, the activity is no longer visible in the *Activity* window, but you can still generate reports based on the archives.

Convert Handnet+: If you have been using HandNet+ or HandNet (our older MS-DOS programs), and are just switching to HandNet for Windows, this converts user information from HandNet+ and adds it to the user list in HandNet for Windows. Information imported includes: user name, user ID number, authority level, and reject threshold; see page 98.

Register: After the first time you use this Version of HandNet, you have fourteen days to register it. You must register it even if you registered your previous Version of HandNet. If you do not register it within fourteen days, you will not be able to log into the program. The process should only take a minute. To register HandNet:

1. If the registration screen is not shown, pick *Register* from the *File* menu, and print the registration form.

2. Fill the form out and fax it to the number at the top of the form. Once we receive your completed form, we will fax an activation code back to you within two business days (since this could take two days for us to send your code back, please print and send the registration form now; do not wait until day fourteen).

3. Pick *Register* from the *File* menu, enter the activation code we sent, and click the *Activate* button. Once you do this, HandNet is permanently functional.

Import TZ: This lets you change the access profile to *Always* or *Never* for many users based on information in a text file; see *Changing Access for Many Users at Once* on page 95.

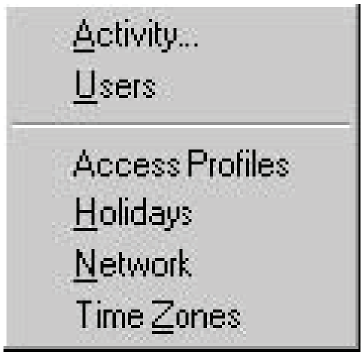
Import Users: If you have readers connected to several different computers (each with its own copy of HandNet) and if users added to one system need to be available on the others, *Import Users* lets you bring in users that were added or changed in another copy of HandNet; see page 99. If all of your readers are connected to a single copy of HandNet, you do not need this feature.

Export Activity: If you want to create custom activity reports using some external report tool, *Export Activity* sends all of your current activity to an access database file called *expactvt.mdb*; see page 115. The main HandNet database files are password protected for security reasons, but this file is not, so you can open it and access any information in it. If you are only going to generate reports with *Activity Reports* on the *File* menu, you do not need this option; using it would only create a file that you do not need.

Exit: This closes the HandNet program, disconnecting it from all readers. All readers will continue to be able to open doors, but the program will not receive any information from the readers or process any alarms while HandNet is not running. Unless you are going to install a new Version of the HandNet software, or you need to restart the computer that HandNet is running on, you do not want to exit the HandNet program. For security purposes, you would generally logout so unauthorized people cannot add users or make changes, but you would leave the HandNet program running all the time.

Reports Menu

To get to the reports menu, click *Reports* on the *File* menu. This menu lets you create custom activity reports and print several stock reports.



Activity: This lets you create reports based on any activity recorded by HandNet. This includes any information in the *Activity* window and any activity that you have chosen to archive. You can customize these reports to include only the information you need; see *Creating and Printing Custom Activity Views* on page 105.

Users: This lists all of the users in the system. The report includes each user's name, ID number, authority level, reject level, and access profile. It also indicates the last reader used, the last access time, and whether the user is enrolled. You can use this report to see if a user is enrolled and to make sure one user is not enrolled with multiple ID numbers. If you have created custom user entries, this report does NOT show any of them.

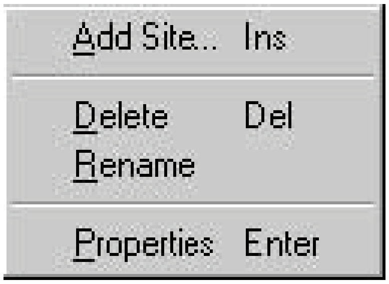
Access Profiles: If you have set up different access profiles to give different types of users access to different readers or at different times, then this report can help you see whether you have set your access profiles up the way you wanted. This report lists each access profile, sites and readers the profile gets access to, and the time zone that users can access each reader; see page 67 for more about setting up access profiles.

Holidays: This list all of the holidays you have set up in HandNet. It lists the name of each holiday, the month, and the date. This report helps you make sure you have correctly added all holidays for the year (if you have set up any time zones to prevent access on holidays, or to give different access on holidays than on other days, the *Holidays* list identifies when those holidays are. If you do not give different access on holidays than on other days, you do not need to set holidays up or print this report); see page 65 for more about setting up holidays.

Network: This report tells whether each site is enabled and connection information (communications port, baud rate, phone number or IP address, time adjustment, and modem speaker status). It also lists readers at the site, whether they are enabled, and their addresses. This report is used during setup to make sure the network is set up properly.

Time Zones: This lists all of the different user access period that you have set up (though we call these access periods *time zones*, they have no connection to the time zones we usually think of that have to do with different times around the world). The report includes the name of each time zone, the time periods it includes, and the days of the week those time periods apply. During setup, this report helps you see if you have set up all of the necessary time zones and configured them correctly (if you do not need to limit access by day or time -that is, if all users may use the readers twenty-four hours a day, seven days a week if they wanted- then you do not need time zones); see page 61 for more about setting up time zones.

Site Menu


Add Site... Ins

Delete Del

Rename

Properties Enter

In HandNet, a site refers to a group of up to thirty-two connected readers. Put another way, one reader is physically connected to the computer (by network, serial cable, or modem), and up to thirty-one additional readers can be daisy chained to that first reader; that is, a cable runs from the first reader to the second, another cable runs from the second to the third, and so on. We call this chain of readers a site. A site does not have any connection to a particular building or location; these readers could be in one building or in more than one building (if the buildings are close enough to run a cable from one to the other), and one building could have one or many sites.

Add Site: This adds a new site to the HandNet network; see page 34. You must set up a site in HandNet before you can set up readers.

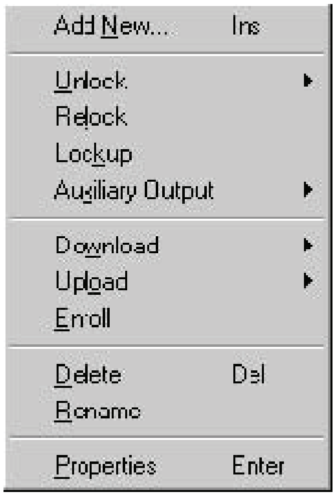
Delete: If you have selected a site in the Network window, *Delete* removes the site and all readers assigned to it. HandNet will ask you to confirm that you want to delete the site. Make sure that you have selected the appropriate site since, if you continue, you will not be able to undo the deletion unless you have made a backup of the files that contain your site and reader information (see page 126 for more about making backups).

Rename: If you have selected a site in the *Network* window, this lets you rename that site (you can also just click once on the site name in the *Network* window and rename it there without using this option). Renaming a site does not change any of its properties, and does not require you to set anything up again; it only changes the name that appears in the lists on the screen and in reports that you generate. You might want to rename a site if you discovered that the original name is not clear.

Properties: This takes you to a window with three tabs that let you look at or change settings related to how the site is connected to the computer with the HandNet software; see *Changing a Site* on page 34 for further detail.

Reader Menu

The *Reader* menu lets you add new readers, delete readers, and rename readers in the HandNet network. You can also unlock, relock, and lockup the selected reader, enroll a user at the selected reader, activate and deactivate auxiliary output, and send (download) time, time zones, users, and setup configuration to selected readers.



To do anything here, except add a reader, you must select one or more readers first.

Add Reader: This lets you add and configure a reader to the HandNet network; see page 42 (you must set up a site before you can add readers in HandNet).

Unlock: When you highlight *Unlock* on the *Reader* menu, you see another menu with two choices: *Indefinite* and *Timed*.

Indefinite unlocks the door connected to that reader and leaves it unlocked until you choose *Relock* on the *Reader* menu to lock it again. If you regularly want a door unlocked during certain hours, pick properties from the *Reader* menu and go to the *Configuration* screen. In the *Auto Unlock Time Zone* you can indicate when the door should be automatically unlocked. The program will automatically lock the door again at the end of the time zone.

Timed unlocks the door connected to that reader and leaves it unlocked only for the number of seconds specified on the *Configuration* page in the *Reader Properties* (that is, it unlocks the door for the same number of seconds that the door would be unlocked if it were opened by a reader).

See *Locking and Unlocking Doors* on page 130 for more about these options.

Relock: If you have unlocked a door with *Unlock, Indefinite* option, this locks it again; see page 128.

Lockup: This disables the lock on the door for the selected reader. The reader will still let users enter their ID numbers and still verify hands, but the door will stay locked even for valid users. The door will stay locked until you choose *Unlock* or *Relock*; see page 128.

Auxiliary Output: If an auxiliary device is connected to a reader, this lets you turn that device on or off for the selected reader; see page 129. *Auxiliary Output* can control local lighting, trigger a third party alarm system, activate a bell, and so on.

Download: This lets you send information to the selected readers. While HandNet automatically sends the appropriate information to readers, occasionally you will need to use this when correcting a problem with a reader; see *Resending Information to a Reader* on page 60.

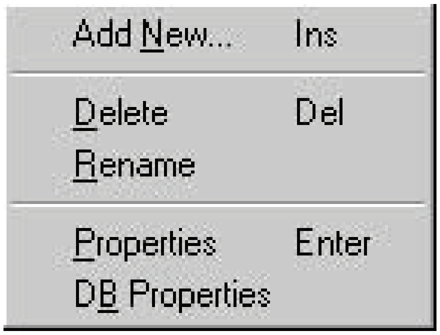
Upload (Users): This lets you get user information from the selected readers. You would do this if you had been using a reader independent of the HandNet program and now wanted to add all of the users stored in that reader to the program; see *Getting User Information from a Reader* on page 99.

Delete: This removes the selected readers from the HandNet network.

Rename: This renames the selected reader. Renaming the reader does not change any of its properties and does not require you to set anything up again; it only changes the name that appears in the lists on the screen and in reports that you generate. You might rename a reader if you discovered that the original name was not clear or if you changed the purpose of the areas the reader gave access to.

Properties: This takes you to a window with a number of tabs that let you look at or change a number of settings related to the reader; see *Changing Reader Settings with Reader Properties* on page 45.

User Menu



The *User* menu lets you add users, delete users, rename users, change information for a selected user, and create custom entries to collect additional information about users (if you have already set up users in a reader that you are connecting to HandNet, do not recreate those users; you can *Upload Users* from the reader; see *Getting User Information from a Reader* on page 99).

To change, delete, or rename users, select a user first on the list of users (for the list of users, pick *Users* from the *View* menu, or press *CTRL-U*).

Add New: This lets you add new users; see page 74. After you add the user, you must enroll the user (see page 87) before the user will have access through the readers.

Delete: This lets you remove a user from the program. You would do this if you never wanted that user to be able to use any of the readers in the HandNet network (if you might need the user again but want to keep the user from using any of the readers, you can also change the user's access profile to *Never*).

Rename: This lets you rename the selected user. You would use this if you entered the user's name incorrectly. You would also use this if you added multiple users at once. When you use *Add multiple new users* to add a number of users automatically, the program uses the ID number for the name. You would want to rename these users so you could identify which ID is for which user.

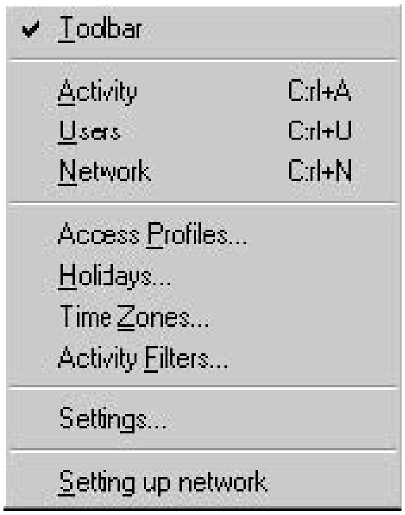
Properties: This lets you look at or change information for the selected user; see *Changing Users* on page 90.

DB Properties: This gives you a summary of the total numbers of enrolled and unenrolled users. It also lets you add custom entries so you can collect additional information about users. For example, depending on your needs, you might collect emergency phone numbers, birthdays, employment start dates, or any other information you needed about your users; see *Adding Custom User Entries* on page 97.

View Menu

The *View* menu lets you open the *Users, Activity,* and *Network* windows (the *Activity* window lists both activity and alarms; the *Network* window lists all of your sites and readers). The *View* menu also lets you turn the toolbar on or off.

It also lets you get to access profiles, holidays, activity filters, time zones, and system settings. You do not need these options on an ongoing basis; they are normally only used when setting HandNet up.



Toolbar: This turns the toolbar off if it is on and turns it on if it is off. The toolbar has icons that help you quickly get to common options; see page 7. The toolbar is shown when you start HandNet. A check is shown by this option when the toolbar is displayed.

Activity: This opens the *Activity* window (or brings it to the front if it is already open and behind other windows). This lets you see recent activity and alarms. If you have created any activity filters to create lists of specific types of activities, these views are also available here. The tabs at the bottom of this window let you switch between the activity list, the alarm list, and any custom views you have created; see page 101 for more about the *Activity* window.

Users: This opens the *Users* window (or brings it to the front if it is already open and behind other windows). This window lists everyone who could potentially gain access through a hand reader; see page 71 for more about the users window (there is no connection between this list and the operators authorized to use HandNet; for people who can use HandNet, see the *Operators* tab in *System Settings* on page 24).

Network: This opens the *Network* window (or brings it to the front if it is already open and behind other windows). This window lists all of your sites and readers; see page 31 for more about the *Network* window.

Access Profiles: If some users can only use certain hand readers and/or only use them at certain times or on certain days, access profiles define when each type of user can use each reader. For example, suppose your maintenance staff should have access to the maintenance rooms seven days a week, your office staff should have access to the office but only during business hours, and your supervisors should have access to everything at any time. You would create three access profiles: one for supervisors, one for office staff, and one for maintenance personnel. These profiles would identify which readers each group could use. In these profiles you would also identify which time periods each group could use the different readers (you would set up these time periods first using time zones). After creating these different profiles, whenever you added a user, you would just identify which group the user was a part of, and the access profile for that group would automatically give the appropriate access; see page 67 for more on setting up access profiles.

To limit access to certain days or times, you must set up time zones before creating access profiles.

If you want all users to be able to use every reader any time, you do not need to set up access profiles. HandNet comes set up with an *Always* profile that lets users use any reader in the system twenty-four hours per day, seven days per week. It also has a *Never* profile that does not let the user verify at any reader at any time.

Holidays: If you have set up any time zones to prevent access on holidays or to give different access on holidays than on other days, the holidays list identifies when those holidays are. If you do not give different access on holidays than on other days, you do not need to use this option; see page 65 for more on setting up holidays.

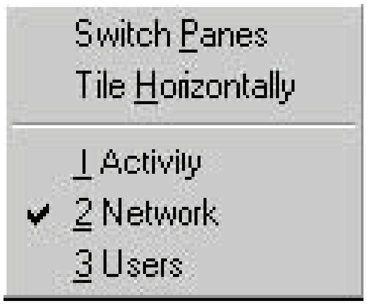
Time Zones: If you want some users to be able to use certain readers only during certain hours or on certain days of the week, time zones let you identify when access is available. For example, suppose some users should only to be able to gain access through certain readers between 8:00 AM and 5:00 PM, Monday through Friday. You would create a time zone that identified these times and days, associate that time zone with appropriate readers using an access profile, and then assign that access profile to the users. After you did this, users with that access profile would only have access during the times you identified in the time zone; see page 61 for more on setting up time zones.

If you do not need to limit access by day or time (that is, if users could use the readers twenty-four hours a day, seven days a week if they wanted), then you do not need to set up time zones.

Activity Filters: This lets you customize the information you see in an activity window by letting you identify the dates, times, sites, readers, users, message types, and messages you want to see. For example, suppose you want to see who's come in through the main entrance without having to wade through messages related to activity at other readers. You could create an activity profile that listed activity only from the main entrance reader and only if the activity was *Identity verified* (the message you get when someone enters an ID and the hand is recognized). You would then be able to choose this view and see only this activity. Activity filters can be much more complex than this; they can filter or limit an activity list to include any subset of information you need (after you create an activity filter, a tab at the bottom of the activity window will list the name of the filter; just click that tab for the corresponding information); see *Creating a Custom Activity View* on page 105 for more information.

Settings: This lets you look at or change system-wide settings; see page 22. This includes the name of the system, security, who can use HandNet, which messages trigger alarms, when old messages should be archived, and settings for importing and exporting users.

Window Menu



The *Window* menu lets you switch between open windows, tile open windows horizontally on the screen, or switch panes within the *Network* window.

You will see a check mark to the left of the window that is currently active.

Switch Panes: If the *Network* window is open, *Switch Panes* switches you back and forth between the list of sites in the left pane of the window, and the list of readers in the right pane of the window. This is primarily useful for users who cannot use a mouse; if you can use a mouse, it is easier to just click the pane you want. If the *Network* window is not open, this choice does not do anything.

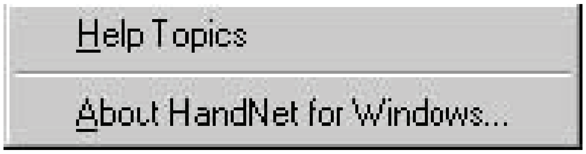
Tile Horizontally: This adjusts any open windows so they fill the HandNet window from side to side and so they do not overlap and cover each other up. If you are not sure what tiling is, see the example on page 9.

Activity: This choice is only here if you have the *Activity* window open. This makes the *Activity* window the active window (if the *Activity* window is not open, open it by typing *CTRL-A* or by picking *Activity* from the *View* menu). The *Activity* window shows the activity log, error messages, and any custom activity views you have created; see page 101 for more about the *Activity* window.

Network: This choice is only here if you have the *Network* window open. This makes the *Network* window the active window. The *Network* window lists sites and readers (if the *Network* window is not open, open it by typing *CTRL-N* or by picking *Network* from the *View* menu); see page 31 for more about the *Network* window.

Users: This choice is only here if you have the *Users* window open. This makes the *Users* window the active window (if the *Users* window is not open, open it by typing *CTRL-U* or by picking *Users* from the *View* menu); see page 71 for more about the *Users* window.

Help Menu



Instead of going to the *Help* menu, you can press *F1* from any screen in HandNet. This takes you to help for the screen you are on. If you need help on something else, you can use the *Contents, Index*, or *Search* tabs at the left of the window to find what you need.

Help Topics: This brings you into the help for HandNet. The *Help* menu contains the same information as this manual, but it lets you more easily search and jump from topic to topic; see page 3.

About HandNet for Windows: This brings up a screen with copyright information, the Version of the program, the product serial number, and the name of the person or company the product is licensed to (unless you need to give your serial number or the program Version number to one our support representatives, or unless you need to check to see if you are licensed to use all the features of the program, you probably will not need to come to this screen).

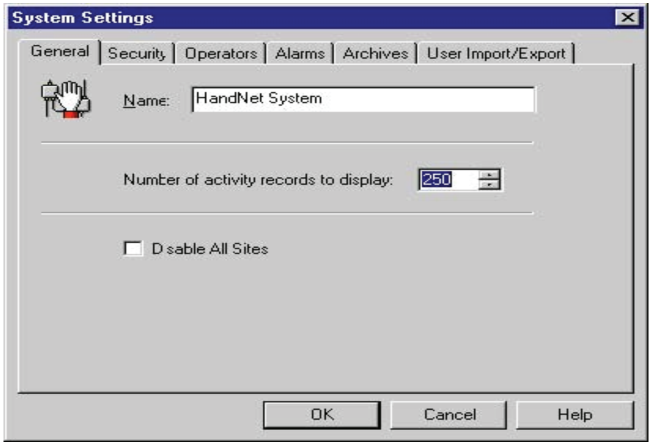
* * * * *

System Wide Settings

Settings on the *View* menu lets you control setup issues that are not related to specific sites or readers. This includes the name of the system, what user changes should be allowed at readers, who can use Handnet, which messages trigger alarms, when old messages should be archived, and settings for importing and exporting users.

General System Settings

To get to the *General* tab, pick *Settings* from the *View* menu.



Name: HandNet System

Number of activity records to display: 250

☐ D sable All Sites

Name of System

Name: This shows the name that appears above the list of sites in the *Network* window.

Amount of Activity to Show

Number of Activity Records to Display: This shows how many of the most recent activities to list in the *Activity* window. HandNet stores activities even after they are no longer listed in the *Activity* window; those that are no longer shown are still stored and still included if you print a report.

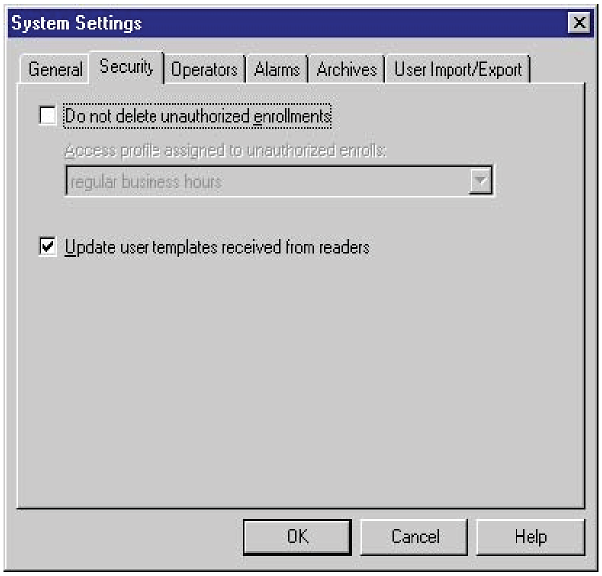
Disable All Sites

Disable All Sites: Check this box if you need to quickly prevent HandNet from trying to communicate with any site. You might check this if you were servicing a number of sites at once.

* * * * *

What User Changes Can Come from Readers

To get to the *Security* tab, pick *Settings* from the *View* menu, and then click the *Security* tab.



□ Do not delete unauthorized enrollments

Access profile assigned to unauthorized enrolls: regular business hours

☑ Update user templates received from readers

Whether Users can be Added at the Reader

Do not delete unauthorized enrollments: When this is not checked (HandNet's initial setting) you can only add new users in HandNet; you cannot add a new user directly at the reader (you can add a user at a reader if the user is in HandNet so you can enroll the user, but if you add a user at the reader that has not been added in HandNet, HandNet will delete the new user). If you want to be able to add and enroll a new user at a reader without adding the user in HandNet first, check this box. If you allow this, and if you add a new user from the reader, the user will be given the access profile selected in the entry below (you can change the access profile on the *Security* tab in *User Properties*; see page 92).

Access profile assigned to unauthorized enrolls: Indicate what access profile should be given to a user who is added at a reader (if you do not want the user to be able to access any readers until you change them in HandNet, choose *Never*).

Whether to Revise the Stored Images of Users' Hands

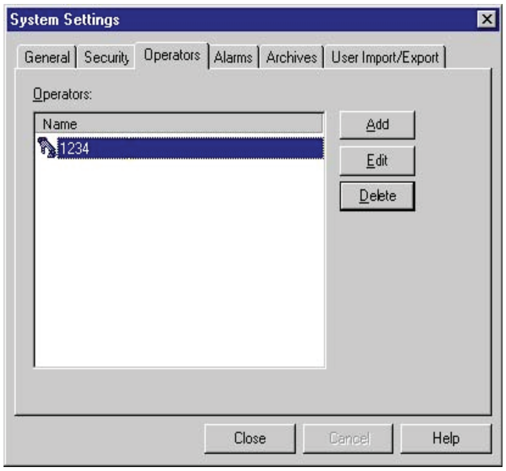
Update user templates received from readers: When you enroll a user, HandNet stores a template that contains information about the shape of the user's hand. If this box is checked, then each time a user gains access, HandNet updates this template. This means that if the user's hand changes gradually (for example, if the user gains or loses a significant amount of weight over time), the image of the user's hand in HandNet will automatically be gradually adjusted as well. If there are gradual changes, checking this prevents users from having access problems as their hands become increasingly different from the original image. If you do not check this, then readers will always compare the user's hand to the original image created when you enrolled the user. We recommend having this checked.

* * * * *

Who Can Use HandNet

The *Operators* tab lists those people who are authorized to use the HandNet program. When you click *Add* or *Edit*, the program brings up the *Operator Definition* box where you control which tasks the operator is allowed to do in HandNet.

To get to this screen, pick *Settings* from the *View* menu, and then click the *Operators* tab.

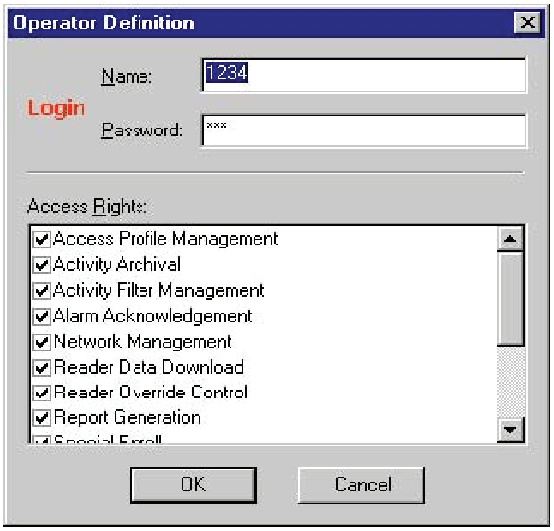


Operators:

Name
1234

Adding or Changing an Operator

You see this box when you add or edit an operator. It has the name and password the operator must use to log into HandNet. The boxes that are checked control which types of activities the operator can do.



Name: 1234

Password: ***

Access Rights:

- ☑ Access Profile Management
- ☑ Activity Archival
- ☑ Activity Filter Management
- ☑ Alarm Acknowledgement
- ☑ Network Management
- ☑ Reader Data Download
- ☑ Reader Override Control
- ☑ Report Generation
- ☑ Special Enroll

Name: Enter the name that the operator will enter on the *Login* screen; see page 4. If the operator is also a user in HandNet (so s/he can gain access through readers), the name you enter here does NOT have be the same as the name in *User Properties*.

Password: Enter the password that the operator will enter on the *Login* screen. Passwords are NOT case sensitive. For example, if the password is *narnia, Narnia* and *NARNIA* would work identically.

Which Options the Operator Can Use

Access Rights: Check the corresponding boxes to determine which tasks the operator can do in HandNet. When you add a new operator, all of the boxes are unchecked; unless you check them, the operator will be able to do little more than look at information on the screen.

Click OK to save your changes and return to the list of operators.

Deleting an Operator

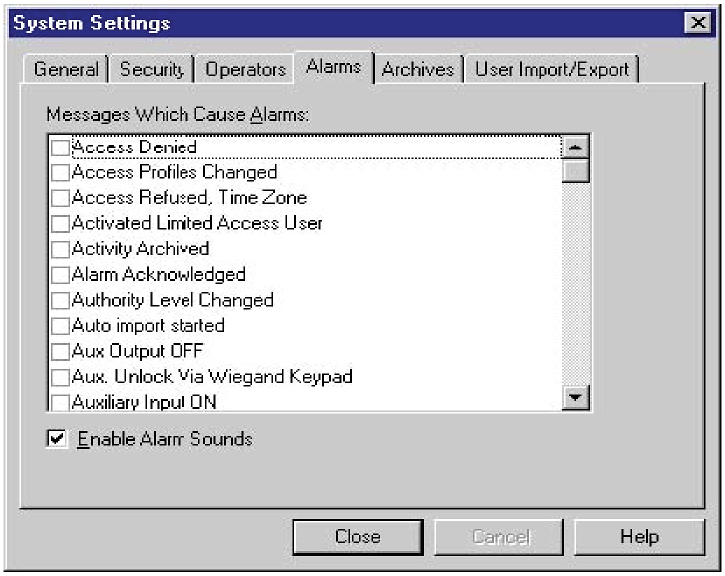
To delete an operator so that person will no longer have access to HandNet, click the operator in the list and click *Delete*. HandNet does NOT ask you to confirm this deletion, so make sure you have highlighted the right operator before you click delete.

If the operator is also a user and if you do not want the user to have access to readers anymore, you must also delete the person from the user list.

* * * * *

Which Messages Trigger Alarms

The *Alarms* tab controls which activities generate alarms in HandNet. To get to this screen, pick *Settings* from the *View* menu, and then click the *Alarms* tab.



System Settings

Messages Which Cause Alarms:

- □ Access Denied
- □ Access Profiles Changed
- □ Access Refused, Time Zone
- □ Activated Limited Access User
- □ Activity Archived
- □ Alarm Acknowledged
- □ Authority Level Changed
- □ Auto import started
- □ Aux Output OFF
- □ Aux. Unlock Via Wiegand Keypad
- □ Auxiliary Input ON

☑ Enable Alarm Sounds

Messages That Cause Alarms

Messages Which Cause Alarms: Check each message that should generate an alarm. What you check here only determines what triggers an alarm in the HandNet program; if you are connected to an auxiliary or external alarm system, actions that trigger external alarms are controlled by the *Auxiliary (AUX) Settings* (see page 48) and *Extended Setup* (see page 51) tabs in *Reader Properties*.

Alarms Sounds

Enable Alarm Sounds: If this is checked, then when an alarm situation occurs, a loud, siren-like alarm sound will begin and continue until you acknowledge the alarm. If this is not checked, when an alarm situation occurs, you will see a red flashing message at the bottom of the screen but will not hear any sound.

* * * * *

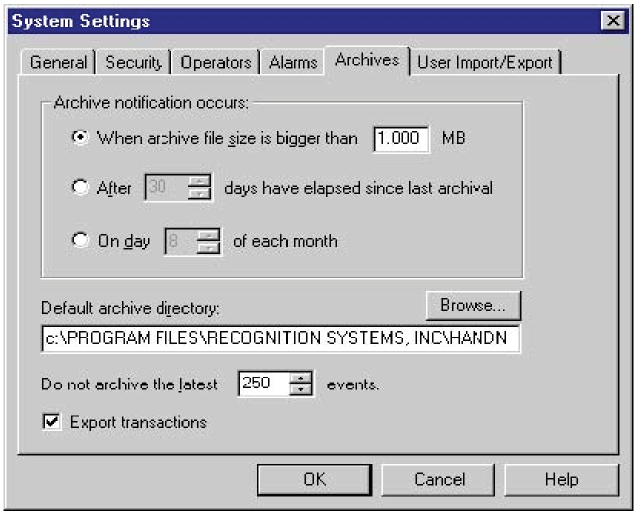
When Past Activity Gets Archived

What Archiving Is

Archiving is moving past activity from the current activity file to a separate file. This keeps the activity file smaller and faster while still keeping the information available for reports if needed. The *Archive* tab controls when HandNet reminds you to archive past activity, where it will make the archive file if you do not choose another location, and the minimum amount of activity to keep available in the current activity file.

You can make an archive at any time use *Archive* on the *File* menu; see page 113.

To get to the *Archives* tab, pick *Settings* from the *View* menu, and then click the *Archives* tab.



Archive notification occurs:

● When archive file size is bigger than 1.000 MB

○ After 30 days have elapsed since last archival

○ On day 8 of each month

Default archive directory:

c:\PROGRAM FILES\RECOGNITION SYSTEMS, INC\HANDN

Do not archive the latest 250 events.

☑ Export transactions

When HandNet Reminds You to Make and Archive

Archive Notification Occurs: This controls when HandNet reminds you to make an archive.

When archive file size is bigger than... reminds you only when there is enough activity for the archive file to reach the size you enter. How long it will take depends on the amount of activity.

After ___ days... reminds you make an archive on a regular basis regardless of the amount of activity during that period. For example, if you wanted to make an archive once a year, you could select this option and enter 365 for the number of days.

On day ___of each month reminds you make an archive once a month. If you want to include all activity from a particular month in the archive, and you also want to keep a number of days worth of recent activity available in the activity window, then you might want to do this later than the first of the month and change the *To* date to the last day of the previous month when you make the archive. For example, if you wanted to keep activity from the past week in the current activity, then you might not make your monthly archive until the 8th of the month. That way, when you have made your archive through the end of the previous month, the past week would still be in the current activity.

Default Archive Directory: This shows the drive and directory (folder) that is automatically filled in for the file location when you make the archive. This is initially set to the same folder that the HandNet program is in, but you can change this if you wish.

What NOT to Archive

Do Not Archive the Latest __ Events: This indicates how many events or activities to keep in the current activity file. You can choose from 1-500. When you make an archive, HandNet this number of the most recent events in the activity file. If you want to keep more events than this in the current activity file, you can do this when you make the archive by changing the *To* date. For example, if you always wanted to keep at least the activity for the past week, when you make the archive, you could set the *To* date a week in the past.

Exporting Activity When Archiving

Export Transactions: If you check this, then whenever you make an archive, HandNet exports all the transactions being archived to an access database file called *expactvt.mdb* (you can also export transactions with *Export Activity* on the *File* menu; see page 115). While the main HandNet database files are password protected for security reasons, this file is not. This lets you create custom activity reports using the activity from HandNet using external report generating tools. If you are only going to generate reports with *Activity Reports* on the *File* menu, you do not need to check this box; doing so would only create a file that you do not need.

* * * * *

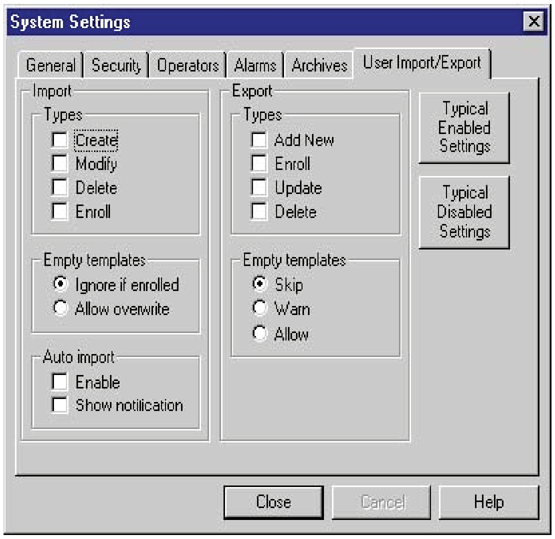
When Users Get Imported and Exported

User Import/ Export Tab

The *User Import/Export* tab is only available if you have purchased the upgrade to the full feature set of Version 2.0.

This tab controls what user information is imported and exported, and whether imports are automatic or manual. You only need this tab if you have readers connected to several different computers (each with its own copy of HandNet) and if users added to one system to be available on the others. If all of your readers are connected to a single copy of HandNet, you do not need this feature.

To get to this screen, pick *Settings* from the *View* menu, and then click the *User Import/Export* tab.



Setting Up for Common Situations

If all of your readers are connected to a single copy of HandNet: You do not need this feature. Click the *Typically Disabled Settings* button to make sure that the import and export features are both turned off.

If you have HandNet running on several computers and you want to be able to add, change or delete users from any of those computers: Click the *Typically Enabled Settings* button to turn both the import and export features on.

If you have multiple computers with HandNet but you only want users added, changed, deleted, or enrolled on this computer: Check the *Enroll, Update*, and *Delete* boxes in the *Export* column, and uncheck all of the boxes in the *Import* side of the screen. This causes HandNet to export users but prevents changes from elsewhere from being imported.

If you have multiple computers with HandNet but you only want users added, changed, deleted, or enrolled on another computer: Check the *Create, Modify, Delete* and *Enroll* boxes in the *Import* column, and uncheck all of the boxes in the *Export* side of the screen (you can also enable *Auto Import* if you wish). This keeps HandNet from creating an export file that you do not need, and enables it to import changes from another computer.

Import Settings

Types: This controls what user information HandNet will import. Make sure that you select the correct choices here before you try to import. When HandNet imports, it empties the *Import* file, discarding those user records that do not meet the conditions you have checked here.

Create: If this box is checked and HandNet finds a new user in the *Import* file, HandNet adds that user to your database. If this box is not checked, HandNet will not import any new users.

Modify: If this box is checked and HandNet finds a user in the *Import* file with the same ID number as a user that you already have, HandNet replaces the information for the user you have with the user in the *Import* file. If this box is not checked and HandNet finds a user in the *Import* file with the same ID number as a user that you already have, HandNet will not change the user that you have. If you do not have this checked, you could end up with different information for a user on different computers.

Delete: If this box is checked and HandNet finds a user marked for deletion in the *Import* file, HandNet deletes that user from your computer as well. If you do not have this checked, you could end up users that are still on your computer that are not in the copies of HandNet running on the other computers.

Enroll: If this box is checked and HandNet finds a newly enrolled user in the *Import* file, HandNet imports the user and the template (image of the user's hand). If you do not check this, you will have to enroll new users on each computer where they are imported.

Empty Templates: If HandNet finds a user that is not enrolled in the *Import* file, and it finds a user with the same ID number that is enrolled, this entry controls what HandNet will do. *Ignore if enrolled* keeps the enrolled Version of the user that you already have rather than replacing the user with the unenrolled user. *Allow overwrite* replaces the enrolled user with the unenrolled one; this means that the user will have to be enrolled again (to avoid this, on the computer that is exporting the users, do not check *Add New* on the *Export* side and make sure *Empty Templates* on the *Export* side is set to *Skip*. This way, users will not be exported until they are enrolled).

Auto Import:

Enable: If you check the *Enable* box, HandNet automatically import users whenever it finds an *import.mdb* file in the HandNet directory. If this box is not checked, then HandNet only import users when you pick *Import Users* from the *File* menu; see page 99.

Show Notification: If you check this box and the *Enable* box above is also checked, then when HandNet automatically imports users, it shows a message on the screen that lets you know that users are being imported. If you do not check this box, then HandNet just imports the users without popping a message up (either way, HandNet also records the activity in the *Activity* window). If the *Enable* box is not checked above, this entry does not apply.

Export Settings

Types: This controls what user information HandNet exports.

Add New: If this box is checked and you add a user, HandNet exports the user. Normally you do not want this box checked; you usually want HandNet to wait until the user is enrolled before exporting the user. If you have this checked, HandNet exports the unenrolled user.

Enroll: If this box is checked, then HandNet exports a new user after the user is enrolled.

Update: If this box is checked and change information for a user, HandNet exports the changed information. This can help keep user information the same on all of the computers.

Delete: If this box is checked and you delete a user, HandNet exports the fact that the user was deleted. If the other copies of HandNet are set up to import deletions, then the user will be removed from those computers as well.

Empty Templates: If you add or change a user that has not been enrolled yet, this controls whether or not HandNet will export it. Normally you only want HandNet to export users after they are enrolled, so you would leave this set to *Skip*.

"Typical" Settings

These buttons automatically check the appropriate options for two situations:

Typically Enabled Settings: This checks the appropriate boxes for a computer to be able to automatically import and export users.

Typically Disabled Settings: This unchecks all of the boxes; this is appropriate for any user who is not running HandNet on more than one computer.

See *Setting Up for Common Situations* on page 28 for more on common setups.

Getting Exported Users to Another Computer

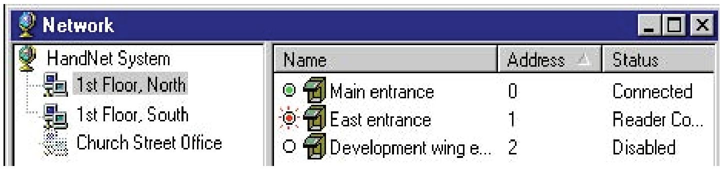
See *Importing Users from Another Copy of HandNet* on page 99 for more on how to get the exported user information to the other computer so you can import them there.

* * * * *

Setting Up Sites and Readers

Seeing Sites and Readers in the Network Window

The *Network* window lists every site and reader that you have added in HandNet. To open this window, pick *Network* from the *View* menu or press *CTRL-N*.



Network

HandNet System
- 1st Floor, North
- 1st Floor, South
- Church Street Office

Name	Address	Status
🟢 Main entrance	0	Connected
🔴 East entrance	1	Reader Co...
○ Development wing e...	2	Disabled

The left pane lists all of your sites (that is groups of connected readers). The right pane lists all of the readers in the currently selected site (to list all readers for all sites, click *HandNet System* at the top of the left pane).

Understanding the Icons to the Left of the Name

You see one of these icons to the left of each reader's name:

🟢	The green light indicates that this reader is currently connected and communicating with HandNet.
◉	The black dot indicates that HandNet communicates with this reader by modem, and HandNet is not currently connected with the reader (when HandNet connects with the readers in that site depends on what you have on the *Schedule* tab in *Site Properties*).
○	The empty circle indicates that you have not enabled this reader. This is the case when you are setting a new reader up (you enable a reader on the *General* tab in *Reader Properties*. You must also enable the site on the *General* tab in the *Site Properties*).
🔴	The red light indicates that there is a communication problem between HandNet and the reader. The reader may not be configured correctly, or there may be a problem with the way the reader is connected.

Changing How the Readers are Sorted

You can sort the list of readers using the information in any column by clicking on the column heading. For example, to sort the list alphabetically by name, click on the name heading. If you click on the same heading again, it will sort the list in reverse order; for example, using the name, it would sort from Z to A. You can also sort by address (this might be useful if you wanted to find the next available number for a new reader), by status (this could be useful to group all of the readers that are not enabled or that are having communication problems), or by site if you clicked *HandNet System* at the top of the site list to list all readers from all sites at once.

Rearranging or Resizing the Columns

To move any column, click the column heading and hold the mouse down. With the mouse held down, drag the column heading to the left or right (see the *User's window* in the online help for an example of this).

You can also change the width of a column by pointing to the edge of the column heading, holding the mouse down, and then dragging the edge of the column to the desired position. This lets you fit more columns in the window.

F5 restores all columns to the width they had when you started HandNet. If you want HandNet to save the new column widths, exit the HandNet program and come back in. HandNet then uses your changed column widths as the new standard or default.

* * * * *

Setting Up Sites, Overview

What a Site Is

In HandNet, a site refers to a group of up to thirty-two connected readers. Put another way, one reader is physically connected to the computer (by network, serial cable, or modem), and up to thirty-one additional readers can be daisy chained to that first reader; that is, a cable runs from the first reader to the second, another cable runs from the second to the third, and so on. We call this chain of readers a site. A site does not have any connection to a particular building or location; these readers could be in one building or in more than one building (if the buildings are close enough to run a cable from one to the other), and one building could have one or many sites.

You control access to each reader separately, so having readers with unrelated purposes in one site is fine; the site designation merely indicates that the readers are physically connected to each other.

There are two parts to setting up a site and readers: you must physically set the readers up and connect them to each other and to the computer, and you must add the site and readers in HandNet. This help only explains adding the site in HandNet. For help setting up and connecting the readers, see the manual that came with the readers.

Before You Enable a Site

If you have been using readers without HandNet and you want to get the users from the reader(s), follow these steps BEFORE enabling the site and reader:

1. Pick *Settings* from the *View* menu.
2. Click the *Security* tab.
3. Check the box by *Do not delete unauthorized enrollments* (see page 23 for more about what this option does; after you have gotten your users from the reader, you may want to check this box again).

If you enable both the site and the reader without changing this setting, HandNet regards all of the users in the reader as unauthorized (because they are not in HandNet yet) and deletes them from the reader. Once it deletes them, there is no way to get them back without adding and enrolling the users again.

* * * * *

Adding or Changing a Site

QUICK STEPS

Adding a Site in HandNet

1. Click *Site* on the main menu bar at the top of the screen, and then pick *Add Site*. This starts the *New Site Wizard*.
2. Complete each screen and then click the *Next* button at the bottom of the screen. The screens that you see in this process vary depending on whether the site is connected to the computer by a serial cable, through a network, or by a modem.
3. On the final screen, indicate whether to enable site
   If the site is physically set up and connected: Enable the site now. Check the *Enable Site* box and then click *Finish*.
   If the site is not physically set up yet: Enable the site later. To do this, you will open the *Network* window, double-click the site in the left pane of the window to open up the site properties, check the *Enabled* box, and then click *OK*.

Adding a Site

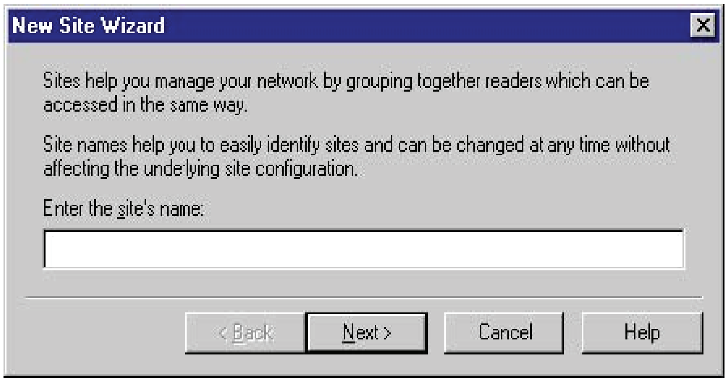
Click *Site* on the main menu bar at the top of the screen, and then pick *Add Site*. This starts the *New Site Wizard*.

Changing a Site

Click a site in the left pane of the *Network* window, pick *Properties* from the *Site* menu, and then click the tab with the information you need to change.

Name

This is the first screen in the process of adding a new site. Enter a name that identifies the site, and then click the *Next* button.



New Site Wizard

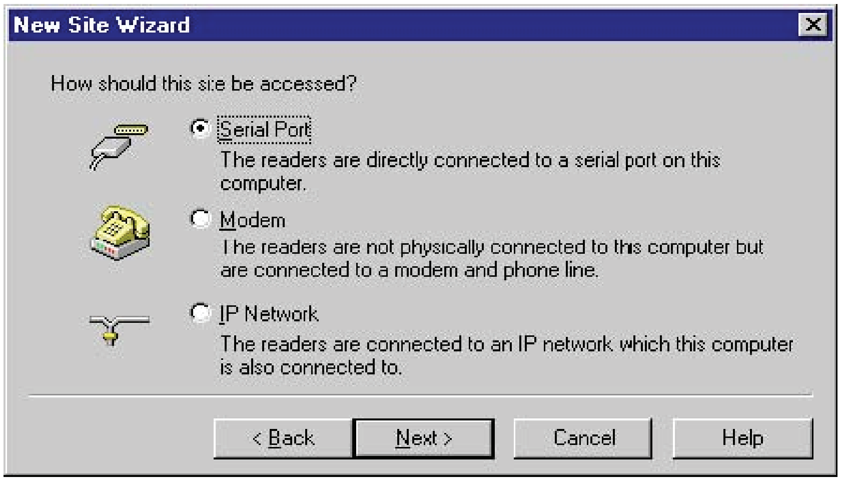
Sites help you manage your network by grouping together readers which can be accessed in the same way.

Site names help you to easily identify sites and can be changed at any time without affecting the underlying site configuration.

Enter the site's name:

Type of Connection

When adding a new site, this screen lets you indicate how HandNet will communicate with the site.



New Site Wizard

How should this site be accessed?

● Serial Port
The readers are directly connected to a serial port on this computer.

○ Modem
The readers are not physically connected to this computer but are connected to a modem and phone line.

○ IP Network
The readers are connected to an IP network which this computer is also connected to.

Serial Port: To connect to a site by running a cable from your computer to the reader, you must have a free serial port on your computer. See the HandKey manual for more on the requirements for the cable. This first reader must have an address of zero (and no other reader in the site can have an address of zero).

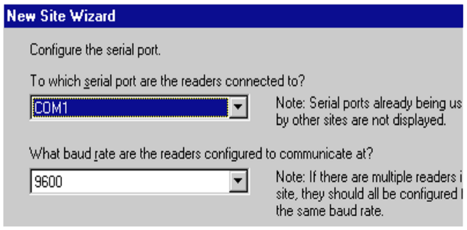
Modem: To connect to a site by modem, the first reader in the site must have a modem installed in it (contact your dealer for more information). This first reader must have an address of zero (and no other reader in the site can have an address of zero).

IP Network: To connect to a site through your network, you must have a TCP/IP network with static IP addresses. Your computer must have a network card and be connected to the network. If the network is faster than 10baseT, you must have a switching hub. The first reader in the site must have an ethernet card (contact your dealer for more information). This first reader will automatically have an address of zero (no other reader in the site can have an address of zero), and you must enter a unique IP address in the reader; see *Configuring the Physical Reader* on page 54 for more detail on this.

Serial Port Connection

To connect to a site by running a cable from your computer to the reader, you must have a free serial port on your computer; see the HandKey manual for more on the requirements for the cable. This first reader must have an address of zero (and no other reader in the site can have an address of zero).

when adding a new site



New Site Wizard

Configure the serial port.

To which serial port are the readers connected to?

COM1

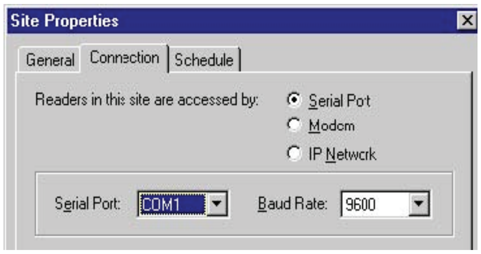
Note: Serial ports already being us
by other sites are not displayed.

What baud rate are the readers configured to communicate at?

9600

Note: If there are multiple readers i
site, they should all be configured t
the same baud rate.

when changing a site



Readers in this site are accessed by: ● Serial Port ○ Modem ○ IP Network

Serial Port: COM1

Baud Rate: 9600

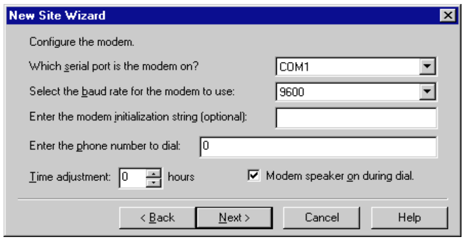
Serial Port: Click this and pick the serial port that the cable from the reader is connected to. If you pick the wrong port here, HandNet will not be able to communicate with the reader. If you have several sites, each must be connected to a different serial port. HandNet only lists ports set up on your computer that are not already used for communicating with another site. If you click this and get a blank list, all of the serial ports are already used. Contact the person who services your computer hardware if you need to add additional serial ports.

Baud Rate: Click this and pick the baud rate, we recommend 9600. While 19200 should theoretically be faster, because of the way the reader sends information, this does not result in any real gain. The speed here must match the speed set in the reader; see *Configuring the Physical Reader* on page 54 for more detail on how to change the baud rate in the reader.

Modem Connection

To connect to a site by modem, the first reader in the site must have a modem installed in it (contact your dealer for more information). This first reader must have an address of zero (and no other reader in the site can have an address of zero).

when adding a new site



New Site Wizard

Configure the modem.

Which serial port is the modem on? COM1

Select the baud rate for the modem to use: 9600

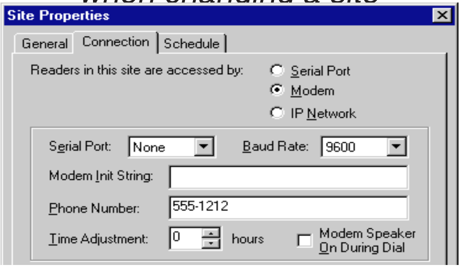
Enter the modem initialization string (optional):

Enter the phone number to dial: 0

Time adjustment: 0 hours

☑ Modem speaker on during dial.

when changing a site



Site Properties

Readers in this site are accessed by: ○ Serial Port ● Modem ○ IP Network

Serial Port: None

Baud Rate: 9600

Modem Init String:

Phone Number: 555-1212

Time Adjustment: 0 hours

□ Modem Speaker On During Dial

Serial Port: If you have an external modem, click this and pick the serial port your modem is connected to; this is usually (but not always) *COM1* or *COM2*. If you have an internal modem, it is usually connected to *COM3* or *COM4*. HandNet only lists ports that are set up on your computer and that are not already used for communicating with another site.

Baud Rate: Choose 9600 if you are connecting to a HandKey II or HandKey CR; choose 2400 if connecting to a HandKey.

Modem Init String: If you need HandNet to send any commands to the modem before dialing, enter the appropriate codes here. The modem must be set up for no data compression, no error correction, an appropriate baud rate, and auto answer. The manual that came with your modem explains the various commands that work with your modem. An inappropriate init string can prevent the modem from connecting. Try connecting without any init string to see if you can communicate; you modem may be automatically set up correctly. If you have problems getting your modem to connect and communicate with the site, here are init strings that have worked for some modems:

Typical Modem Strings		AT&F&C1&D2X1V1E0 AT&C1&D2X1V1E0 AT&C1X1VE0
Rockwell Chip Set Modems		AT&D2E0&Q0N0S37=5
US Robotics Sportster 14.4 F/M		AT&F0 AT&FX0&C1&D2&H0&N6&K0S0=0
Everex 2400E		AT&F
Hayes Accura 14,400	1200 Baud	AT&F&C1&D2&K0S0=0S37=5
	2400 Baud	AT&F&C1&D2&K0S0=0S37=6
Hayes Optima 14,400	1200 Baud	AT&F&C1&D2&K0S0=0S37=5
	2400 Baud	AT&F&C1&D2&K0S0=0S37=6
Practical Peripherals PM144MTII	1200 Baud	AT&F&C1&D2&K0S0=0S37=5
	2400 Baud	AT&F&C1&D2&K0S0=0S37=6
Practical Peripherals 14.4 FXSA	1200 Baud	AT&D2E0&Q0N0S37=5
	2400 Baud	AT&D2E0&Q0N0S37=6

Cardinal 33.6 V.34/V.FC	1200 Baud	ATE0S37=5&C1&D2&K0
	2400 Baud	ATE0S37=6&C1&D2&K0
Multitech Model MT1932ZPX		AT&F&C1&D2X1V1E0&E0&E3&E7&E8&E10&E12&E14$MB1200$SB1200
Zoom Model cc4336	2400 Baud	AT&Q0&K0+MS=2

Phone Number: If you have to dial some digit to get an outside line, enter this digit followed by a comma before the phone number. If the number is a long distance number, enter the one and the area code as appropriate. For example, if you had to dial a nine for an outside line, and the number was long distance and required one and an area code, you would enter the number like this:

9, 1-802-555-1212

You do not have to enter the dashes; they do not make a difference. You could equally well enter the number above like this:

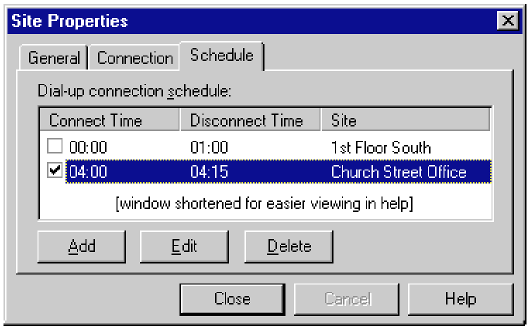
9,18025551212

Time Adjustment: If this site is in a different time zone, enter the number of hours the time difference is. For example, if you are in New York and were setting up a connection with a site in California, you would enter *-3* since in California it is three hours earlier than in New York. If you are in California and setting up a connection with a site in New York, you would enter *3* since it is three hours later in New York. Only do this if you want all times reflecting the time zone you are currently in.

Modem Speaker On During Dial: If you check this box, when HandNet connects to this site, it turns the modem speaker on so you can hear it dialing and connecting. If there is a problem connecting, turning the modem speaker on can help identify where the problem is. Unless you are having a problem connecting, we do not recommend checking this box.

Scheduling a Connection Time

If you are connecting to sites by modem, this screen shows when HandNet is scheduled to connect with each site. You can only change the connection time for the current site (this screen does not apply if you are not communicating by modem; if you connect by serial port or through a network, HandNet stays connected to the site continuously and does not need a scheduled connection time).



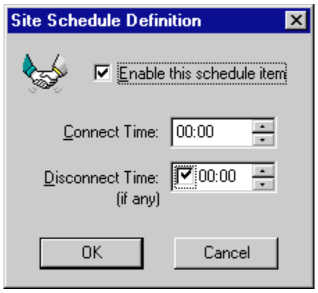
Dial-up connection schedule:

Connect Time	Disconnect Time	Site
□ 00:00	01:00	1st Floor South
☑ 04:00	04:15	Church Street Office

[window shortened for easier viewing in help]

Adding a New Scheduled Connection Time

When you choose to add a new schedule time, you see this screen:



☑ Enable this schedule item

Connect Time: 00:00

Disconnect Time: (if any) ☑ 00:00

Enable this schedule item: This box must be checked for HandNet to make the connection. Only uncheck this box if the modem is not set up yet at the site and you do not want HandNet to try to communicate with the site.

Connect Time: Enter the time that you want HandNet to try to connect. This must be at least one minute later than the disconnect time for the previous connection. For example, if another connection is scheduled to end at 5:00, the new connection can be scheduled for 5:01, but not for 5:00. If the phone lines are busy when HandNet tries to connect, it will keep trying until it makes a connection (or reaches the *Disconnect Time*).

Disconnect Time: If you uncheck this box, HandNet will stay connected to this site continuously. Since the modem will be continuously connected to that site, you will not be able to schedule a connection to any other site; if you need more than one connection, this must be checked. When you enter a disconnect time, it must be after the start time. For example, you cannot schedule a connection to both begin and end at 5:00; if the connection begins at 5:00, the disconnect time must be 5:01 or later.

When you enter the disconnect time, allow enough time for HandNet to download all of the potential activity in the reader. The reader can send about 100 events a minute. This means that if the reader were full (with 5000 events), it could take up to an hour to get all of the activity. The amount of activity you have each day and the number of times you connect to reader during the day determine how long your connection must be.

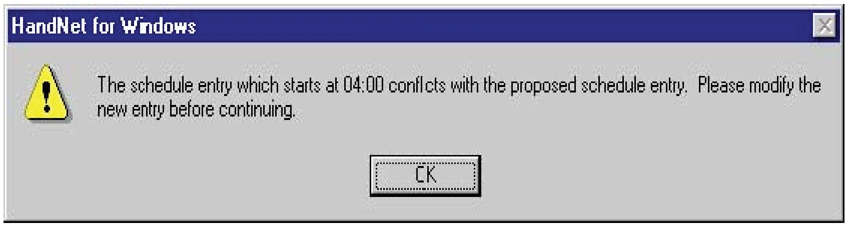
When HandNet reaches the disconnect time, it disconnects even if there is still activity that the reader needs to send. When HandNet disconnects, if the reader is not done sending activity, a few activities would be lost. If there is regularly more activity at the reader than the connection time allows for, the reader's memory would eventually fill up, at which point additional activity would also cause activity to be lost. To avoid this, make sure the time between the *Connect Time* and the *Disconnect Time* is long enough to get all of the activity.

Changing or Deleting a Scheduled Communication Time

Even though HandNet lets you see the scheduled connection times for all sites, HandNet only lets you change a scheduled time for the site with which you are currently working. To change a scheduled time for a different site, you must go to the properties for that site, select the scheduled time there, and then click the *Edit* button.

If You Get a Message that the Time Conflicts

If the time that you enter conflicts with the time that HandNet is already scheduled to communicate with a different site, you see a message like this:


HandNet for Windows

The schedule entry which starts at 04:00 conflcts with the proposed schedule entry. Please modify the new entry before continuing.

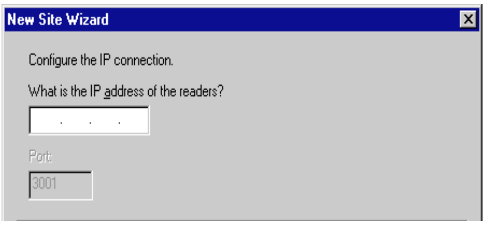
Make sure that each other scheduled connection has a disconnect time. If you schedule a connection with no end time, HandNet would never disconnect from that site, so it would not be possible to schedule another connection. If you want to have more than one scheduled connection, each connection must have a disconnect time.

Also make sure the connect time is at least one minute later than the disconnect time for the previous connection. For example, if another connection is scheduled to end at 5:00, the new connection can be scheduled for 5:01, but not for 5:00.

IP Address

You see this screen if you indicate that HandNet will communicate with this site through a network.

when adding a new site

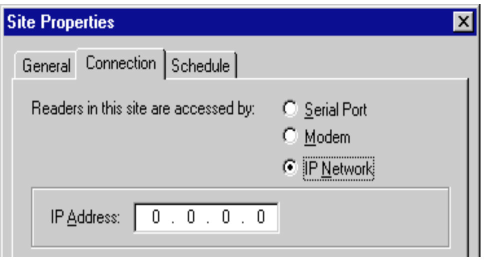

New Site Wizard

Configure the IP connection.

What is the IP address of the readers? . . .

Port: 3001

when changing a site


Site Properties

Readers in this site are accessed by: ○ Serial Port ○ Modem ● IP Network

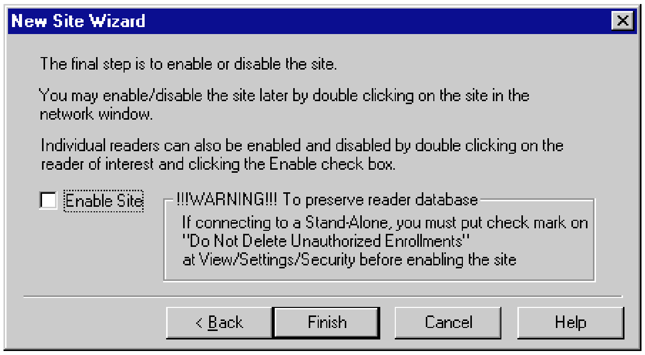
IP Address: 0 . 0 . 0 . 0

IP address: Each site must have a unique IP address. Ask your network administrator for an appropriate address. The address you enter here must match the address you enter in the reader; see *Configuring the Physical Reader* on page 54 for more on how to change the address in the reader.

Port: This entry no longer applies; it is always grayed out.

Enabling the Site

This is the final screen that you see in the *New Site Wizard* (when you go back to *Site Properties* to change this site, this is on the *General* tab).



New Site Wizard

The final step is to enable or disable the site.

You may enable/disable the site later by double clicking on the site in the network window.

Individual readers can also be enabled and disabled by double clicking on the reader of interest and clicking the Enable check box.

□ Enable Site

!!!WARNING!!! To preserve reader database

If connecting to a Stand-Alone, you must put check mark on "Do Not Delete Unauthorized Enrollments" at View/Settings/Security before enabling the site

Enable Site: You must enable the site before HandNet can communicate with the readers in it, but you might not want to enable it yet. Please read the sections below if you are not sure.

If the site is not physically set up yet

If the site is not physically set up yet, do not enable it; you do not want HandNet to repeatedly try to communicate with something that is not there. This would slow the system down.

If you have been using readers independently of HandNet and you need to get users from the readers

If you have been using readers independently of HandNet and if you want to get the users from the readers into HandNet, **you also do NOT want to enable the site until you have set HandNet to accept users from the reader that are not in HandNet.** To do this:

1. Click *Finish* without checking the *Enable Site* box.
2. Pick *Settings* from the *View* menu.
3. Click the *Security* tab.
4. Check the box by *Do not delete unauthorized enrollments* (see page 23 for more about what this option does; after you have gotten users from the reader, you may want to check this box again).

If you enable both the site and the reader without changing this setting, HandNet will regard all of the users in the reader as unauthorized (because they are not in HandNet yet) and it will delete them from the reader. Once it deletes them, there is no way to get them back without adding and enrolling the users again.

If you are ready to connect

If the site is physically set up and you do not need to get users from the readers (or if you have already changed the setting above), then you can enable the site now. Check the *Enable Site* box and then click *Finish*.

To Enable the Site Later

After you leave this screen, you can enable the site by doing this:

1. Open the *Network* window.
2. Double-click the site in the left pane of the window to open up the site properties (or click once and pick *Properties* from the *Site* menu).
3. Check the *Enabled* box and then click *OK*.

* * * * *

Setting Up Readers, Overview

There are two parts to setting up readers: 1) physically setting the readers up and connecting them to each other and to the computer; and 2) adding the site and readers in HandNet. This manual only explains adding the site and readers in HandNet. For help setting up and wiring readers, see the manual that came with the readers.

Before You Enable the Reader

Before you add readers, you must set up the site they are connected to; see page 34.

If you have been using readers without HandNet and you want to get users from the reader(s), follow these steps BEFORE enabling the site and reader:

1. Pick *Settings* from the *View* menu.
2. Click the *Security* tab.
3. Check the box by *Do not delete unauthorized enrollments* (see page 23 for more about what this option does; after you have gotten your users from the reader, you may want to check this box again).

If you enable the site and the reader without changing this setting, HandNet regards all users in the reader as unauthorized (because they are not in HandNet yet) and deletes them. Once it deletes them, there is no way to get them back without adding and enrolling the users again.

Selecting Readers

Most options on the *Reader* menu are disabled until you select a reader.

To select a single reader: Click that reader in the list.

To select multiple readers that are together on the list: Click the first reader in the group, hold the *SHIFT* key down, and click the last reader that you want to select.

To select multiple readers that are not together on the list: Click the first reader to select, hold the *CTRL* key down, and click each other reader that you want to select.

Renaming a Reader

You might rename a reader if you discovered that the original name was not clear or if you changed the purpose of the areas the reader gave access to. Renaming the reader does not change any of its properties and does not require you to set anything up again; it only changes the name that appears in the lists on the screen and in reports that you generate.

To rename a reader:

1. If the *Network* window is not open, pick *Network* from the *View* menu (or press *CTRL-N*).
2. Click the reader in the right pane of the *Network* window.
3. Pick *Rename* from the *Reader* menu (you could also right click and pick *Rename*, or you could double-click the reader and change the name in the *Reader Properties*).

* * * * *

Setting Up a New Reader

QUICK STEPS

Adding a New Reader

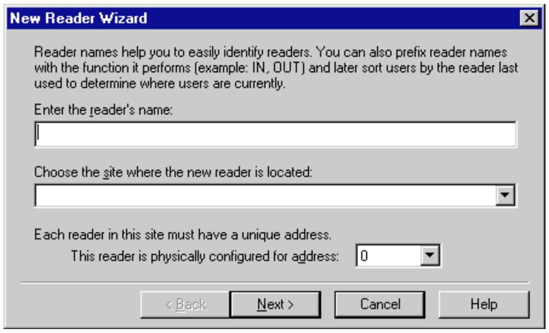
1. Click *Reader* in the main menu bar at the top of the screen, and then pick *Add New*. This starts the *New Reader Wizard*.
2. On the second screen of the *New Reader Wizard*, indicate whether you want to set the reader up by going through each configuration screen, or whether you want to copy the settings from another reader. Copy the settings from another if the settings are identical or even similar to the other reader (if you copy settings, you can use *Properties* on the *Reader* menu to make changes).
3. If you are setting up the reader by going through each configuration screen, see the different tabs in the *Reader Properties* for help with particular entries. Click the *Next* button at the bottom of the screen to continue with the next screen.
4. Make sure that the address in the reader matches the address you entered on the first reader properties screen; see *Configuring the Reader* for more details.
5. Once the reader is physically connected and set up correctly, enable the reader. To do this, open the *Network* window, double-click the site in the right pane of the window to open the *Reader Properties*, check the *Enabled* box, and then click *OK*.

Getting Started

When you pick *Add New...* from the Reader menu, HandNet starts the *New Reader Wizard*. This takes you through the process of adding the reader.

Name and Address Screen

This is the first screen that you see when adding a new reader:



Reader names help you to easily identify readers. You can also prefix reader names with the function it performs (example: IN, OUT) and later sort users by the reader last used to determine where users are currently.

Enter the reader's name:

Choose the site where the new reader is located:

Each reader in this site must have a unique address.

This reader is physically configured for address: 0

Enter the reader's name: Enter any name that clearly describes the reader's function and location. This name is used in the *Activity* window and in activity reports to identify where activity took place.

Choose the site where the new reader is located: Click this to pick the site (group of readers) that this reader is connected to. You must set the site up before you can add the reader.

This reader is physically configured for address: HandNet automatically fills in the first available address that has not been used yet in this site. For example, if you already have readers 0, 1, and 2 in this site, HandNet automatically fills in an address of 3. You can change this if you wish. The first reader in each site my be reader 0; other readers in the site can use any number up to 254. Readers do not need to be numbered sequentially. For example, your readers could be numbered 0, 1, 2, 3... or they could be numbered 0, 100, 110, 137... Within a site, each reader must have a

unique number. For example, you cannot have two readers in the same site that both use the address of 1. However, you can reuse numbers in different sites. For example, if you have twenty sites, you could have a reader with an address of 1 in each of them.

Make sure the address matches the address in the reader

The number here must match the address entered in the reader; see *Configuring the Physical Reader* on page 54 for more on how to set the address up in the reader.

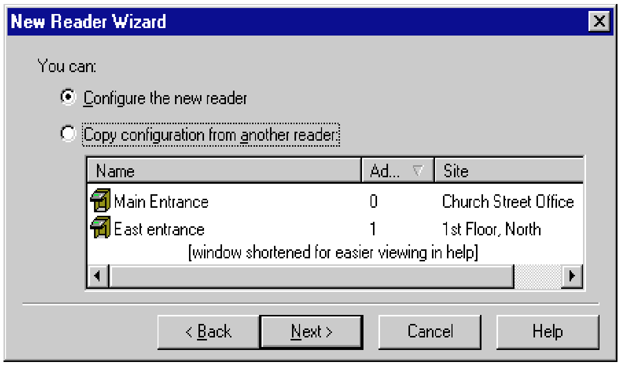
Never put more than 32 readers in a site

Even though HandNet allows numbers from 0 to 254, you should never have more than thirty-two readers in a site. While it is sometimes technically possible to connect more than thirty-two readers, not all readers support this, and even for readers that do, connecting more than this causes unacceptably slow response times from readers. The software was not designed to handle more than this, and we cannot guarantee results with more than thirty-two readers. If you feel that more than thirty-two readers in a single site is essential for you, please contact us to discuss your situation first; in nearly all cases, the preferable (and sometimes only) solution is to set up additional site(s).

Click *Next* to go on to the next screen. This button is disabled until you have filled in all of the entries on this screen.

Configuration

This is the second screen that you see in the process of adding a new reader. This screen lets you choose whether you want to set the reader up by going through each configuration screen in the reader properties, or whether you want to copy the settings from another reader. Copy the settings from another reader if the settings are identical or even similar to the other reader. If you copy the settings from another reader, and you want to make the settings slightly different, you can use *Properties* on the *Reader* menu to make changes; see page 45.



New Reader Wizard

You can:

● Configure the new reader

○ Copy configuration from another reader:

Name	Ad...	Site
Main Entrance	0	Church Street Office
East entrance	1	1st Floor, North

[window shortened for easier viewing in help]

Configure the new reader: This lets you go through each of the *Reader Properties* screens so you can choose the appropriate settings on each. The *Reader Properties* screens are explained starting on page 45. You would choose this for the first reader you add. You would also choose this if you wanted very different settings from the other readers. For example, if other readers are set to trigger an auxiliary alarm after certain events and you do not want this reader to trigger an alarm, or if other readers have an automatic unlock time and you do not want that for this reader, then you might want to use this option.

Copy the configuration from another reader: If another reader has the same or nearly the same settings as you want for this reader, copying settings from the other reader is faster. It also protects you from accidentally

making the settings slightly different if you want readers configured exactly the same way.

If you choose this option, click the reader in the list to copy the settings from and then click the *Finish* button (the *Next* button changes to a *Finish* button when you choose this option).

When you copy the configuration from another reader, HandNet does NOT enable the reader. You must go to the *General* tab in the *Reader Properties* to enable the reader before HandNet will communicate with it; see page 45.

If you copy the settings from another reader, and you want to make the settings slightly different, you can use *Properties* on the *Reader* menu to make changes; see page 45.

* * * * *

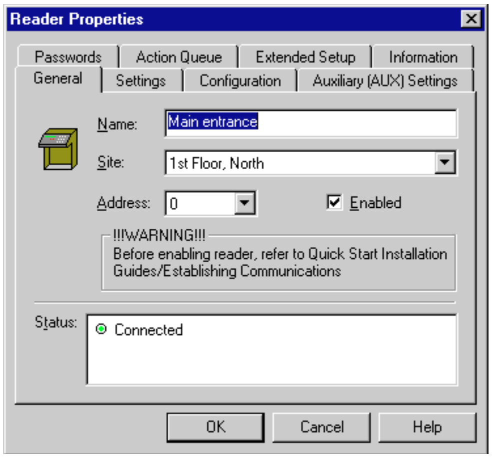
Changing Reader Settings with Reader Properties

Getting to the Reader Settings

Click a reader in the right pane of the *Network* window, and pick *Properties* from the *Reader* menu (or just double-click the reader in the *Network* window). You are initially on the *General* tab; click any other tab to jump to the corresponding screen.

General

This screen contains the reader's name and address, the site the reader is a part of, and whether or not the reader is currently enabled and connected.



Name: Main entrance

Site: 1st Floor, North

Address: 0

☑ Enabled

!!!WARNING!!!
Before enabling reader, refer to Quick Start Installation Guides/Establishing Communications

Status: ● Connected

Name: The name is to help you identify the reader. Changing the name does not affect any of the reader's other settings or connection. If you change the name of the reader, the new name is used in activity reports for activity at that reader, even if the activity occurred before the name change.

Site: This is the site (that is, the group of up to thirty-two readers) that this reader is associated with.

Address: The number here can be from 0 to 254. If the site is connected by IP Network, the first reader in the site (the one with the ethernet card) must be reader 0. Other readers can use any number and do not need to be numbered sequentially. For example, your readers could be numbered 0, 1, 2, 3... or they could be numbered 0, 100, 110, 137.... You can use the same reader number in more than one site. For example, if you have twenty sites, you could have a *Reader One* in each of them.

The number here must match the address entered in the reader; see *Configuring the Physical Reader* on page 54 for more on how to set the address up in the reader.

Even though HandNet allows numbers from 0 to 254, you should never have more than thirty-two readers in a site. While it is sometimes technically possible to connect more than thirty-two readers, not all readers support this, and even for readers that do, connecting more than this causes unacceptably slow response times from readers. The software was not designed to handle more than this, and we cannot guarantee results with more than thirty-two readers. If you feel that more than thirty-two readers in a single site is essential for you, please contact us to discuss your situation first; in nearly all cases, the preferable (and sometimes only) solution is to set up additional site(s).

Enabled: This should be checked once reader setup is done and users should have access through the reader. Leave this unchecked if you do not want HandNet to try to communicate with the reader at this point.

If you have been using readers without HandNet and you want to get the users from the reader, follow these steps BEFORE enabling the site and reader:

1. Pick *Settings* from the *View* menu.

2. Click the *Security* tab.

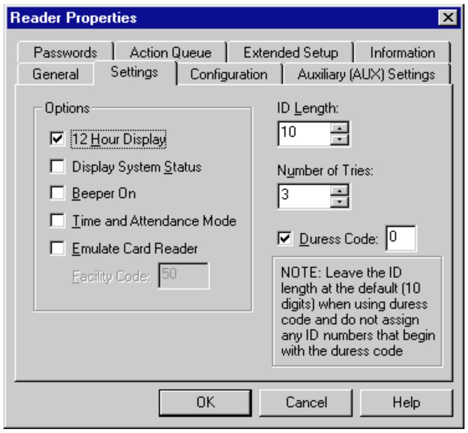
3. Check the box by *Do not delete unauthorized enrollments* (see page 23 for more about what this option does. After you have gotten your users from the reader, you may want to check this box again).

If you enable both the site and the reader without changing this setting, HandNet will regard all of the users in the reader as unauthorized (because they are not in HandNet yet) and it will delete them from the reader. Once it deletes them, there is no way to get them back without adding and enrolling the users again.

Status: This indicates whether the reader is connected.

Settings

This screen controls the reader's display and other factors that affect what happens when the user enter an ID number at the reader.



☑ 12 Hour Display

□ Display System Status

□ Beeper On

□ Time and Attendance Mode

□ Emulate Card Reader

Facility Code: 50

ID Length: 10

Number of Tries: 3

☑ Duress Code: 0

NOTE: Leave the ID length at the default (10 digits) when using duress code and do not assign any ID numbers that begin with the duress code

12 Hour Display: If you check this, the reader displays times after noon using the numbers one through twelve; if it is not checked, it uses twenty-four hour time. For example, if this is checked 5:00 PM displays on the reader as 5:00; if this is not checked, 5:00 PM displays as 17:00.

Display System Status: Do not check this option unless asked to by one of our support staff. This displays technical information on the reader display about the status of different aspects of the reader. It is not relevant to normal use of the reader.

Beeper On: If this is checked, the reader beeps each time you press a button on it; if this is not checked, the reader does not beep. In a high security setting, you might want the beeps off to make it harder for a casual observer to figure out how many digits are in the ID number. In other contexts, your choice here depends only on your preference; some people like the beeps since it lets them know that they have not missed the button; others prefer not to hear them.

Time and Attendance Mode: Do not check this option. If you check this, the reader asks users for additional information related to time and attendance tracking (whether one is coming in or out or leaving for a job, the job number you are working on, etc.). However, HandNet is currently NOT able to store or track this information.

Emulate Card Reader: If you want the readers to send output directly to a lock and unlock it, leave this unchecked. If you have an access control panel and want the reader to send information formatted like card output to that control panel, check this box.

Facility Code: This only applies if you are emulating a card reader.

ID Length: If all of your user IDs are the same length, you can enter the number of digits here so that users do not have to press *ENTER* or *YES* after typing the ID at the reader. For example, if all of your IDs are four digits long, then you could enter *4* here. Then, at the reader, once the user had entered four digits, the reader would ask the user to place the hand (assuming the ID was valid). Without this, the user would have to type the four digits and then press the *ENTER* or *YES* button on the reader. However, if you use a duress code (see below), do not enter a number here. This is because the duress code adds a digit; if your IDs are four digits, the user will have to be able to enter five digits if they ever need the duress code. If you are using a duress code, leave this set to ten.

Number of Tries: If a user enters a valid ID number but the users hand does not match the image stored, the reader does not give access. This entry controls how many times the user can try to get access before the reader will block the user's ID and not allow further tries. This prevents someone from making repeated tries to gain access with someone else's ID number. Normally three is a good setting here; it allows for two retries if the user did not place the hand correctly, but limits the number of attempts someone can make.

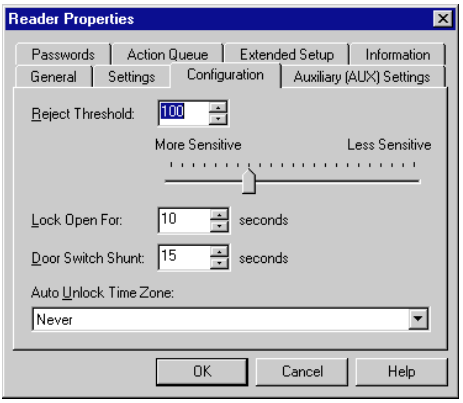
If the user does not gain access after the number of tries here, the reader no longer accepts that user's ID until another user successfully gains access through that reader.

Duress Code: A duress code is single digit that users can enter before the ID number to indicate that they are in danger or that someone else is forcing them to open the door. For example, suppose that you set zero up as a duress code. If a user is being forced to let someone into the building, instead of entering the regular ID of *1234*, the user would enter *01234*. The system would still grant access as it would for the normal ID, but it would also trigger an alarm. This could be merely the alarm in the HandNet program, or, it could also trigger an external alarm through the *Auxiliary Settings*; see page 49.

Zero (0) is often a good digit for the duress code because you cannot begin a user ID with zero if you enroll users from the command menus on the reader (while HandNet distinguishes between *5* and *0005*, the process of adding a user from the reader command menu does not. This means that if you create a user with an ID of *0005* in HandNet and try to enroll that user with the command menus on the reader, when you type *0005*, the reader would think you were enrolling User Five. This would not correspond with *0005* in HandNet).

Configuration

This screen controls how closely the typical user's hand must match the image that is stored, how long the door can stay open, and when (if ever) the door should be automatically unlocked.



Reader Properties

Reject Threshold: 100

Lock Open For: 10 seconds

Door Switch Shunt: 15 seconds

Auto Unlock Time Zone: Never

Reject threshold: The lower this number is, the more closely the user's hand must match the image or template of the hand stored in HandNet. Thirty

(the lowest possible number) requires the hand shape and position to match very closely; two hundred fifty (the highest possible number) will grant access if the hand match is close but not exactly the same. One hundred is good for most contexts; enter a lower number if you have an especially high security situation. You can either enter a number or drag the pointer.

If particular users have trouble placing their hands consistently because of arthritis or some other hand condition, you can override the reader's setting for an individual user on the *Security* tab in the *User Properties*; see page 93.

Lock Open For: This is the number of seconds the door stays unlocked once a user's hand is recognized.

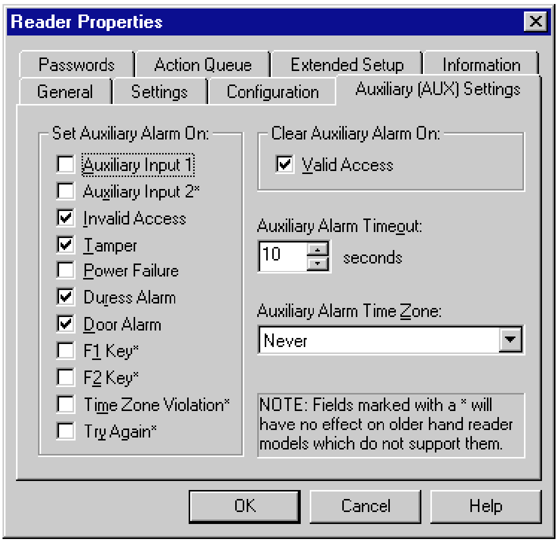
Door Switch Shunt: This is the number of seconds the door can be open before potentially triggering an alarm. The *Alarms* tab in *System Properties* (see page 25) and the *Door Alarm* on the *Auxiliary (AUX) Settings* (see below) and *Extended Settings* (see page 51) tabs control whether this causes an alarm.

Auto Unlock Time Zone: This controls when (if ever) the door is automatically unlocked. For example, you might want a door unlocked during normal business hours, and you might want the door to require hand recognition for access during other hours. You would set up a time zone that reflected the hours you wanted the door open and then pick that time zone here (see page 61 for more on setting up time zones). When you reached the start time, HandNet would unlock the door, and when you reached the end of the time zone, HandNet would lock it again. Leave this set to *Never* if you always want the door locked.

Auxiliary (AUX) Settings

Readers can communicate with auxiliary devices like alarms, lights, or security cameras. HandKey readers can communicate with one auxiliary device; this screen controls when and under what conditions output is sent to that device. HandKey II and HandKey CR readers can communicate with up to three auxiliary devices; this screen controls the output to the first; the *Extended Setup* tab (see page 51) controls output to the second and third.

To get to this screen, click a reader in the right pane of the *Network* window, pick *Properties* from the *Reader* menu, and then click the *Auxiliary (AUX) Settings* tab.



Set Auxiliary Alarm On:
- ☐ Auxiliary Input 1
- ☐ Auxiliary Input 2*
- ☑ Invalid Access
- ☑ Tamper
- ☐ Power Failure
- ☑ Duress Alarm
- ☑ Door Alarm
- ☐ F1 Key*
- ☐ F2 Key*
- ☐ Time Zone Violation*
- ☐ Try Again*

Clear Auxiliary Alarm On:
- ☑ Valid Access

Auxiliary Alarm Timeout: 10 seconds

Auxiliary Alarm Time Zone: Never

NOTE: Fields marked with a * will have no effect on older hand reader models which do not support them.

Set Auxiliary Alarm On: Even though this says *Set Auxiliary Alarm On*, the device does not have to be an alarm; this can trigger any type of auxiliary device. If a condition occurs and the corresponding box is checked, HandNet turns auxiliary output on if it is during the time zone selected at the bottom of the column on the right.

Auxiliary Input 1: This occurs if the reader receives input from an auxiliary input device. This is irrelevant if you do not have an auxiliary input device connected to the reader.

Auxiliary Input 2: This occurs if the reader receives input from the second auxiliary input device (HandKey II and HandKey CR support two auxiliary input devices; HandKey readers support just one). This is irrelevant if you do not have a second auxiliary input device connected to the reader.

Invalid Access: This occurs if someone repeatedly entered a valid ID at a reader, and each time the reader does NOT recognize the user's hand (at the reader, the user would see the message *ID Refused*, and the *Activity* window would show the message *Access Denied*). The number of times that a user can try before this occurs depends on the *Number of Tries* entry on the *Settings* tab in the *Reader Properties*; see page 47. If this occurs, someone might be trying to gain access with someone else's ID.

Tamper: This occurs if someone has shaken the reader roughly or opened the reader. Unless someone was servicing the reader, this message generally warrants further investigation.

Power Failure: This occurs if the reader loses power from an external source. While this could just be due to an ordinary power failure, sometimes someone trying to gain invalid access will cut power in an attempt to disable alarm systems.

Duress Alarm: This occurs if a user entered the duress code. This code indicates that the user is in trouble or that someone is forcing the user to give him/her access; see page 47 for more on setting up a duress code.

Door Alarm: This occurs if the door connected to the reader is forced open, or if the door is kept open for longer than allowed based on the *Door Switch Shunt Time* on the *Configuration* tab in the *Reader Properties*; see page 48.

F1 / F2 Key: This occurs if the corresponding key was pressed on the reader keypad (HandKey II and HandKey CR have F1 and F2 keys to the right of the number keys. The HandKey reader does not have these buttons, what you check here does not make any difference for that type of reader).

Time Zone Violation: This occurs if a user enters a valid ID at a reader, but the user is not authorized to have access during the hours or days of the week based on the time zone associated with the reader in the access profile.

Try Again: This occurs if a user enters a valid ID at a reader, but the reader does not recognize the user's hand (this situation causes the *Identity Unknown* message in the *Activity* window). This could be just the result of incorrect hand placement (if this happens repeatedly, HandNet generates the *Invalid Access* condition above.)

Clear Auxiliary Alarm On: If the auxiliary device is turned on, this controls whether it will be shut off when someone gains valid access (that is, enters a valid ID number and has his/her hand recognized). If this is checked, the alarm (or other auxiliary output) is turned off when a valid user gains access through that reader; if this is not checked, the output continues until the time entered in the following entry ends or until you go to the *Reader* menu, highlight *Auxiliary Output*, and pick *Off*; see page 129.

Auxiliary Alarm Timeout: This indicates the number of seconds that the auxiliary device should be on for.

Auxiliary Alarm Time Zone: This controls when HandNet should turn output to an auxiliary device on. For example, if the auxiliary device is a set of floodlights, it would only help to turn the lights on if the condition occurred at night. To do this, you would create a time zone for night hours, and then assign that time zone here (see page 61 for more on setting up time zones). If this says *Always*, HandNet turns output on for the auxiliary device whenever the checked condition(s) occur.

Passwords

This screen controls the passwords needed to access the menus available through entered command mode on the reader. Generally the passwords below are adequate since a user must be set up with the appropriate authority level on the *Security* tab in *User Properties* (see page 92), and the user must know how to get to these menus in the reader before the passwords below would do any good.

What is available on the different reader menus

1. **Service:** This lets you recalibrate the reader and change the reader's status display.

2. **Setup:** This lets you control reader setup issues including how the reader is connected to your computer network, what language the reader displays in, the date/time, etc.

3. **Management:** This lets you list users.

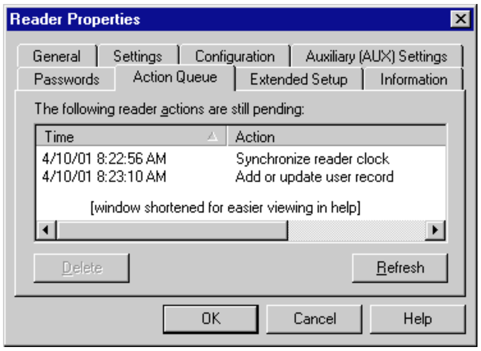
4. **Enrollment:** This lets you add or remove users.

5. **Security:** This lets you control the passwords for the reader menus, change time zones, enroll users who do not need hand access, etc.

For more detail, see the reader manual.

Action Queue

If the reader is not connected to HandNet continuously (typically only the case if HandNet communicates with the reader by modem), this screen lists changes that have not been sent to the reader yet. These actions will be sent to the reader the next time the modem connects.



The following reader actions are still pending:

Time	Action
4/10/01 8:22:56 AM	Synchronize reader clock
4/10/01 8:23:10 AM	Add or update user record

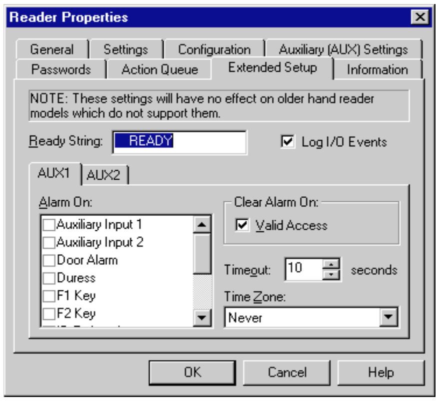
[window shortened for easier viewing in help]

To get to this screen, click a reader in the right pane of the *Network* window, pick *Properties* from the *Reader* menu, and click the *Action Queue* tab.

If there is been a change that requires that certain actions NOT be sent to the reader, you can select those actions in the list and click *Delete*.

Extended Setup

Readers can turn auxiliary devices like alarms, lights, or security cameras on or off. HandKey II and HandKey CR readers can communicate with up to three auxiliary devices; this screen controls the output to the second and third auxiliary devices; the *Auxiliary (AUX) Settings* tab controls output to the first; see page 48. If you have a HandKey (instead of a HandKey II or HandKey CR), this screen does not apply since the HandKey only supports one auxiliary device.



NOTE: These settings will have no effect on older hand reader models which do not support them.

Ready String: READY ☑ Log I/O Events

Alarm On:
□ Auxiliary Input 1
□ Auxiliary Input 2
□ Door Alarm
□ Duress
□ F1 Key
□ F2 Key

Clear Alarm On:
☑ Valid Access

Timeout: 10 seconds

Time Zone: Never

Ready String: This is the text that appears in the reader display when the reader is ready and waiting for the user to enter an ID. For example, if you want the readers to read *Enter ID* instead of *Ready* you could change the text here. You can enter up to fourteen characters. If you want this text centered in the reader's display, add spaces before the text if needed.

Log I/O Events: This entry only applies to the HandPunch. We do not recommend connecting a HandPunch to HandNet. The HandPunch is used for tracking time and attendance, which is not what HandNet is for. If you do connect a HandPunch and this box is checked, the reader records all activity (including invalid access attempts, door alarms, accessing command mode on the reader, etc.); if you do not have this checked, the HandPunch only records successful accesses. If you have an ID3D HandKey, HandKey II, or HandKey CR, the reader records all activity regardless of whether this is checked or not.

AUX1/AUX2

Aux1 contains the settings for the second auxiliary device that can be connected to a HandKey II or HandKey CR reader; *Aux2* contains the settings for the third (the settings for the first are on the *Auxiliary (AUX) Settings* tab; see page 48).

Alarm On: Even though this says *Alarm On*, the device does not have to be an alarm; this could trigger any type of auxiliary device. If a condition occurs and the corresponding box is checked, HandNet turns auxiliary output on if it is during the time zone selected at the bottom of the column on the right.

Auxiliary Input 1: This occurs if the reader receives input from an auxiliary input device. This is irrelevant if you do not have an auxiliary input device connected to the reader.

Auxiliary Input 2: This occurs if the reader receives input from the second auxiliary input device (HandKey II and HandKey CR support two auxiliary input devices; HandKey readers support just one). This is irrelevant if you do not have a second auxiliary input device connected to the reader.

Door Alarm: This occurs if the door connected to the reader is forced open, or if the door is kept open for longer than allowed based on the *Door Switch Shunt Time* on the *Configuration* tab in the *Reader Properties*; see page 48.

Duress Alarm: This occurs if a user entered the duress code. This code indicates that the user is in trouble or that someone is forcing the user to give him/her access; see page 47 for more on setting up a duress code.

F1 / F2 Key: This occurs if the corresponding key was pressed on the reader keypad (HandKey II and HandKey CR have F1 and F2 keys to the right of the number keys. The HandKey reader does not have these buttons, what you check here does not make any difference for that type of reader).

Invalid Access: This occurs if someone repeatedly entered a valid ID at a reader, and each time the reader does NOT recognize the user's hand (at the reader, the user would see the message *ID Refused*, and the *Activity* window would show the message *Access Denied*). The number of times that a user can try before this occurs depends on the *Number of Tries* entry on the *Settings* tab in the *Reader Properties*. If this occurs, someone might be trying to gain access with someone else's ID.

Power Failure: This occurs if the reader loses power from an external source. While this could just be due to an ordinary power failure, sometimes someone trying to gain invalid access will cut power in an attempt to disable alarm systems.

Tamper: This occurs if someone has shaken the reader roughly or opened the reader. Unless someone was servicing the reader, this message generally warrants further investigation.

Time Zone Violation: This occurs if a user enters a valid ID at a reader, but the user is not authorized to have access during the hours or days of the week based on the time zone associated with the reader in the access profile.

Try Again: This occurs if a user enters a valid ID at a reader, but the reader does not recognize the user's hand. This could be just the result of incorrect hand placement (if someone repeatedly entered a valid ID at a reader, and each time the reader does NOT recognize the user's hand, this would generate the *Invalid Access* condition above).

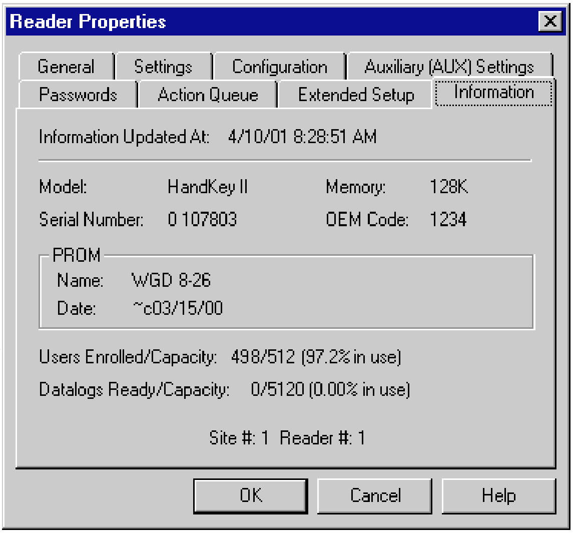
Clear Auxiliary Alarm On: If the auxiliary device is turned on, this controls whether it will be shut off when someone gains valid access (that is, enters a valid ID number and has his/her hand recognized). If this is checked, the alarm (or other auxiliary output) is turned off when a valid user gains access through that reader; if this is not checked, the output continues until the time entered in the following entry ends or until you go to the *Reader* menu, highlight *Auxiliary Output*, and pick *Off*; see page 129.

Timeout: This indicates the number of seconds that the auxiliary device should be on for.

Time Zone: This controls when HandNet should turn output to an auxiliary device on. For example, if the auxiliary device are a set of floodlights, it would only help to turn the lights on if the condition occurred at night. To do this, you would create a time zone for night hours, and then assign that time zone here (see page 61 for more on setting up time zones). If this says *Always*, HandNet turns output on for the auxiliary device whenever the checked condition(s) occur.

Information

This screen contains information about the reader. A key piece of information on this screen is the *Users Enrolled/Capacity:* this reflects the amount of available space in the reader. For example, the screen below reflects a reader with 498 users and space for up to 512 users. You could only add fourteen more users before this reader reached its limit. If you were approaching this limit, you would want to consider a memory upgrade for the reader so it would have space for additional users.



Information Updated At: 4/10/01 8:28:51 AM

Model: HandKey II
Memory: 128K
Serial Number: 0 107803
OEM Code: 1234

PROM
Name: WGD 8-26
Date: ~c03/15/00

Users Enrolled/Capacity: 498/512 (97.2% in use)
Datalogs Ready/Capacity: 0/5120 (0.00% in use)

Site #: 1 Reader #: 1

Most of the other information on this screen is helpful if your reader needs service, but not relevant to the ongoing use of the reader.

To get to this screen, click a reader in the right pane of the *Network* window, pick *Properties* from the *Reader* menu, and then click the *Information* tab.

* * * * *

Configuring the Physical Reader

While most of the information in the reader is controlled through HandNet, you must initially set up certain settings in the reader so it can communicate with HandNet. You do this through the command menus on the reader.

For readers with a network (ethernet) card: The IP address in this reader must match the *IP address on the Connection* tab in *Site Properties*; see page 39.

For a reader connected by serial port or connected as part of a chain of readers: The address in the reader must match the address on the *General* tab in *Reader Properties*; see page 45. The serial settings must also be correct, and the baud rate must match the baud rate on the *Connection* tab in *Site Properties*; see page 35.

We do not recommend changing any other settings through the reader command menus. All other settings can be controlled through *Reader Properties* in HandNet; see page 45 (if you were to make other changes directly in the reader, these would be overridden by the settings in HandNet when you enabled the reader).

Getting to the Setup Menu in the Reader

1. Enter command mode on the reader:

   If you have a HandKey II or HandKey CR reader: Press *CLEAR*, and then press *ENTER*.

   If you have an ID3D HandKey reader: Press *#* AND *** (you can press them at the same time, or one after the other).

If you have not used the reader with HandNet before, or if you have used it with HandNet and cleared its memory, the display looks like this.

```
ENTER PASSWORD
```

Type the password for the setup menu and press *ENTER* or *#.* If you have not changed it, the password is two (2).

If you have previously used the reader with HandNet and are reconfiguring it for another site or location, you may see:

```
READY:
*:
```

If the display looks like this, type your user ID and press *ENTER* or *#*. The reader will ask you to place your hand. Once you place it, you should then see the *Enter Password* display shown above. Type the password for the *Setup* menu and press *ENTER* or *#*. If you have not changed it, the password is two (2).

Changing the Reader Address

You must set the address in readers that are connected to the computer by a serial cable, and in readers that are connected to another reader (that is, readers that are not the first reader in the site). You cannot change the address in a reader that has an ethernet card; these readers automatically have an address of zero (0).

The following steps are specific to the HandKey II and CR; the menus are slightly different in other readers. Please see the manual that came with the reader if you are not sure how to find the correspond settings in your reader.

1. If you have not already done so, follow the steps on page 54 for getting to the reader setup menu.
2. Press the ** / NO* button until the display looks like this:

```
SET ADDRESS
*  NO     YES #
```

3. Press the *# / YES* button. The display will look like this:

```
RDR ADD ID 1
NEW?:
```

4. Type the new address. The address you enter must match the address on the *General* tab in *Reader Properties*; see page 45. Press *YES* or *ENTER*. The display returns to:

```
SET ADDRESS
*  NO     YES #
```

5. If you are done changing settings, press *CLEAR* to leave the *Reader Command* menu. If you need to change others settings, press *NO* until you get to the next setting you need to change.

Changing the Serial Settings and Baud Rate

You must have appropriate serial settings and baud rate in readers that are connected to the computer by a serial cable, and in readers that are connected to another reader (that is, readers that are not the first reader in the site). These settings do not apply to a reader with an ethernet card.

The following steps are specific to the HandKey II and CR; the menus are slightly different in other readers. Please see the manual that came with the reader if you are not sure how to find the correspond settings in your reader.

1. If you have not already done so, follow the steps on page 54 for getting to the reader setup menu.
2. Press the *NO* button until the display looks like this:

```
SET SERIAL
* NO     YES #
```

3. Press the *YES* button. The display will look like this:

```
SET RS-485/422?
* NO     YES #
```

4. Typically you will answer *YES* here. The display now asks for the baud rate. The baud rate here must match the rate on the *Connection* tab in *Site Properties*. Generally 9600 is appropriate.

   If you have a HandKey II or HandKey CR:

   The display will show the baud rate:

```
SET RS-485/422?
* NO     YES #
```

   To accept the rate shown and continue, press *YES*. To change the rate, press *NO* to cycle through the choices until you find the one you want.

   If you have an ID3D HandKey: The baud rate is represented by a code:

baud rate	code	baud rate	code
38.4K	0	2400	4
19.2	1	1200	5
9600	2	600	6
4800	3	300	7

   For example, for 9600, you would enter the code of two (2).

5. The reader will display:

```
SET RS-232?
* NO     YES #
```

Unless you have a printer connected directly to the reader, you would typically answer *NO* here. If you have a printer directly connected to this reader, answer *YES* (most users working with HandNet print from HandNet rather than connecting a printer directly to the reader). The only other time you might say *YES* here was if you had a single reader connected directly to HandNet with a serial port; there is a way to wire the connection to use RS-232 (if this were the case, you would say *YES*, pick the appropriate baud rate, and then indicate that RS-232 was connected to 1-Host (that is, HandNet)).

6. Once you are done, you see the *Set Serial* display again:

```
   SET SERIAL
*  NO     YES #
```

7. Press *CLEAR* to leave the command menu.

Changing the IP Address in a Reader with an Ethernet Card

You must set the IP address in a reader with an ethernet card. Before you do this, get the appropriate IP address and gateway (if needed) from your network administrator. If you have a WAN (wide area network), you also need the subnet mask; only certain subnet masks are supported; see the table below.

1. If you have not already done so, follow the steps on page 54 for getting to the reader setup menu.

2. Press the *NO* button until the display looks like this:

   SET SERIAL
   *** NO   YES #**

3. Press the *YES* button. The display will look like this:

   IP ADDRESS
   000.000.000.000

   If the display says *Set RS-485/422?* at this point, the reader does NOT have a network card. Contact your dealer if you need to get one.

4. Quickly type the correct address; if you pause for more than about four seconds while entering the IP address, the reader advances to the next display without saving your change. The address will have four parts separated by periods. Enter each part as three digits; if one part has less that four digits, add zeros before that part of the number to make it three digits. You do not have to enter the periods. For example, if your administrator gave you the address 192.9.210.10, you would enter:

   192 009 210 010

   This address must match the IP address on the *Connection* tab in *Site Properties*; see page 39. Press *YES* or *ENTER*. The display will now look like this:

   GATEWAY
   000.000.000.000

5. If your network administrator has told you to enter a gateway, do so; otherwise press *YES* or *ENTER*. As with the IP address, if you change this, you must type fairly quickly; if you pause for more than about four seconds while entering the gateway, the reader advances to the next display without saving your change. Once press *ENTER*, you see:

   HOST BITS: 0
   NEW?

6. If you are communicating over a LAN (local area network), type zero (0) for the Host Bits and press *YES* or *ENTER*. If you have a WAN, enter the number from the table below that corresponds to your subnet mask (only the subnet masks listed are currently supported). If you are not sure, check with your network administrator.

For this subnet mask:	Enter this for the host bits:	For this subnet mask:	Enter this for the host bits:
255.255.255.255	0	255.255.224.0	13
255.255.255.254	1	255.255.192.0	14
255.255.255.252	2	255.255.128.0	15
255.255.255.248	3	255.255.0.0	16
255.255.255.240	4	255.254.0.0	17
255.255.255.224	5	255.252.0.0	18
255.255.255.192	6	255.248.0.0	19
255.255.255.128	7	255.240.0.0	20
255.255.255.0	8	255.224.0.0	21
255.255.254.0	9	255.192.0.0	22
255.255.252.0	10	255.128.0.0	23
255.255.248.0	11	255.0.0.0	24
255.255.240.0	12		

7. The reader will display:

```
  9600 BAUD
* NO     YES #
```

The speed you choose should match the baud rate you are setting in the rest of the readers in this site. Generally 9600 is appropriate. To accept the rate shown and continue, press *YES*. To change the rate, press *NO* to cycle through the choices until you find the one you want.

Once you press *YES*, the reader display returns to:

```
  SET SERIAL
*  NO     YES #
```

8. If you missed one of the settings because the reader display changed too quickly for you, press *YES* to go through the settings again. If you are done changing settings, press *CLEAR* to leave the command menus.

9. If you need the changes to take effect immediately, disconnect the power from the reader, wait a few seconds, and then connect the power again. This resets the reader. If you do not do this, it may take up to six minutes for the changes to take effect.

* * * * *

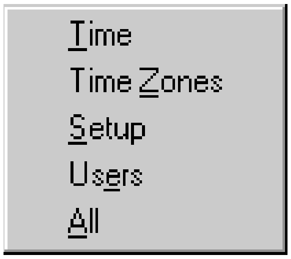
Resending Information to a Reader

Why You Might Need to Resend Information

While HandNet automatically sends the appropriate information to readers, occasionally you will need to use this when correcting a problem with a reader. You can do this with *Download* on the *Reader* menu.

Getting to the Download Option

To do this, select one or more readers, and go to the *Reader* menu, click *Download*, and then click the type of information to send.



Time: This sends the current time from the computer to the selected reader(s). You typically only need to use this option if the time changed (for example, for Daylight Savings Time). You can select all of your readers and send the time to all of them at once, or you can select specific readers.

Time Zones: This sends time zone and holiday information to the selected reader(s). You need to download this information if you change *Time Zones* (page 61) or *Holidays* (see page 65).

Setup: This sends configuration information to the selected readers. In most cases this is done automatically.

Users: After adding users, you need to download them to the hand readers so the readers will recognize the new users. This sends all current users to the selected readers.

All: This sends *Time, Time Zones, Setup*, and *User* information to the selected reader(s). You would use this when you set up a new reader so the reader had all the needed information.

Confirming That You Want to Send Information to the Reader

Whenever you choose to download information to readers, HandNet asks you to confirm that you want to download to the selected reader. Click *YES* to continue.

* * * * *

Settings That Control User Access

Setting Up Time Zones

What Time Zones Are

Time zones are periods of time on different days of the week when users can have access. There is no connection between what we call time zones in HandNet and the time zones we usually think of that have to do with different times around the world. This does not have anything to do with Eastern, Central, Mountain, or Pacific time; it only has to do with controlling which hours of the day access is available through readers.

When You Need to Set Up Time Zones

If you want some users to be able to use certain readers only during certain hours or on certain days of the week, time zones let you identify when access is available. For example, suppose some users should only be able to gain access through certain readers between 8:00 AM and 5:00 PM, Monday through Friday. You would create a time zone that identified these times and days, associate that time zone with appropriate readers using an access profile, and then assign that access profile to the users. After you did this, users with that access profile would only have access during the times you identified in the time zone.

You can also use time zones to determine when certain doors should be automatically unlocked; see *Automatically Unlocking a Door on a Scheduled Basis* on page 128.

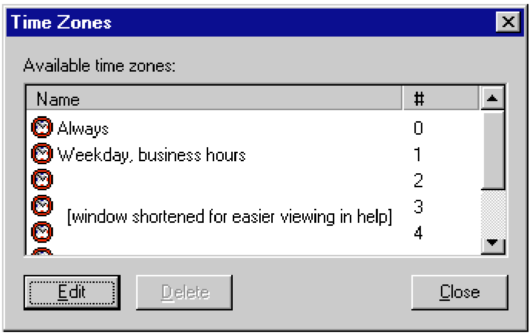
If users should have different access on holidays than on other days, you can set different hours for holidays in the time zone. You will have to also set up holidays; see page 65.

When You Do not Need to Set Up Time Zones

If you do not need to limit access by day or time (that is, if users could use the readers twenty-four hours a day, seven days a week if they wanted), and if you do not want doors to unlock automatically, you do not need to set up time zones.

Getting to the List of Time Zones

1. Click the *View* menu.
2. Click *Time Zones*. You see a screen like the one below (though the time zones listed will be different). From here you can add, change, or delete time zones.



Time Zones

Available time zones:

Name	#
Always	0
Weekday, business hours	1
	2
[window shortened for easier viewing in help]	3
	4

Adding or Changing Time Zones

The first time zone is *Always* and the last (#61) is *Never*; you cannot change either of these.

To add a time zone, click one of the blank lines in the time zone list and click *Edit*. To change a time zone, click the time zone to change and click *Edit*. Change the *Time Zone Definition* screen (see below) as needed and then click OK to return to this list. You can then add or change another or click *Close* when done.

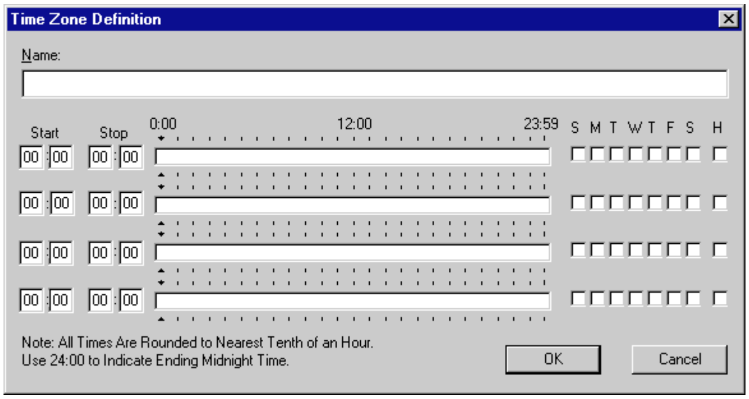
Deleting Time Zones

Click the time zone and click *Delete*. The program asks if you are sure you want to delete the time zone. Click *Yes*.

If you try to delete a time zone and get a message that the time zone is used in an access profile, you must close the time zone window, go to access profiles and select a different time zone for each reader that had this time zone selected if you still want to delete it.

Time Zone Definition Screen

This screen determines what hours access is available on different days of the week. A time zone is active if the time is equal to or after the start time and before the stop time, and if the day of the week matches one of those checked.



Time Zone Definition

Name:

Start	Stop	0:00 … 12:00 … 23:59	S	M	T	W	T	F	S	H
00 : 00	00 : 00		□	□	□	□	□	□	□	□
00 : 00	00 : 00		□	□	□	□	□	□	□	□
00 : 00	00 : 00		□	□	□	□	□	□	□	□
00 : 00	00 : 00		□	□	□	□	□	□	□	□

Note: All Times Are Rounded to Nearest Tenth of an Hour.
Use 24:00 to Indicate Ending Midnight Time.

Name: Enter a name that will be clear to you so that when you associate the time zone with a reader in an access profile, you will be sure to pick the right one.

You can assign four different periods in each time zone if you need them; for example, if you want to give access during different hours on different days. Be sure to leave lines that you do not need blank.

Start/Stop Times: Enter hours after noon using military time. Use the chart below or see the examples if you need help. Times are divided into tenths of an hour, so HandNet rounds minutes to the nearest six minute interval. For example, if you enter 8:02, the program rounds this to 8:00; if you enter 8:03, the program rounds it to 8:06.

	Enter on the Time Zone screen		Enter on the Time Zone screen
noon	12:00	**7:00 PM**	19:00
1:00 PM	13:00	**8:00 PM**	20:00
2:00 PM	14:00	**9:00 PM**	21:00
3:00 PM	15:00	**10:00 PM**	22:00
4:00 PM	16:00	**11:00 PM**	23:00
5:00 PM	17:00	**midnight**	00:00 if a start time; 24:00 if a stop time
6:00 PM	18:00		

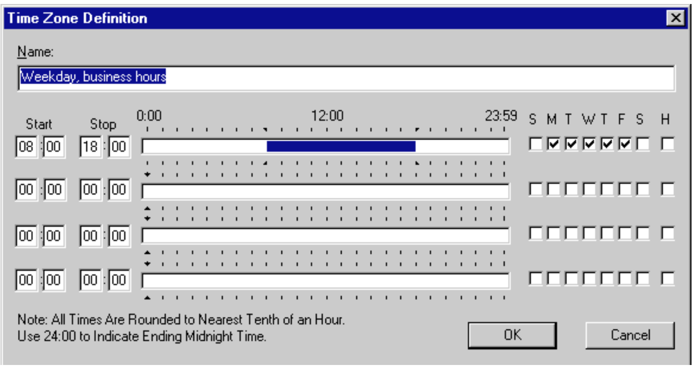
If a time zone must cross midnight (for example, if you want to give access between 8:00 PM and 4:00 AM), you must use two lines to create that access time. The first line would give access from 20:00 to 24:00 (that is, 8:00 PM to midnight), and the next line would give access on the same days of the week from 0:00 to 4:00 (that is, midnight to 4:00 AM). See the third example on the following page.

Days of the Week: Check the boxes for each of the day of the week that access should be available. The letters over the boxes correspond to the days of the week (Sunday through Saturday); H stands for holiday. If access is different on holidays than on other days, you must also set up holidays; see page 65. See the examples on the following page.

Click *OK* when done.

Examples of Time Zone Settings

These settings give access between 8:00 AM and 6:00 PM, Monday through Friday. They do not give any access on Saturday, Sunday, or Holidays. The blue bar in the center section of the screen shows when access is available.



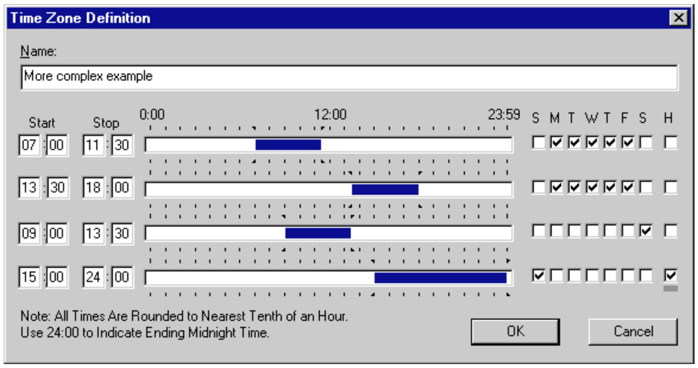
Time Zone Definition

Name: Weekday, business hours

Start	Stop	S	M	T	W	T	F	S	H
08 : 00	18 : 00	□	☑	☑	☑	☑	☑	□	□
00 : 00	00 : 00	□	□	□	□	□	□	□	□
00 : 00	00 : 00	□	□	□	□	□	□	□	□
00 : 00	00 : 00	□	□	□	□	□	□	□	□

Note: All Times Are Rounded to Nearest Tenth of an Hour.
Use 24:00 to Indicate Ending Midnight Time.

The following settings give access from 7:00 to 11:30 in the morning on weekdays, from 1:30 in the afternoon to 6:00 PM also on weekdays, from 9:00 in the morning to 1:30 in the afternoon on Saturdays, and from 5:00 PM to midnight on Sundays and holidays.



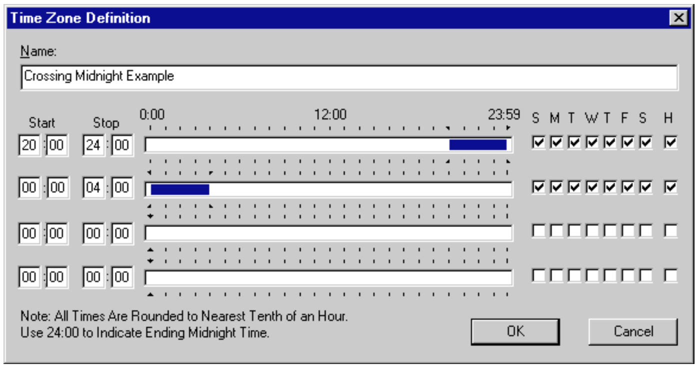
Time Zone Definition

Name: More complex example

Start	Stop	S	M	T	W	T	F	S	H
07 : 00	11 : 30	□	☑	☑	☑	☑	☑	□	□
13 : 30	18 : 00	□	☑	☑	☑	☑	☑	□	□
09 : 00	13 : 30	□	□	□	□	□	□	☑	□
15 : 00	24 : 00	☑	□	□	□	□	□	□	☑

Note: All Times Are Rounded to Nearest Tenth of an Hour.
Use 24:00 to Indicate Ending Midnight Time.

The following settings show how to cross midnight. This gives access from 8:00 PM through 4:00 AM any day of the week. Notice that this requires two lines to set up: the first going from 8:00 PM to midnight, and the next going from midnight to 4:00 AM.



Time Zone Definition

Name: Crossing Midnight Example

Start	Stop	S	M	T	W	T	F	S	H
20 : 00	24 : 00	☑	☑	☑	☑	☑	☑	☑	☑
00 : 00	04 : 00	☑	☑	☑	☑	☑	☑	☑	☑
00 : 00	00 : 00	□	□	□	□	□	□	□	□
00 : 00	00 : 00	□	□	□	□	□	□	□	□

Note: All Times Are Rounded to Nearest Tenth of an Hour.
Use 24:00 to Indicate Ending Midnight Time.

* * * * *

Setting Up Holidays

When You Need to Set Up Holidays

If you want to prevent access on holidays or to give different access on holidays than on other days, the holidays list identifies when those holidays are. When you reach a holiday in the list, HandNet applies the holiday access times instead of the regular access times (if you set holidays up, you will also have to set up time zones to indicate what access users should have on different days; see page 61 for more on setting up time zones).

When You Do not Need to Set Up Holidays

If you do not give different access on holidays than on other days, you do not need to set up any holidays.

Adjusting Holidays Each Year

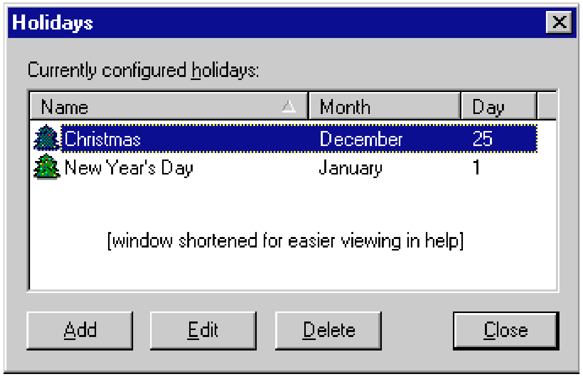
If you set holidays up, remember to return to the holidays setup at the beginning of each year to adjust each holiday that is celebrated on a different date than the previous year. For example, Thanksgiving, Memorial Day, and Labor Day are on different dates each year. Also, while holidays like Christmas and New Year's are always on the same date, when these holidays fall on a weekend, the day they are taken off is sometimes on a different date.

Getting to the Holidays List

1. Click *View* from the *Main Menu* bar.
2. Click *Holidays*. You see a list like this one below. From here you can add, change, or delete holidays.

Adding or Changing Holidays

To add a holiday, click *Add*; to change a holiday, click the holiday in the list and then click *Edit*. When you add or edit, you see this screen:



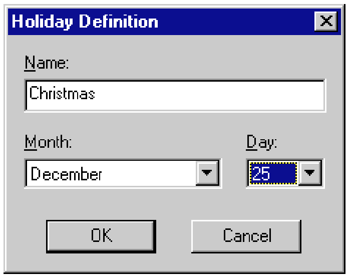
Currently configured holidays:

Name	Month	Day
Christmas	December	25
New Year's Day	January	1

[window shortened for easier viewing in help]

Name: Enter a name to help you identify the holiday.

Month: Click this entry and pick the month from the list (you could also press *TAB* from the *Name* entry and then type the first letter of the month. If more than one month begins with the same letter, typing that letter cycles through those months).



Name: Christmas

Month: December

Day: 25

Day: Click this entry and pick the day from the list (you could also press *TAB* from the *Month* entry and then type the first digit. For example, if you want to get to twenty-five, you would type two (2) several times. The first time you type two (2), the date would show *2*; when you type two (2) a second time, you would see *20*; typing two again would switch to *21*; you would repeat this until you got to the number you need).

Click *OK* when each entry is correct.

Deleting Holidays

To delete a holiday: Click the holiday in the list and click *Delete*.

* * * * *

Setting Up Access Profiles

When You Need to Set Up Access Profiles

If some users can only use certain hand readers and/or only use them at certain times or on certain days, access profiles define when each type of user can use each reader. For example, suppose your maintenance staff should have access to the maintenance rooms seven days a week, your office staff should have access to the office but only during business hours, and your supervisors should have access to everything at any time. You would create three access profiles: one for supervisors, one for office staff, and one for maintenance personnel. These profiles would identify which readers each group could use. In these profiles you would also identify which time periods each group could use each reader (you would set up these time periods first using *Time Zones*). After creating these different profiles, whenever you added a user, you would just identify which group the user was a part of, and the access profile for that group would automatically give the appropriate access.

To limit access to certain days or times, you must set up time zones before creating access profiles; see page 61 for more on setting up time zones.

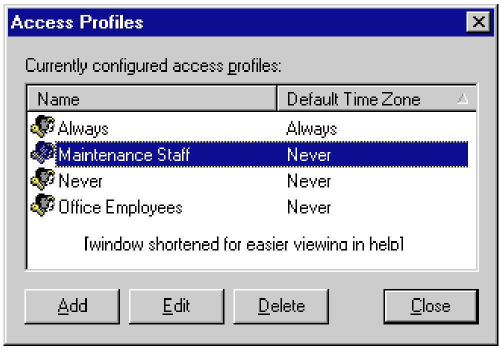
When You Do Not Need to Set Up Access Profiles

If you want all users to be able to use every reader any time, you do not need to set up access profiles. HandNet comes set up with an *Always* profile that lets users use any reader in the system twenty-four hours per day, seven days per week (it also has a *Never* profile that does not let the user verify at any reader at any time).

Getting to the List of Access Profiles

1. Click the *View* menu from the main menu bar.

2. Click *Access Profiles*. You see a screen like the one below (though the profiles listed will be different). From here you can add, change, or delete access profiles.



Access Profiles

Currently configured access profiles:

Name	Default Time Zone
Always	Always
Maintenance Staff	Never
Never	Never
Office Employees	Never

[window shortened for easier viewing in help]

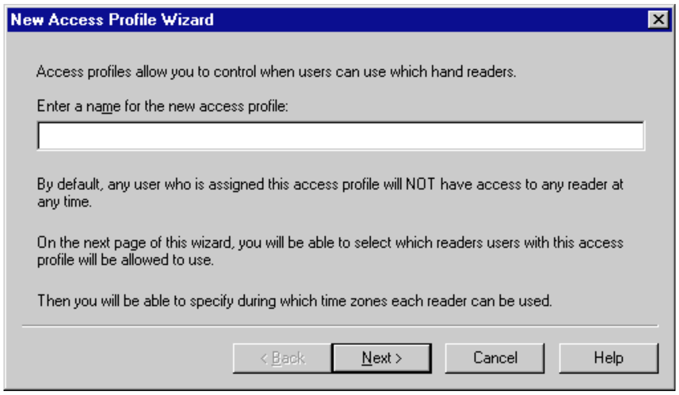
The *Default Time Zone* shown on this list does NOT reflect the time zones associated with the readers in this profile; it only reflects the time zone that HandNet initially picks if you associate another reader with this profile. Except for the *Always* profile, this column always says *Never*.

Adding an Access Profile

Click the *Add* button to add an access profile. This starts the *New Access Profile Wizard*.

New Access Profile Wizard, Screen 1

You see the *New Access Profile Wizard* when you add a new access profile to the list of access profiles.



Access profiles allow you to control when users can use which hand readers.

Enter a name for the new access profile:

By default, any user who is assigned this access profile will NOT have access to any reader at any time.

On the next page of this wizard, you will be able to select which readers users with this access profile will be allowed to use.

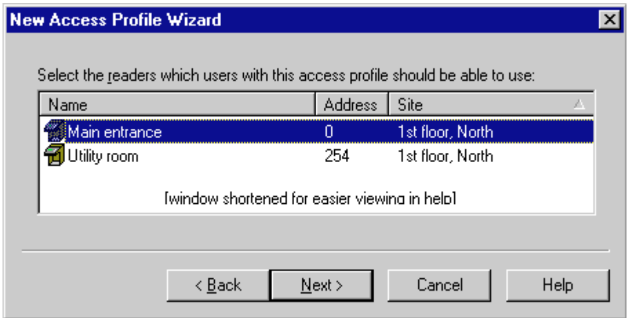
Then you will be able to specify during which time zones each reader can be used.

Name: Enter a name that describes the group of users that this access profile will be used for. For example, if this profile gives access that is appropriate for all of your maintenance staff, you could use that for the name. The important thing is for the name to be clear so that you do not give inappropriate access to users.

Click the *Next* button to go to the next screen.

New Access Profile Wizard, Screen 2

The second screen in the *New Access Profile Wizard* lists all of your readers (typically you will have many more than the two shown in the example below). Select each reader that you want to give access to with this profile, and then click *Next*.



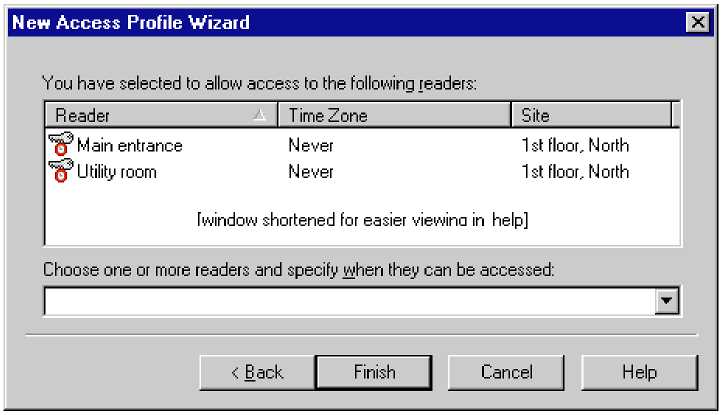
Select the readers which users with this access profile should be able to use:

Name	Address	Site
Main entrance	0	1st floor, North
Utility room	254	1st floor, North

[window shortened for easier viewing in help]

New Access Profile Wizard, Screen 3

The third and final *New Access Profile Wizard* screen shows all of the readers that you selected on the previous screen (if you discover that you missed a reader on the previous screen, click the *Back* button to return to the list of all readers and select it there).



You have selected to allow access to the following readers:

Reader	Time Zone	Site
Main entrance	Never	1st floor, North
Utility room	Never	1st floor, North

[window shortened for easier viewing in help]

Choose one or more readers and specify when they can be accessed:

When you come to this screen, each reader has a time zone of *Never*; you must change the time zone for each reader to give access to that reader through this profile.

To associate time zones with the readers:

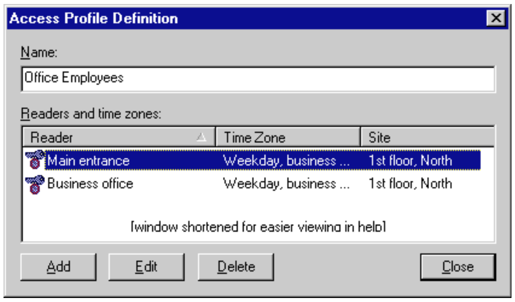
1. Select one or more readers on the list. If you forget to select readers, HandNet still lets you do the following step but it will not have any effect.

2. Click on the entry under *Choose one or more readers...* and select a time zone there. HandNet uses that time zone for each selected reader.

If you need to associate a different time zone with some readers, repeat these steps until you have specified a time zone for each reader. For example, suppose you were creating an access profile for maintenance workers, and suppose these workers had access to building entrances and maintenance facilities twenty-four hours a day, but they only had access to the business offices during normal business hours. You would select the entrance and maintenance readers and associate a time zone of *Always* with them. You would then select the business office readers and associate your normal business hours time zone with those readers.

Changing an Access Profile

To change an access profile, click it on the list and then click the *Edit* button. That brings up a list of readers that have been associated with the profile. The list looks like this:



Name: Office Employees

Readers and time zones:

Reader	Time Zone	Site
Main entrance	Weekday, business ...	1st floor, North
Business office	Weekday, business ...	1st floor, North

[window shortened for easier viewing in help]

To add another reader to those associated with this profile: Click the *Add* button to bring up the *Access Profile Override* box (shown on the following page). Complete the entries there and click *OK*.

To change the time zone a reader is accessible with this profile: Click the reader in the list and click *Edit* to bring up the *Access Profile Override* box. Click the *Time Zone* entry, select the appropriate time zone, and then click *OK*.

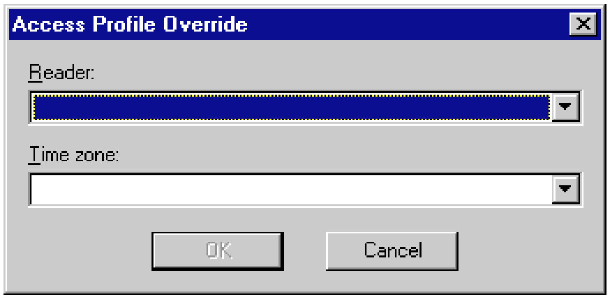
To change the time zone for several readers at once: Hold the *CTRL* key down and click each reader that you want to change the time zone. When all the appropriate readers are selected, click *Edit*. This brings up the *Access Profile Override* box but you can only change the *Time Zone* entry. Click the *Time Zone* entry, select the appropriate time zone, and then click *OK*.

To remove one or more readers from this access profile: Select the reader(s) in the list and click *Delete*.

Click *Close* to return to the list of profiles.

Access Profile Override Box

You see this same screen whether you are adding a reader to a profile or editing a reader that you have added previously (when adding the entries are initially blank; when editing, the entries are filled in with your previous choices).



Reader: Click this to choose a reader that should be associated with this profile. This only lists readers that have not already been added to this profile. If you click this and an empty pick box comes up, then you have already added all readers to this profile. This entry is disabled if you are changing several readers at once.

Time Zone: Click this and pick the time zone that the users with this profile should have access to the selected reader(s). If you have selected several readers, this changes all of them at once.

Click *OK* to return to the list of readers in this profile.

Deleting an Access Profile

To delete an access profile, click the profile on the list and click the *Delete* button. HandNet does not ask you to confirm the deletion, so make sure you pick the right one.

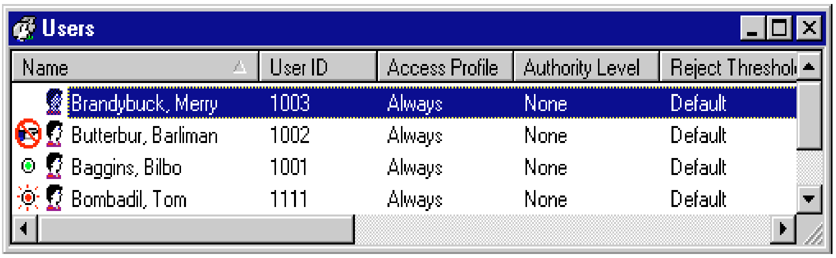
If you get a message that the access profile you are trying to delete is still assigned to a user, go to the list of users, double-click the user to go to the *User Properties*, click the *Security* tab, and select a different access profile for the user there. The message only lists the last user that the profile was assigned to, so there may be other users that also use the profile. Check the list of users to see if any other users use that profile (click the heading of the profile column in the user list to sort by profile; that will put all users with each profile together). If you find any other users using the profile you want to delete, select a different profile for each of them as well. Once no users are using the profile, you can return to this option and delete the profile.

* * * * *

Adding and Maintaining Users

Users Window

The users window lists every user that is in HandNet. To open this window, pick *Users* from the *View* menu or press *CTRL-U*.



Users

Name	User ID	Access Profile	Authority Level	Reject Threshol
Brandybuck, Merry	1003	Always	None	Default
🚫 Butterbur, Barliman	1002	Always	None	Default
🟢 Baggins, Bilbo	1001	Always	None	Default
🔴 Bombadil, Tom	1111	Always	None	Default

Understanding the Icons to the Left of the Name

	No icon indicates that the user is enrolled able to use any readers permitted by the access profile.
🚫	The no access icon indicates that the user is not enrolled yet and hence will not have access to any readers. You must enroll the user to give access; see page 87.
🟢	The green light indicates that the user currently has access, and that the limited access feature was used to so this access will automatically expire at some point; see page 93 for more about limited access.
●	The black dot indicates that the limited access feature was used to set a begin and end date/time for this user's access, and the user does NOT have access because the access period has not started yet; see page 93 for more about limited access.
🔴	The red light indicates that the limited access feature was used to set a begin and end date/time for this user's access, and the user does NOT have access because the access period has ended; see page 93 for more about limited access.

Changing How the User List is Sorted

You can sort the list of users using the information in any column by clicking on the column heading. For example, to sort the user list alphabetically by name, click on the name heading. If you click on the same heading again, it will sort the list in reverse order (for example, using the name, it would sort from Z to A). Usually sorting by name or ID is most useful, but occasionally you might sort by another column to put all similar users together. For example, if you were preparing to change or delete a particular access profile, you might sort by the access profile column so that all users with that profile would be together on the list.

Rearranging Columns in the User Window

To move any column, click the column heading and hold the mouse down. With the mouse held down, drag the column heading to the left or right; see the online help for an example of this.

You might want to move columns to keep important information like user IDs out of view, or, if you have created custom user entries, you might want to move them to where you can see them, since they are initially out of view.

F5 restores all columns to the positions they had when you started HandNet. If you want HandNet to save the new column positions, exit the HandNet program and come back in. HandNet then uses your changed column positions as the new standard or default.

Changing Column Width

You can also change the width of a column by pointing to the edge of the column heading, holding the mouse down, and then dragging the edge of the column to the desired position. This lets you fit more columns in the window (or, if you wanted to hide information from the casual observer, you could make columns wider to push other columns out of view); see the online help for an example of this.

F5 restores all columns to the widths they had when you started HandNet. If you want HandNet to save the new column widths, exit the HandNet program and come back in. HandNet then uses your changed column widths as the new standard or default.

Columns of Information in the User Window

User ID: The ID number the user must enter at the reader to gain access.

Access Profile: The profile determines which readers the user can access and when. You set up access profiles using *Access Profiles* on the *View* menu. You can change a user's access profile on the *Security* tab in *User Properties*; see page 92.

Authority Level: This indicates whether the user is allowed to access the command menus on the readers. For most users, this should say *None.* You can change a user's authority level on the *Security* tab in *User Properties*; see page 92.

Reject Threshold: The reject threshold controls how closely a user's hand must match the stored hand profile for the user to gain access. If this says *Default*, then HandNet uses the *Reject Threshold* on the *Configuration* tab in the *Reader Properties* (see page 47). If this says *Default** (with an asterisk), this means the user does not need hand recognition to gain access because the user was set up with a special enrollment; see page 76. If this shows a number, someone chose to override the standard reject threshold on the *Security* tab in *User Properties*; see page 93. A lower number requires a very precise match to gain access; a high number requires the hand to match less exactly. Thirty is the lowest number possible; 250 is the highest. One might use a lower number for users with access to the highest security areas; one might need a higher number if a user had arthritis or other hand condition that made it impossible to consistently place the hand on the reader in exactly the same position.

Last Site: This lists the last site where the user gained access. This is blank for a new user who has not accessed a reader yet.

Last Reader: This lists the last reader the user gained access through. This is blank for a new user who has not accessed a reader yet.

Last Time Used: This shows the date and time of the user's last access.

Limited State: This says *Unlimited* for users who are not set up to only have access for a limited period of time, that is, for users whose access will continue indefinitely. For users who are set up to only have access for a limited period of time, this says *Waiting* if the access period has not started yet, *Limiting* if the user currently has access, and *Expired* if the user's access period has ended; see page 93 for more about limited access.

Limited Start Time: If this user has been set up to have access for a limited period of time, this shows the date and time that the user's access begins. HandNet will not give the user access before this date/time. This is blank for other users; see page 93 for more about limited access.

Limited End Time: If this user has been set up to have access for a limited period of time, this shows the date and time that the user's access ends. HandNet will not give the user access after this date/time. This is blank for other users; see page 93 for more about limited access.

Additional Custom Columns: If you created any custom user entries, those columns would be listed as well; see page 97 for more about adding custom entries.

* * * * *

Adding Users Overview

Before You Add Users

If you are going to limit access to specific time periods or specific readers, set up *Time Zones* (see page 61) and *Access Profiles* (see page 67) before you set your users up.

Choosing How to Add the Users

If you have already set up users in a stand alone reader: You do not need to add users; you can upload user information from the reader; see *Getting User Information from a Reader* on page 99.

If you have been using one of our MS-DOS HandNet products (HandNet or HandNet Plus): You do not need to add users; you can import them from HandNet(+); see page 98.

If you only have one user to add, if you do not assign ID numbers sequentially, if you are adding users with different access profiles, if you want to fill in custom entries when adding the users, or if users choose their own ID numbers: Add a single new user; see page 76.

If a user needs access without hand recognition: Add a single new user and choose the *Special Enrollment* option. Before you do this, read *Adding a User Who Has Access Without Hand Recognition* below.

If you have many new users with the same access profile and you want automatically assigned ID numbers: Add multiple new users; see page 81.

Adding a User Who Has Access Without Hand Recognition

If a user has severe arthritis, missing fingers, or other hand deformities that keep the user's hand from being recognized, you can give the user access without hand recognition (if you choose this, the reader still asks the user to place a hand on the reader so it will not be apparent to others that hand recognition is not required, but the reader does not check the image of the hand; it gives access regardless of whose hand is placed there). **Since bypassing hand recognition gives you reduced security, only use this as a last resort.** Try these options first:

If the user only has a problem with the right hand: Enroll the user using the left hand (the user will place the hand palm up on the reader).

If the user has all of his/her fingers and is just having trouble with placing the hand consistently: On the *Security* screen in *User Properties*, check *Override the reader's reject threshold*, and drag the pointer to the far right (the *Less Sensitive* side). This causes the reader to be more tolerant of what it considers a match for that user's hand.

If these options are not possible, or if you try them and they do not work, then you will have to set the user up so that hand recognition is not required. To do this, follow the steps below.

1. If you have already added this user, open the *User* window, click the user once, press the *DEL* key (or pick *Delete* from the *User* menu), and confirm that you want to delete the user.

2. Click the *User* menu and then click *Add New….* This takes you to the first screen of the *New User Wizard*.

3. Check the *Special Enrollment* box. Since this option does give lower

security, HandNet asks you to confirm that you want to do this; click *Yes*.

4. Click the *Next* button.
5. Complete the rest of the process just as you would for any other new user.
6. Since the reader does not have to recognize this user's hand, you do not need to enroll this user; once you click *Finish*, the process is done for this user.

Allowing Users to be Added at the Reader

HandNet is initially set up to only allow new users to be added in the program; you can enroll a user at a reader, but you cannot add a new user there. If you want to be able to add and enroll a new user at a reader without adding the user to HandNet first, do this:

1. Click the *View* menu.
2. Click *Settings*.
3. Click the *Security* tab.
4. Check the box by *Do not delete unauthorized enrollments*.
5. Underneath this, indicate what access profile should be given to a user who is added at a reader (if you do not want the user to be able to access any readers until you change them in HandNet, choose *Never*).
6. Click the *OK* button at the bottom of the box.

Preventing Users from Being Added at Readers

Follow the steps above to get to the *Security* tab and make sure that *Do not delete unauthorized enrollments* is NOT checked.

* * * * *

Adding a Single New User

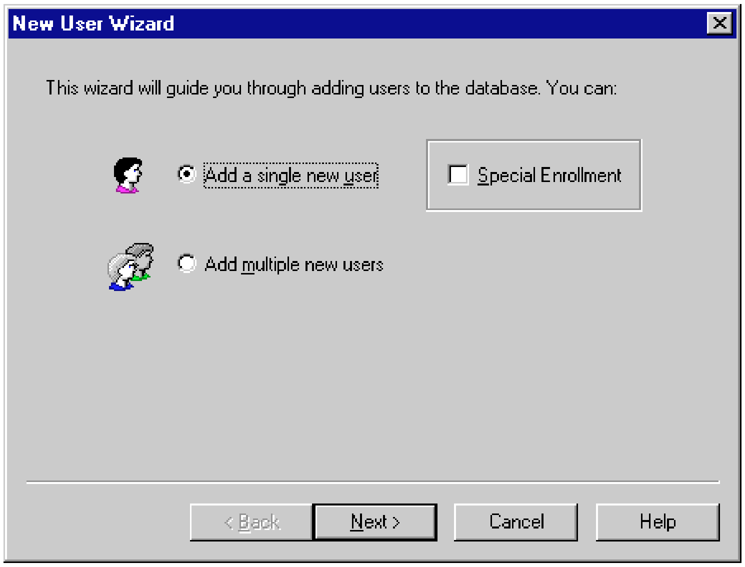
QUICK STEPS

Adding a Single User

1. Click the *User* menu and then click *Add New...*. This takes you to the first screen of the *New User Wizard*.
2. *Add a single new user* is automatically selected, so click *Next* to continue.
3. On the *Name/ID* screen, enter the name and the ID number you are assigning to that user, and then click *Next* to continue.
4. On the *Security* screen, choose the access profile, authority level, and other security options. If you have set up custom user entries, click *Next*; otherwise click *Finish*.
5. If you see the *Custom* entries screen, fill in the column on the right and then click *Finish*.
6. Once you are done adding the user, you must enroll the user before the user will have access; see page 87.

Beginning the Process

To begin adding a new user, pick *Add New...* from the *User* menu.


New User Wizard

This wizard will guide you through adding users to the database. You can:

● Add a single new user

□ Special Enrollment

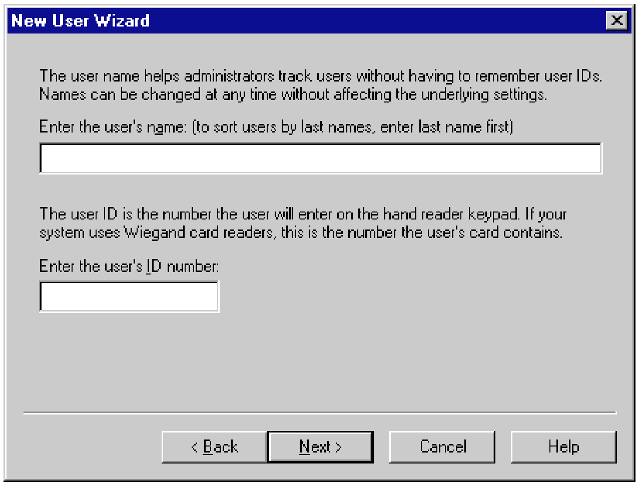
○ Add multiple new users

Special Enrollment: Check this box only if the user has severe hand deformities that require you to give the user access without hand recognition. This box is disabled if you are adding multiple users; if you are enrolling a user without hand access, you must add a single user.

Click *Next* to continue.

Name/ID Screen

This is the second screen in the process of adding a single new user:



New User Wizard

The user name helps administrators track users without having to remember user IDs. Names can be changed at any time without affecting the underlying settings.

Enter the user's name: (to sort users by last names, enter last name first)

The user ID is the number the user will enter on the hand reader keypad. If your system uses Wiegand card readers, this is the number the user's card contains.

Enter the user's ID number:

Name: Enter the user's name.

If you want to sort the list of users by last name: Enter the last name first. For example, if the user's name is Sam Gamgee, you would enter *Gamgee, Sam*.

If you have two users with the same name: You must enter a unique name for each user. If two users have the same name, you might add a middle initial, or you might add a job description after each. For example, if you have two users named John Jones, you might enter something like *Jones, John (engineer)* and *Jones, John (maintenance).*

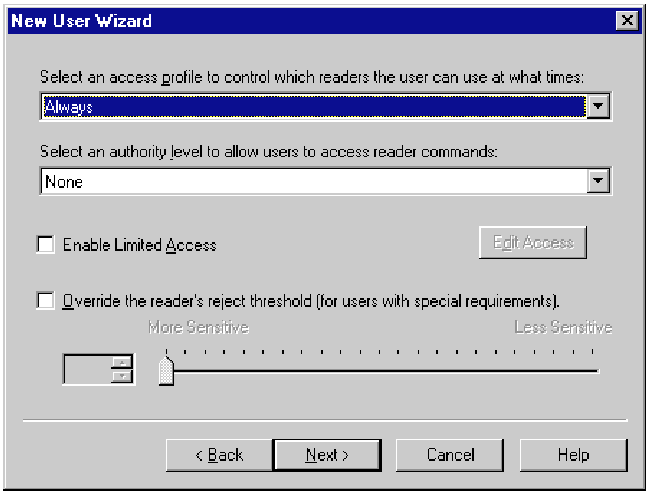
ID Number: Each number must be unique (if you could give the same number to two users, the reader would not know which was trying to gain access). Longer numbers are slightly more secure, but four or five digits are generally adequate in context where user's must enter the number. You may enter up to ten digits if you do not use a duress code, or up to nine digits if you do use a duress code. If you use a duress code, make sure that you do not create an ID that begins with that digit (see page 47 for more about duress codes). If you have set up an ID length on the *Settings* tab in the *Reader Properties* (see page 46), make sure that you do not create an ID that is longer than this.

If you use Wiegand card readers: Enter the ID number that is stored on the card.

Do not begin an ID with 0 (zero) if you are going to enroll the user with the command menus on the reader: HandNet lets you enroll a user by either picking *Enroll* from the *Reader* menu, or by using the *Command* menus on the reader (see page 88 for more about these options). If you are going to use the command menus on the reader, the *ID Number* should not begin with zero (0). While HandNet distinguishes between *5* and *0005*, the process of adding a user from the reader command menu does not. This means that if you create a user with an ID of 0005 in HandNet and try to enroll that user with the command menus on the reader, when you type 0005, the reader thinks you are enrolling user 5. This will not correspond with 0005 in HandNet. If you are going to use *Enroll* on the *Reader* menu, you can begin an ID with zero (0) (if you are never going to begin an ID with zero, this might be a good choice for a duress code if you use one).

Security Screen

This screen controls what this user has access to and when.



Select an access profile to control which readers the user can use at what times: Always

Select an authority level to allow users to access reader commands: None

□ Enable Limited Access

□ Override the reader's reject threshold (for users with special requirements).

Select an access profile to control which readers the user can use at what times: Click this entry for a list of available access profiles. If this user can use all readers at all times, choose *Always*. If you do not want the user to be able to use any readers, choose *Never*. For other access, select the appropriate profile. You must set access profiles up before they are available here; see page 67 for more on setting up access profiles.

Select an authority level to allow users to access reader commands: This determines what the user can do at the reader. Each higher level gives access to the lower levels as well. For example, a user with an authority level of four can also use the *Level 1, 2* and *3* menus. Except for recalibrating the reader (part of *Level 1*), and enrolling a user if you have not purchased the upgrade to the full feature set, HandNet can control every setting in the reader, so there is generally no need to control settings through the reader menus.

None: This lets the reader gain access through the reader, but not use the command menus in the reader to change the reader's settings. This choice is appropriate for most users.

(1) Service: This lets you recalibrate the reader and change the reader's status display.

(2) Setup: This lets you control reader setup issues including how the reader is connected to your computer network, what language the reader displays in, the date/time, etc.

(3) Management: This lets you list users.

(4) Enrollment: This lets you add or remove users.

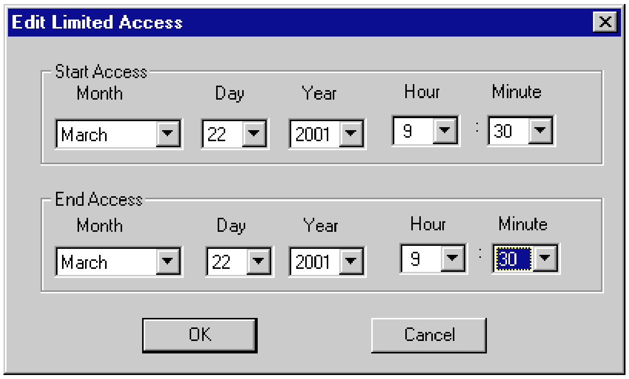
(5) Security: This lets you control the passwords for the reader menus, change time zones, enroll users who do not need hand access, etc.

See the HandKey manual for more on directly changing settings through the reader.

Limited Access

Enable limited access: This gives a user access for a specific date range. For example, suppose a contractor or temporary employee was going to be working in your building for a month. Or suppose an employee gave notice that s/he was leaving for a new job in two weeks. Once this period was over, you would not want these users to have access. Rather than having to remember to disable the user on the appropriate date, this option lets you set a start and end date/time so the user is automatically enabled and disabled at the appropriate points.

To set up start and end date/times, check the box by this button and then click the *Edit Access* button (this button only works if you have checked the box). This takes you to the *Edit Limited Access* screen:



Edit Limited Access

Start Access

Month	Day	Year	Hour	Minute
March	22	2001	9	30

End Access

Month	Day	Year	Hour	Minute
March	22	2001	9	30

To change either start or end date or time, click the corresponding entry and pick from the list that comes up.

This option is disabled if you have not purchased the license upgrade to the full feature set of Version 2.0.

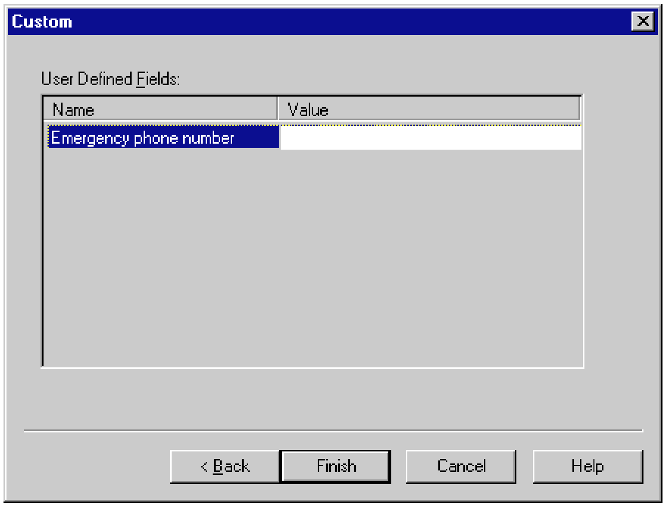
This option is NOT for limiting access to specific readers or for specific times of the day; to control that, use the *Access Profiles* entry.

Override the reader's reject threshold (for users with special requirements): For users with a physical condition like arthritis that prevents them from placing their hands on the reader in exactly the same way each time, this option lets you control how exact the hand match must be for the reader to grant access.

Normally you would not change this when adding the user. Instead, add and enroll the user, and then see if the user is having trouble gaining access. If a user is having trouble getting access consistently, go to the *Security* tab in the *User Properties* and change this entry there. You would check this box and then slide the pointer further to the right (the *Less Sensitive* side). If a user has a really severe hand condition, it is possible to give access without hand recognition, but because this offers reduced security, that should only be a last resort.

Custom Entries Screen

You only see this screen if you have set up any custom user entries (see page 97). The entries on this screen vary depending on what you have set up. For each entry on this screen, type the information in the *Value* column.



Name	Value
Emergency phone number	

Click *Finish* when done.

What to Do Next

The next step is to enroll the user; see page 87.

* * * * *

Adding a Group of Users at Once

You would add a group of users at once if you have to add many new users with the same access profile and other security access options, and if you want HandNet to automatically assign sequential ID numbers (if each user needs a different access profile, if you need to assign non-sequential ID numbers, or if you want to fill in custom user entries while adding the users, add single users instead; see *Adding a Single New User* on page 76).

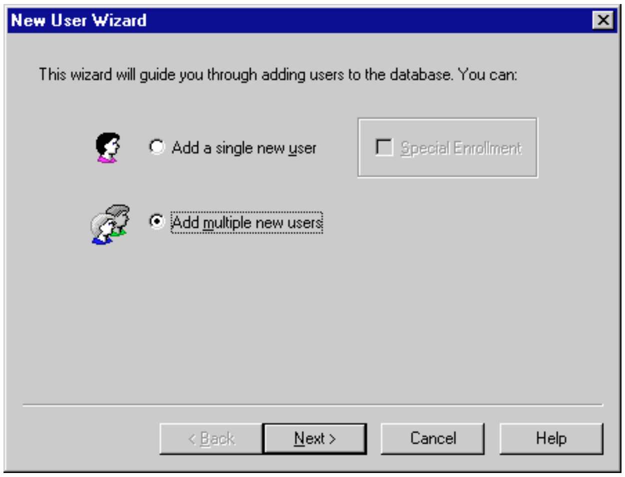
QUICK STEPS

Adding Multiple Users

1. Click the *User* menu and then click *Add New....* This takes you to the first screen of the *New User Wizard*.
2. Click *Add multiple new users*, and then click *Next*.
3. On the screen that asks for the number of users and starting ID, enter the number of users to create, and the ID number for the first new user. Click *Next* to continue.
4. On the *Security* screen, choose the access profile to assign to each of the new users. If needed, you can change the authority level and limited access. Do NOT change the user reject threshold. If you need to, you can later change this individually for a user who is having access problems. Click *Next* to continue.
5. The next screen shows the progress in adding the users. Once the process is done, click *Finish*.
6. You need to enroll the users before they have access. Typically, you will also rename the users since adding multiple users at once uses the ID number for the name.
7. If you have set up custom user entries, you will also want to edit the *Properties* for each user, click the *Custom* tab, and fill the appropriate information in there.

Beginning the Process

To begin adding a new user, pick *Add New...* from the *User* menu.



New User Wizard

This wizard will guide you through adding users to the database. You can:

○ Add a single new user

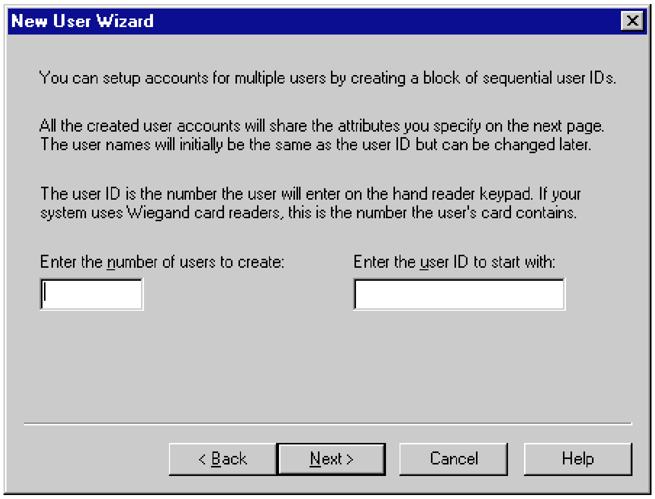
□ Special Enrollment

● Add multiple new users

Click the *Radio* button by *Add Multiple Users*, and then click the *Next* button.

Number of Users to Add and Starting ID

After you choose to add multiple users at once on the first screen of the *New User Wizard*, you see this screen.



You can setup accounts for multiple users by creating a block of sequential user IDs.

All the created user accounts will share the attributes you specify on the next page.
The user names will initially be the same as the user ID but can be changed later.

The user ID is the number the user will enter on the hand reader keypad. If your system uses Wiegand card readers, this is the number the user's card contains.

Enter the number of users to create:

Enter the user ID to start with:

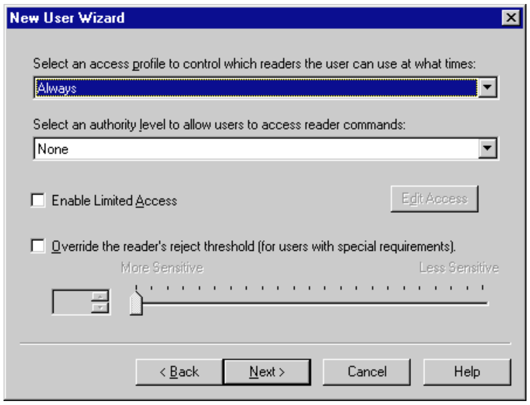
Number of users to create: Enter the number of users you want to add.

User ID to start with: Enter the starting user ID number. Use the number of digits that you would like for the final ID. For example, if you always want a five-digit ID number and you want to start with *1*, enter 00001 rather than just *1*. If you enter *00001*, HandNet will use *00002* next, then *00003*, and so on. If HandNet finds that a number is already used, if will skip that number and use the next available number. For example, if you enter *1000* as the starting number and *1000* through *1020* are all used, HandNet will automatically skip these numbers and start at *1021*. When the program adds the numbers at the end of the process, it lets you know if it had to skip any existing ID numbers.

However, do not begin an ID with zero (0) if you are going to enroll the user with the command menus on the reader. HandNet lets you enroll a user by either picking *Enroll* from the *Reader* menu, or by using the *Command* menus on the reader. If you are going to use the *Command* menus on the reader, the ID number should not begin with zero (0). While HandNet distinguishes between *5* and *0005*, the process of adding a user from the reader command menu does not. This means that if you create a user with an ID of *0005* in HandNet and try to enroll that user with the command menus on the reader, when you type *0005*, the reader thinks you are enrolling User Five, and this will not correspond with *0005* in HandNet. If you are going to use *Enroll* on the *Reader* menu, you can begin an ID with zero (if you are never going to begin an ID with zero, this might be a good choice for a duress code if you use one; see page 47 for more about duress codes).

Security Options

This screen controls what this user has access to and when.



New User Wizard

Select an access profile to control which readers the user can use at what times: Always

Select an authority level to allow users to access reader commands: None

□ Enable Limited Access

□ Override the reader's reject threshold (for users with special requirements).

After you click *Next* on this screen, HandNet adds the new users.

Select an access profile to control which readers the user can use at what times: Click this entry for a list of available access profiles. If these users can use all readers at all times, choose *Always*. If you do not want these users to be able to use any readers at this point, choose *Never*. For other access, select the appropriate profile. You must set access profiles up before they are available here; see page 67 for more about setting up access profiles.

Select an authority level to allow users to access reader commands: This determines what the users can do at the reader. For most users, *None* is the appropriate choice.

Each higher level gives access to the lower levels as well. For example, users with an authority level of four can also use the *Level 1, 2* and *3* menus. Except for recalibrating the reader (part of *Level 1*), and enrolling a user if you have not purchased the upgrade to the full feature set, HandNet can control every setting in the reader, so there is generally no need to control settings through the control menus in the reader.

None: This lets the reader gain access through the reader, but not use the command menus in the reader to change the reader's settings. This choice is appropriate for most users.

(1) Service: This lets you recalibrate the reader and change the reader's status display.

(2) Setup: This lets you control reader setup issues including how the reader is connected to your computer network, what language the reader displays in, the date/time, etc.

(3) Management: This lets you list users.

(4) Enrollment: This lets you add or remove users.

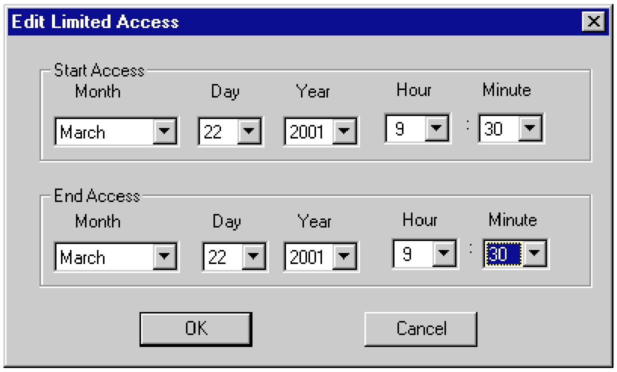
(5) Security: This lets you control the passwords for the reader menus, change time zones, enroll users who do not need hand access, etc.

See the HandKey manual for more on directly changing settings through the reader.

Limited Access

Enable limited access: This gives a user access for a specific date range. For example, suppose a contractor or temporary employee was going to be working in your building for a month. Or suppose an employee gave notice that s/he was leaving for a new job in two weeks. Once this period was over, you would not want these users to have access. Rather than having to remember to disable the user on the appropriate date, this option lets you set a start and end date/time so the user is automatically enabled and disabled at the appropriate points.

To set up start and end date/times, check the box by this button and then click the *Edit Access* button (this button only works if you have checked the box). This takes you to the *Edit Limited Access* screen:



Edit Limited Access

Start Access

Month	Day	Year	Hour	Minute
March	22	2001	9	30

End Access

Month	Day	Year	Hour	Minute
March	22	2001	9	30

To change either start or end date or time, click the corresponding entry and pick from the list that comes up.

This option is disabled if you have not purchased the license upgrade to the full feature set of Version 2.0.

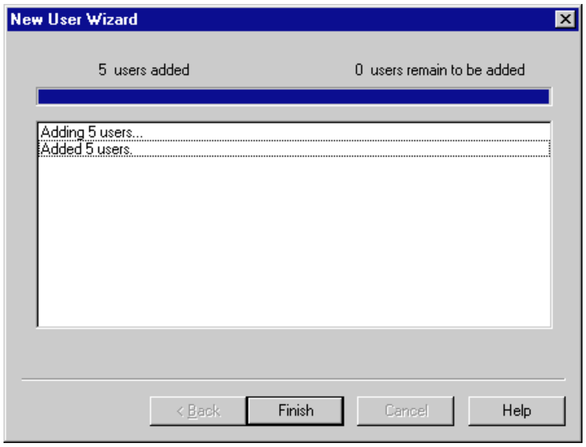
This option is NOT for limiting access to specific readers or for specific times of the day; to control that, use the *Access Profiles* entry.

Override the reader's reject threshold (for users with special requirements): Never change this option when adding multiple users at once. For users with a physical condition like arthritis that prevents them from placing their hands on the reader in exactly the same way each time, this option lets you control how exact the hand match must be for the reader to grant access. Only change this for individual users who are having trouble gaining access, never for a whole group of users at once.

If you later discover that a user is having trouble getting access consistently, go to the *Security* tab in the *User Properties* and change this entry there; see page 92. You would check this box and then slide the pointer further to the right (the *Less Sensitive* side). If a user has a really severe hand condition, it is possible to give access without hand recognition, but because this offers reduced security, that should only be a last resort; see *Adding a User Who Has Access Without Hand Recognition* on page 74 for more on this.

Progress Bar

This is the final screen in the process of adding new users. If you are adding a large number of users, it gives you an idea of how much longer the process will take.



Adding 5 users...
Added 5 users.

If HandNet tries to add ID numbers that are already used, you see messages about those numbers being skipped (this will not changed the number of new users that are added).

What to Do Next

After you click *Finish* to leave the screen above, you need to enroll the users before they have access; see page 87. You will typically also want to rename the users since this process uses the ID number for the name; page 90. And if you created custom user entries, you will want to go to the *Custom* tab in *User Properties* to fill these entries in for each user; see page 94.

* * * * *

Teaching Users How to Place Their Hands on Readers

Correct Hand Placement

Because the reader is looking at the shape of the hand, it is important that you place your hand on the reader the same way every time. When you put your hand on the reader, do this:

- If you are wearing a ring, make sure the stone is up in its normal position.
- Slide your hand forward onto the platen (moving forward like a plane would land at the airport; not straight down like a helicopter would land). Place your hand gently and comfortably; there is no need to apply pressure.
- Keep your hand flat. You should feel the platen with your palm and with the bottom of your fingers.
- Once you hand is flat on the platen, gently close your fingers so they touch against the finger pins. Again, there is no need to apply pressure or press hard. Watch the lights on the hand diagram on the top of the reader; if a light stays on, that finger is not making proper contact with the pin.

Left Hand Placement

If you have been enrolled with your left hand, follow the instructions above, but put your left hand palm up on the reader. The back of your hand should be as flat as possible against the platen.

* * * * *

Enrolling Users

Before a user can have access, you must take the user to a reader and have the reader create an image or template of the user's hand. If you have purchased the upgrade to the full feature set, you can start this process using *Enroll* on the *Reader* menu. If you have not purchased this upgrade, you must use the reader command menus to start the enrollment process.

Using the Enroll Option on the Reader Menu

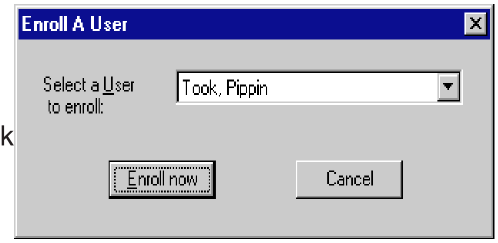
Before you enroll a user, add the user in HandNet; see page 76. You should also teach the user about correct hand placement; see page 86.

1. If the *Network* window is not open, press *CTRL-N* to open it.

2. In the *Network* window, click the reader to enroll the user at.

3. Click the *Reader* menu, and click *Enroll*. You see a screen like this:

4. If the user to enroll is not shown, click the entry and pick the user's name. Then click *Enroll now*.


Enroll A User

Select a User to enroll: Took, Pippin

5. The reader asks the user to place and remove his/her hand three times (if it asks for the hand more than three times, the user is not placing his/her hand consistently; go over the instructions for correct hand placement).

Unless you get a message indicating that there was a problem, the user is now enrolled.

Manually Enrolling Users Using the Reader Command Menus

Before you enroll a user, add the user in HandNet; see page 76. You should also teach the user about correct hand placement on page 86.

1. Check the list of users to make sure you have an authority level of four or higher. If you have an authority level of none, one, two, or three, you cannot do this (to change your authority level, double-click your name on the list of users, click the *Security* tab, click the *Authority Level* entry, and select the appropriate level).

2. Go to the reader to be recalibrated, and enter command mode on the reader:

   If you have a HandKey II or HandKey CR reader: Press *CLEAR*, and then press *ENTER*.

   If you have an ID3D HandKey reader: Press # AND * (you can press them at the same time, or one after the other).

   The display on the reader should look like this:

```
      READY
    * :
```

3. Type your user ID number (the same one you enter to get access through the reader), and press *ENTER* or *#.* The reader asks you to place your hand. Once it recognizes your hand, this display looks like this:

```
ENTER PASSWORD
```

4. Type *4* and press *ENTER* or *#* (this is the standard password for the *Enrollment* menu in the reader; if you have changed this on the *Passwords* screen in the *Reader Properties*, enter the password you have set up).

   If you have a HandKey II or HandKey CR reader: The display should now look like this:

```
   ADD USER
*  NO     YES #
```

   If you have an ID3D HandKey reader: The display should now look like this:

```
 ENROLL USER
*  NO     YES #
```

   If the reader shows the *READY* screen again instead of this screen, then either you placed your hand improperly or you do not have the rights to do this; carefully check step one again.

5. Press the *YES / #* button. This display should now look like this:

```
ID?
:
```

6. Type the ID number of the user to enroll and press *ENTER* or *YES / #*. The display should now look like this:

```
** PLACE HAND **
    1/3
```

7. Have the user place his/her hand on the reader. The reader will ask the user to remove the hand and place it again. The reader should ask the user to place his/her hand three times; if it asks for the hand more than three times, the user is not placing his/her hand consistently; go over the instructions for correct hand placement.

   Once the user has correctly placed the hand three times, the reader asks for the time zone:

```
ENTER TIME ZONE
    (0)?:
```

8. When the user has access to this and other readers is controlled by the access profile you have assigned in the user's properties, so just press *ENTER* or *YES / #.*

9. The reader briefly flashes the message *User Enrolled* and then returns you to the *Add User* or *Enroll User* display. Enroll another user if needed, or press the *CLEAR* button to leave the *Enrollment* menu and return to the reader to its normal display.

* * * * *

Changing Users

Overview

QUICK STEPS

Changing Users

1. If the user window is not shown, press *CTRL-U* or pick *Users* from the *View* menu.
2. Double-click the user to change information. This takes you to the *General* tab in the *User Properties* (you can also click the user once and then pick *Properties* from the *User* menu).
3. Click the tab that has the information you want to change:
   To change the user's name or ID: this is on the *General* tab.
   To change the users access level, authority, limited access, or the reader's sensitivity: Click the *Security* tab.
   To change Custom entries: Click the *Custom* tab.
4. Change information as needed ant then click *OK*.

Renaming Users

1. If the user window is not shown, press *CTRL-U* or pick *Users* from the *View* menu.

2. Double-click the user to rename. This takes you to *User Properties*.

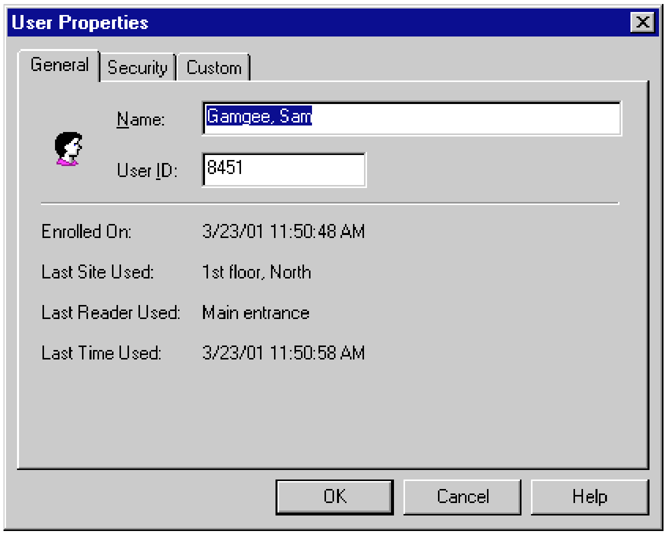
3. Type the new name, and then press *ENTER* or click *OK*.

Alternate Methods

Right-click the user's name and pick *Rename* from the menu that pops up; click the user once and pick *Rename* from the *View* menu; or click the user once, pause for long enough so the computer will not think you are double-clicking, and then click directly on the user's name.

User Properties, General

The *General* tab in *User Properties* lets you change the user's name or ID. It also shows when the user last accessed a reader.



User Properties

General | Security | Custom

Name: Gamgee, Sam

User ID: 8451

Enrolled On: 3/23/01 11:50:48 AM

Last Site Used: 1st floor, North

Last Reader Used: Main entrance

Last Time Used: 3/23/01 11:50:58 AM

Name: Enter the user's name.

If you want to sort the list of users by last name: Enter the last name first. For example, if the user's name is Sam Gamgee, you would enter *Gamgee, Sam*.

If you have two users with the same name: You must enter a unique name for each user. If two users have the same name, you might add a middle initial, or you might add a job description after each. For example, if you have two users named John Jones, you might enter something like *Jones, John (engineer)* and *Jones, John (maintenance)*.

ID Number: If you change a user's ID, be sure to let the user know. The user will not be able to gain access through any reader without knowing the correct ID.

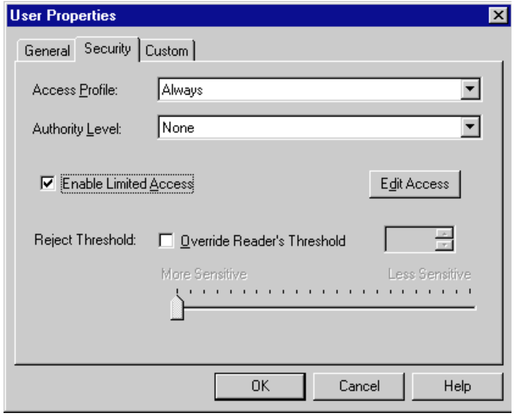
Each number must be unique (if you could give the same number to two users, the reader would not know which was trying to gain access). Longer numbers are slightly more secure, but four or five digits are generally adequate in context where user's must enter the number. You may enter up to ten digits if you do not use a duress code, or up to nine digits if you do use a duress code. If you use a duress code, make sure that you do not create an ID that begins with that digit; see page 47 for more about duress codes. If you have set up an *ID length* on the *Settings* tab in the *Reader Properties*, make sure that you do not create an ID that is longer than this; see page 47 for more about ID length.

If you use Wiegand card readers: Enter the ID number stored on the card.

Do not begin an ID with zero (0) if you are going to enroll the user with the command menus on the reader: HandNet lets you enroll a user by either picking *Enroll* from the *Reader* menu, or by using the command menus on the reader. If you are going to use the command menus on the reader, the ID number should not begin with zero (0). While HandNet distinguishes between 5 and 0005, the process of adding a user from the reader does not. This means that if you create a user with an ID of 0005 in HandNet and try to enroll that user with the command menus on the reader, when you type 0005, the reader thinks you are enrolling user 5; this will not correspond with 0005 in HandNet. If you are going to use *Enroll* on the *Reader* menu, you can begin an ID with zero (if you are never going to begin an ID with zero, this might be a good choice for a duress code if you use one).

User Properties, Security

The *Security* tab controls what this user has access to and when.



Access Profile: Always

Authority Level: None

☑ Enable Limited Access

Reject Threshold: □ Override Reader's Threshold

Select an access profile to control which readers the user can use at what times: Click this entry for a list of available access profiles. If this user can use all readers at all times, choose *Always*. If you do not want the user to be able to use any readers at this point, choose *Never*. For other access, select the appropriate profile. You must set access profiles up before they are available here.

Select an authority level to allow users to access reader commands: This determines what the user can do at the reader. For most users, *None* is the appropriate choice.

Each higher level gives access to the lower levels as well. For example, a user with an authority level of four can also use the *Level one, two* and *three* menus. Except for recalibrating the reader (part of level 1), and enrolling a user if you have not purchased the upgrade to the full feature set, HandNet can control every setting in the reader, so there is generally no need to control settings through the reader menus.

None: This lets the reader gain access through the reader, but not use the command menus in the reader to change the reader's settings. This choice is appropriate for most users.

(1) Service: This lets you recalibrate the reader and change the reader's status display.

(2) Setup: This lets you control reader setup issues including how the reader is connected to your computer network, what language the reader displays in, the date/time, etc.

(3) Management: This lets you list users.

(4) Enrollment: This lets you add or remove users.

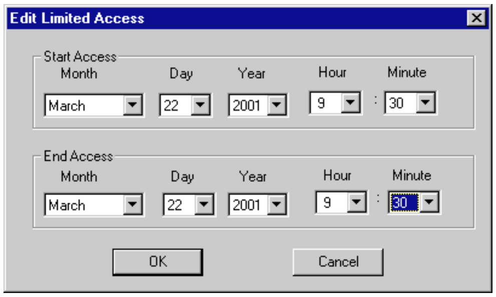
(5) Security: This lets you control the passwords for the reader menus, change time zones, enroll users who do not need hand access, etc.

See the HandKey manual for more on directly changing settings through the reader.

Limited Access

Enable limited access: This gives a user access for a specific date range. For example, suppose a contractor or temporary employee is going to be working in your building for a month. Or suppose an employee gives notice that s/he is leaving for a new job in two weeks. Once this period is over, you would not want these users to have access. Rather than having to remember to disable the user on the appropriate date, this option lets you set a start and end date/time so the user is automatically enabled and disabled at the appropriate points.

To set up start and end date/times, check the box by this button and then click the *Edit Access* button (this button only works if you have checked the box). This takes you to the *Edit Limited Access* screen:



Edit Limited Access

Start Access
Month: March | Day: 22 | Year: 2001 | Hour: 9 : Minute: 30

End Access
Month: March | Day: 22 | Year: 2001 | Hour: 9 : Minute: 30

To change either start or end date or time, click the corresponding entry and pick from the list that comes up.

This option is disabled if you have not purchased the license upgrade to the full feature set of Version 2.0.

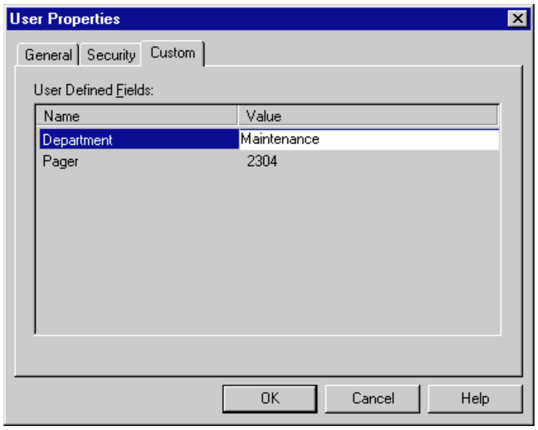
This option is NOT for limiting access to specific readers or for specific times of the day. To control that, use the *Access Profiles* entry.

Override the reader's reject threshold (for users with special requirements): For users with a physical condition like arthritis that prevents them from placing their hands on the reader in exactly the same way each time, this option lets you control how exact the hand match must be for the reader to grant access.

If a user is having trouble getting access consistently, check this box and then slide the pointer further to the right (the *Less Sensitive* side). If a user has a really severe hand condition, it is possible to give access without hand recognition, but because this offers reduced security, that should only be a last resort.

User Properties, Custom

You only see entries on the *Custom* tab if you have set up custom user entries (see page 97 for more on creating custom user entries). The entries on this screen vary depending on what you have set up; the entries on your screen will probably be completely different from the examples show below.



Name	Value
Department	Maintenance
Pager	2304

To change a value, click the item in the *Value* column and then enter the correct value.

When You Are Done

When you are done changing *User Properties*, click the *OK* button at the bottom of the screen.

* * * * *

Changing Access for Many Users at Once

Import TZ Option

Import TZ on the *File* menu lets you change the access profile to *Always* or *Never* for many users based on information in a text file (this file would be created with some other program).

Caution

If you use this option, be aware that there are security risks involved: if you mistype a number in the file, you could easily give full access to a different user than you intended. And unlike most other changes in HandNet, the fact that this option is used and the fact that a user's access is changed is NOT reflected in the activity log, so you will not have any record of the change. In most contexts, it is more appropriate to change user access through the *Security* tab in *User Properties*; see page 92.

File Format

Each line of the file would list a user ID number followed by a comma, and then either 0 (zero) to set that user's access profile to *Always*, or sixty-one, to set that user's profile to *Never* (currently, you cannot use the file to switch to any other profile). For example, suppose your text file looked like this:

```
1001, 0
1002, 0
1003, 61
21345, 0
43567, 61
```

If you import this file, HandNet would set the access profile to *Always* for users with the IDs of 1001, 1002, and 21345, and it would set the profile to *Never* for users with IDs 1003 and 43567. It would not change the access profiles for any other users. If HandNet could not find a user with the corresponding ID number, or if you have something other than zero or sixty-one after the comma, HandNet would skip that line. It would not give you any message or tell you the line was skipped. If you have any lines that did not match the format above (for example, if you do not have the comma between the ID and the zero or sixty-one), HandNet would give a message at the end of the process that tells you how many bad records are ignored. If other lines are in the correct format, HandNet would still process them successfully.

You do not see any message or progress bar during the import process. If you are importing many records, you could have some delay where it looks like nothing is happening. For example, on a 166MHz processor, importing 1,000 records takes slightly over thirty seconds; you would not see any activity while this is happening.

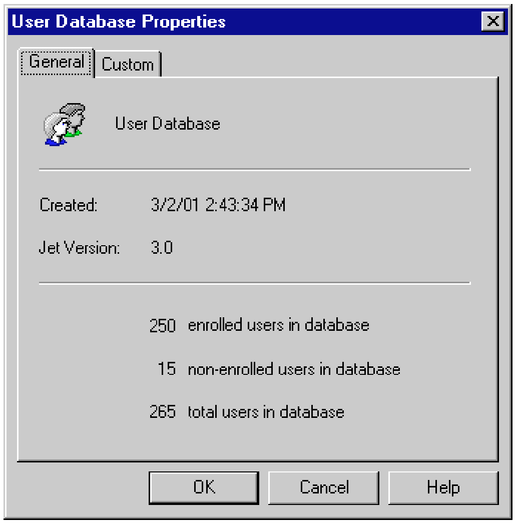
* * * * *

User Database Properties

What Information Is Shown

This screen shows general information about the whole user database, including the date it is created, the Version number, the number of enrolled users and number of non-enrolled users, and the total number of users in the database. You do not typically need this information during normal use of the program. However, if you want to add or change custom user entries, you would come to this screen and then click the *Custom* tab.

You get to this screen by picking *DB Properties* from the *User* menu.



User Database

Created: 3/2/01 2:43:34 PM

Jet Version: 3.0

250 enrolled users in database

15 non-enrolled users in database

265 total users in database

* * * * *

Adding Custom User Entries

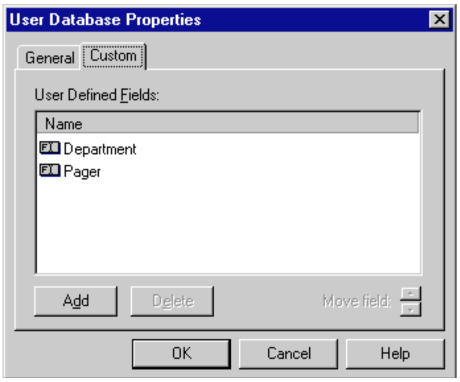
To collect additional information about users in HandNet, you can add additional custom entries. HandNet then asks for this information on the *Custom* screen of *New User Wizard* (see page 80) and the *Custom* tab in the *User Properties* (page 94).

What you might want to collect could vary widely depending on how you are using HandNet: emergency phone numbers, employment start dates, department, pager number. You can add as many entries as you need.

The information that you add in custom entries is only available on the screen, either in *User Properties* or on the list of users (available by picking *Users* from the *View* menu). Currently, HandNet does not include custom user information on any reports.

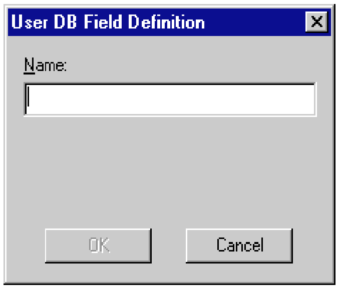
Getting to the List of Custom Entries

1. Click the *User* menu and then click *DB Properties*.
2. Click the *Custom* tab. You will see a screen like this, but with different entries.



Adding a New Entry

To add a new custom entry, click the *Add* button. You see this screen:



Type the name of the field or entry to add and press *ENTER* or click *OK*. Make sure that you enter the name of the entry correctly; once you continue, you cannot change the name.

Deleting a Custom Entry

Click the entry in the list and click *Delete*. Be sure that you are deleting the correct item; the program will not ask you to confirm the deletion, and once you delete a custom entry, all information that you have entered for users in that entry is gone. For example, suppose you create an *Emergency Phone Number* entry and entered phone numbers for all of your users. If you delete emergency phone numbers here, all of the phone numbers that you enter would be gone and there would be no way to get them back unless you make a backup of your HandNet information.

Changing the Order of the Entries

On the *Custom* screen in the *User Properties*, the entries in the same order as they are listed here. To change the order of the entries, click the entry to move and then click the up or down arrows next to the words *Move field*.

* * * * *

Converting Users from MS-DOS HandNet or HandNet+

If you have been using one of our MS-DOS programs (either HandNet or HandNet+), *Convert HandNet+...* on the *File* menu lets you import your users so you do not have to enter and enroll them again. This option brings in each user's name, ID number, authority level, and reject threshold.

If you have been using an older Version of HandNet for Windows, you do not need to do anything to convert that information.

To Convert HandNet Plus Users

1. If you have been using HandNet rather than HandNet Plus, follow the steps below to convert your user information from HandNet to HandNet Plus format.
2. Pick *Convert HandNet+* from the *File* menu.
3. If you have installed HandNet+ somewhere other than in C:\HNET, click the *Browse* button and go to the directory where HandNet+ is installed. Then click the *Open* button.
4. Click the *Convert* button. The HandNet+ database is converted to HandNet for Windows™ format.
5. This con Version does not bring in the access profiles for the users, so when this is done you must assign an access profile to each user on the *Security* tab in *User Properties*.

To Convert MS-DOS HandNet Users

If your DOS Version of HandNet is in the standard /HNETdirectory: Press *F1* while in HandNet to pop up the help. In the index, type *convert* and open the topic on converting HandNet+ information. In this topic there is a button that automatically does this process for you.

If your DOS Version of HandNet is NOT in the standard /HNET directory:

1. Copy the *convert.exe* file from the HandNet for Windows directory to the directory the MS-DOS Version of HandNet is located. The standard location for HandNet for Windows is *C:\Program Files\Schlage Biometrics, Inc.\HandNet for Windows.* For example, to copy the convert file from this directory to *c:\hnet*, you would type:

```
copy c:\progra~1\recogn~1\handne~1\convert.exe c:\hnet\
```

2. Switch to the directory the MS-DOS Version of HandNet is in. For example, to switch to the *\hnet* directory, you would type *cd\hnet* and press *ENTER*.
3. Make a backup copy of the file that contains your user information. This file is called *id_dbase.dat*. For example, you might type:

```
copy id_dbase.dat id_dabase.bak
```

4. Type *convert* and press *ENTER*. This should convert the information to HandNet Plus format. Once you have done this, you are ready to import the information into HandNet for Windows using the steps described above.

* * * * *

Importing and Exporting Users

Getting User Information from a Reader

If you have already set up users in a reader that you are connecting to HandNet, you do not need to recreate those users. You can get user information from the reader by doing this:

1. Pick *Network* from the *View* menu (or type *CTRL-N*).
2. On the list of readers in the right pane of the *Network* window, select the reader(s) to get user information from.
3. Click the *Reader* menu, click *Upload*, and click *Users*.
4. The program asks you to confirm that you want to upload users from the reader; click *Yes* to continue.

Importing Users from Another Copy of HandNet

You only need to import users if you have readers connected to several different computers (each with its own copy of HandNet) and if users added to one system need to be available on the others. If all of your readers are connected to a single copy of HandNet, you do not need this feature.

The export feature is only available if you have purchased the upgrade to the full feature set of Version 2.0.

Setting Up Import Settings First

Make sure that you select the correct choices for what to import on the *User Import/Export* tab in *System Settings* before you try to import; see page 28. When HandNet imports, it empties the *Import* file, discarding those user records that do not meet the conditions you have checked there.

Importing Users From Another Computer

1. On the computer where you exported users, go to the HandNet directory and copy the file *export.mdb* to a floppy disk (you could also copy this file to a network drive, attach it to an e-mail, etc.).
2. Rename the file on the disk (or in the new location) to *import.mdb*.
3. Put this *import.mdb* file into the HandNet directory on the computer where you want to import users.
4. If you do not have that copy of HandNet set up to import automatically, pick *Import Users* from the *File* menu (if you have the *Enable* box under *Auto Import* checked on the *User Import/Export* tab in *System Settings*, HandNet starts importing as soon as it finds the *import.mdb* file in the directory; see page 28).

The activity window lists each user that is added, deleted or changed.

Exporting Users to Another Copy of HandNet

You only need to export users if you have readers connected to several different computers (each with its own copy of HandNet) and if users added to one system need to be available on the others. If all of your readers are connected to a single copy of HandNet, you do not need this feature.

The export feature is only available if you have purchased the upgrade to the full feature set of Version 2.0.

Automatically Exporting Users

HandNet can automatically export users when you create, enroll, change or delete users. When HandNet exports users is controlled by the items in the *Export* column on the *User Import/Export* tab in *System Settings*; see page 28.

Manually Exporting Users

1. Go to the *Users* window.
2. Select the users to export. To select multiple users that are together on the list, click the first user, hold the *SHIFT* key down, and click the last user that you want to select. To select multiple users that are not together on the list, click the first user to select, hold the *CTRL* key down, and click each other user that you want to select.
3. Right-click (this brings up a menu).
4. On the menu, point to *Export*, and then pick *Selected* (or pick *All* to export every user in the list whether selected or not).

You will see a message with a progress bar that indicates that the users are being exported (if you only selected a few users, this may vanish almost instantly). Once this box disappears, the export process is done.

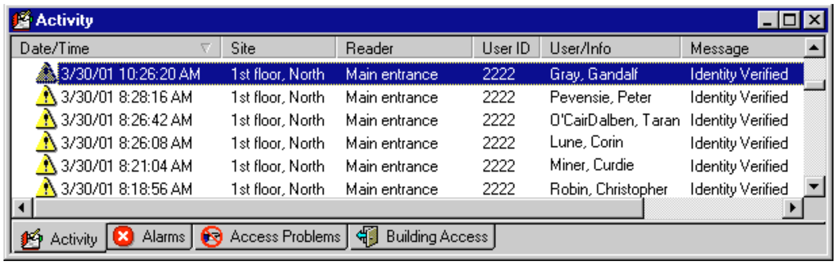
To import these users on the other computer, see the instructions for *Importing Users from Another Copy of HandNet* on page 99.

* * * * *

Monitoring Ongoing Activity

Activity Window

The *Activity* window lists everything that happens at any reader connected to HandNet, and any change made in the HandNet program. To open this window, pick *Activity* from the *View* menu, or press *CTRL-A*.



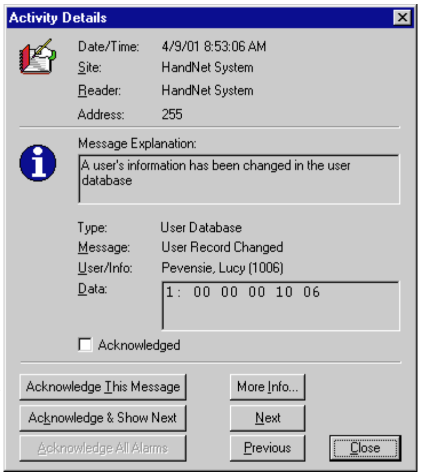
Date/Time	Site	Reader	User ID	User/Info	Message
3/30/01 10:26:20 AM	1st floor, North	Main entrance	2222	Gray, Gandalf	Identity Verified
3/30/01 8:28:16 AM	1st floor, North	Main entrance	2222	Pevensie, Peter	Identity Verified
3/30/01 8:26:42 AM	1st floor, North	Main entrance	2222	O'CairDalben, Taran	Identity Verified
3/30/01 8:26:08 AM	1st floor, North	Main entrance	2222	Lune, Corin	Identity Verified
3/30/01 8:21:04 AM	1st floor, North	Main entrance	2222	Miner, Curdie	Identity Verified
3/30/01 8:18:56 AM	1st floor, North	Main entrance	2222	Robin, Christopher	Identity Verified

Only the first two tabs at the bottom of this screen (*Activity* and *Alarms*) are always there. The others are merely examples of custom activity views that you can create as needed; see *Creating Custom Activity Views* on page 104.

Rearranging or Resizing Columns in the Activity Window

To move any column, click on the column heading and hold the mouse down. With the mouse held down, drag the column heading to the left or right.

Getting More Detail about an Activity in the Activity Window



Date/Time: 4/9/01 8:53:06 AM
Site: HandNet System
Reader: HandNet System
Address: 255

Message Explanation:
A user's information has been changed in the user database

Type: User Database
Message: User Record Changed
User/Info: Pevensie, Lucy (1006)
Data: 1: 00 00 00 10 06

☐ Acknowledged

When you double-click on an activity in the *Activity* window, you get a screen like this that tells more about that activity.

Date/Time: This shows the date and time when the activity occurred. The date is listed in month/day/ year order, and the time lists hours/minutes/seconds.

Site: If this activity happened at a reader, this shows the name of the site the reader is associated with.

Reader: If this activity happened at a reader, this shows the reader's name.

Address: If this activity happened at a reader, this shows the reader's address; this address should correspond with the name of the reader listed above. If this activity occurred in the HandNet program, this says *255*.

Message Explanation: This shows some additional explanation of the message. For more explanation, see the complete list of activity messages starting on *Activity Messages* on page 116.

Type: Each message falls into one of ten categories. When you are creating an activity filter or custom activity report, you can limit your report or activity view to specific types of messages; see *Message Types* on page 111 for more detail.

Message: This shows the same message that you saw on the list in the *Activity* window.

User/Info: If this message is associated with a particular user, this shows the user's name and ID number.

Data: This shows technical detail about the message that is not relevant to your use of the program. This is occasionally useful to support in debugging a problem.

Acknowledged [checkbox]: This shows whether this message has been acknowledged yet. You cannot uncheck this box once it is marked. You also can check the box directly; you must use one of the three *Acknowledge...* buttons below.

Buttons on the Activity Details Screen

Acknowledge This Message: This marks the message as acknowledged. After the message on the activity or alarm list, you will see *:ACK* followed by the name of the operator who acknowledged the message and the date/time when it was acknowledged. If this is an alarm, this also shuts the alarm off.

Acknowledge & Show Next: This acknowledges the current message and shows the next message. By next, we mean more recent in time; that is, the message above the current message on the activity list.

Acknowledge All Alarms: This button is disabled unless there is an alarm that has not been acknowledged yet. You might use this button if you see several related alarms on the list and you want to acknowledge them all at once.

More Info: This brings up the online help.

Next: This shows the message that occurred more recently in time, that is, the message directly before this on the activity list.

Previous: This shows the message that occurred before this message in time, that is, the message directly after it on the activity list.

* * * * *

Getting to and Acknowledging Alarms

Getting to the Alarms List

Alarms are listed with the rest of the activity in the *Activity* window, but we have also provided a separate view with just the alarms. To see this view, click the *Alarms* tab at the bottom of the *Activity* window.

Acknowledging an Alarm

If an alarm is triggered in HandNet, do this to acknowledge it and turn it off.

1. If the *Activity* window is not shown, press *CTRL-A* or pick *Activity* from the *View* menu.

2. Double-click the alarm message with the bell icon next to it (you can see it both in the regular activity view or by clicking the *Alarm* tab at the bottom of the window).

3. Click one of the *Acknowledge...* buttons at the bottom left of the window (you cannot just click the checkbox by the word acknowledged; you must click one of the buttons). After the message on the *Activity* or *Alarm* list, you will now see *:ACK* followed by the name of the operator who acknowledged the message and the date/time it was acknowledged.

4. Take whatever action is appropriate in response to the alarm.

What Situations Cause Alarms

Which situations trigger alarms depends on which items are checked on the *Alarms* tab in the *System Settings*; see page 25.

* * * * *

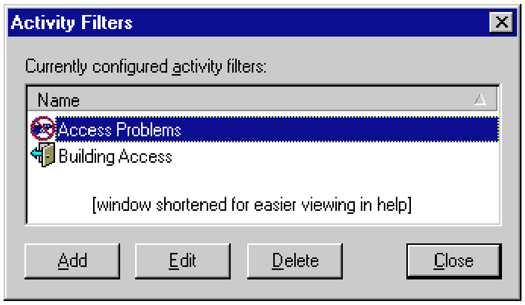
Creating and Printing Custom Activity Views

Creating a Custom Activity View

The main *Activity* window lists all activity that occurs: every access from every reader, every failed access, every user addition and enrollment, every alarm, and so on. Sometimes its useful to see less than this. For example, if you wanted to identify users who were having access problems, you might want to see only the *Identity Unknown* and *Access Denied* messages (the messages that can occur when someone enters a valid ID but then does not get a match on the hand). Or if you want to identify who has come in the building, you might want to see only *Identity Verified* messages and only for the readers that controlled entrances to the building.

You can create (and print reports on) custom views for these or any other subsets of activity, limiting the view to specific messages, dates, times, users, and/or readers. To create a custom activity view:

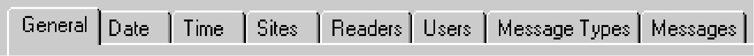
1. Click the *View* menu, and click *Activity Filter*. You see a list of any custom activity views if you have created any yet. This list looks like this, but the *filters* listed will be different.



[window shortened for easier viewing in help]

2. Click the *Add* button to create a new filter (that is, a set of conditions that will filter out only the information you want to see). This takes you to the first *Activity Filter* screen (to change a filter you have already created, click the filter and then click *Edit*).

3. Give the filter a name, associate an icon if you wish, and then go to each tab where you want to include something less than all of the activity.



   Each tab is initially set up to include all information; go to those where you want to limit or filter out particular information. For example, if you only want activity at certain readers, you would go to the *Readers* tab. If you only want certain messages, go to the *Messages* tab. The options on these tabs are explained, starting on page 107.

4. When you have entered all of the conditions needed, click the *OK* button at the bottom of the window.

To start this process, you could also right click on the bar at the bottom of the *Activity* window, and then pick *Add New Filter...*.

Removing a Custom Activity View

This does not remove any activity from HandNet; it only removes the custom view of the activity.

1. Click the *View* menu, and click *Activity Filter*. You will see a list of any custom activity views you have created.

2. Click the view or filter to remove and click *Delete*.

Printing an Activity Report Based on an Activity Window

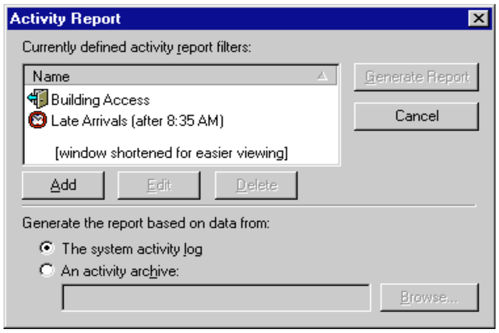
1. Right-click on the bottom bar of the *Activity* window (where the *Activity* and *Alarms* tabs are).

2. Pick *Generate Report*.

3. In the report window that comes up, click the printer icon in the header; see *Printing or Viewing Reports* on page 127 for more detail.

Creating a Custom Activity Report from the Reports Menu

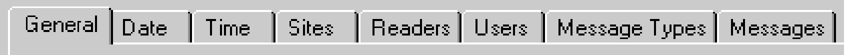
If you have not already created a custom activity view, or if you need to run the report on archived activity, then follow these steps to design the report.


Activity Report
Currently defined activity report filters:
Name
Building Access
Late Arrivals (after 8:35 AM)
[window shortened for easier viewing]
Generate Report
Cancel
Add
Edit
Delete
Generate the report based on data from:
● The system activity log
○ An activity archive:
Browse...

1. From the *Main Menu* bar, click *File*, click *Reports*, and click *Activity....* You see a screen like this (if you created any custom reports they would be listed; your reports may be very different from the samples listed here).

2. Click the *Add* button to create a report (that is, a set of conditions that will filter out only the information you want to see). This takes you to the first *Activity Report* screen (to change a report you have already created, click the filter and then click *Edit*). The screens that you see are identical to those that you see when creating a custom activity view.

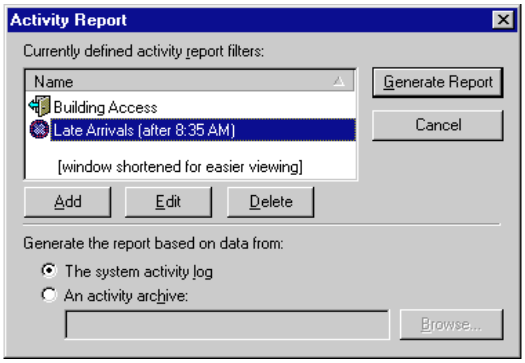
3. Give the report a name, associate an icon if you wish, and then go to each tab where you want to include something less than all of the activity.



Each tab is initially set up to include all information; go to those where you want to limit or filter out particular information. For example, if you only wanted activity at certain readers, you would go to the *Readers* tab. If you only want certain messages, go to the *Messages* tab. The options on these tabs are explained starting on page 107.

4. When you have entered all of the conditions needed, click the *OK* button at the bottom of the window. This returns you to the list of reports.

Printing an Activity Report from the Reports Menu


Activity Report
Currently defined activity report filters:
Name
Building Access
Late Arrivals (after 8:35 AM)
[window shortened for easier viewing]
Generate Report
Cancel
Add
Edit
Delete
Generate the report based on data from:
● The system activity log
○ An activity archive:
Browse...

1. From the main menu, click *File*, click *Reports*, and then click *Activity Reports*. You see a screen like this (if you have created any custom reports they would be listed; your reports may be very different from the samples listed here).

2. If you have not already designed the report, see *Creating a Custom Activity Report* from the *Reports* Menu above for help designing it.

3. Click the report in the list of reports at the top of the window.

4. At the bottom of the window, indicate which activity to generate the report from:

   The system activity log: This includes all the activity that has occurred since the last time you archived activity (and that meets your report conditions).

   An activity archive: This includes all activity that meets your report conditions that is in the archive file that you pick. Click the *Radio* button by this choice, click the *Browse* button, and pick the file. HandNet lists files that have an *.hna* extension. Pick the *Archive* file and click *OK*.

   If the activity that you want is in several archive files, you will have to run the report several times, once for each archive file. If you need the information in a single report, you can export each report to a file and then use another program to combine the reports into a single file.

5. Click the *Generate Report* button. HandNet generates the report and shows it in a new window on the screen.

6. Click the *Printer* icon near the middle of the header to print the report, or click the icon with the envelope to export the content of the report to a file. You can export to a variety of formats including Word, Excel, Lotus 1-2-3, .rtf, text, and others; see *Printing or Viewing Reports* on page 127 for more detail.

   If the printer icon is disabled and grayed-out, you do not have a printer set up yet on this computer (to set up a printer, go to the Windows *Start* menu, highlight *Settings*, pick *Printers*, and click *Add Printer*).

7. To close the *Report* window when done, click the *X* in the upper-right corner of the window.

* * * * *

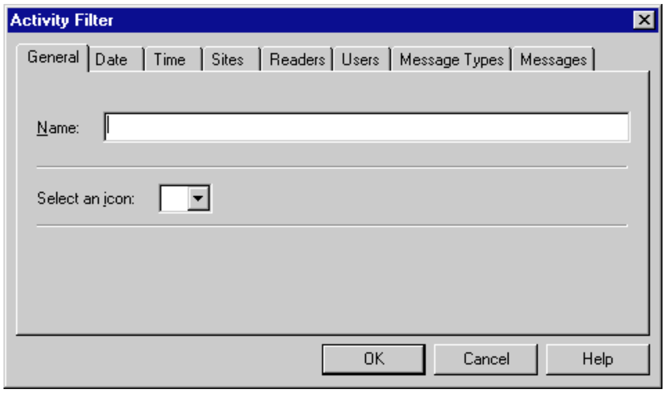
Condition Screens for Creating Custom Activity Views/Reports

When you create an activity filter (that is, a custom view of your activity; see page 104), or when you design a custom activity report (see page 105), you see the screen shown below.

Each tab is initially set up to include all information; you only need to go to those tabs where you want to limit or filter out particular information. For example, if you only want activity at certain readers, you would go to the *Readers* tab. If you only want certain messages, you would go to the *Messages* tab.

General

This screen contains the name and icon associated with activity filter or report.



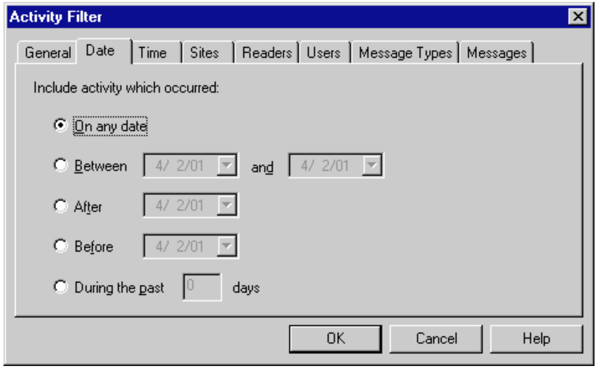
Name: Enter a name that describes the conditions that determine what activity will be included.

Icon: If you want an icon associated with the this activity view/report, click the this entry. You do not have to choose an icon if you do not want to. If you do not want an icon, do not pick an icon; once you pick one, you cannot go back to having no icon.

Do not click *OK* until you have gone to the other tabs and set up those conditions that limit the activity.

Date

This screen lets you limit the activity you see to certain dates.



Include activity which occurred:

● On any date

○ Between 4/ 2/01 and 4/ 2/01

○ After 4/ 2/01

○ Before 4/ 2/01

○ During the past 0 days

On any date: This includes activity from any date that is in the activity file. This is always the initial choice when you create a new report or activity filter.

Between: This includes any activity between the dates entered or on those dates. For example, if you chose *Between 05/01/01 and 05/31/01*, activity from both 05/01 and 05/31 would be included along with the activity in between.

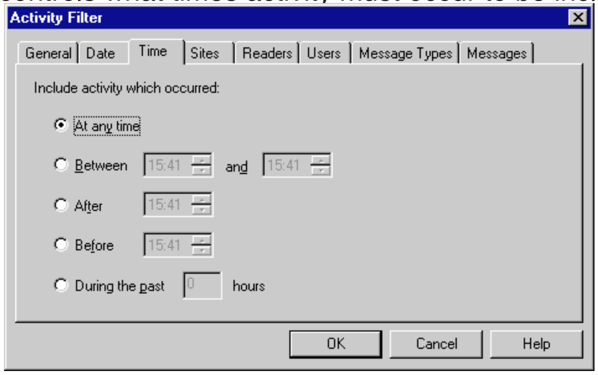
After: This includes activity that is after the date that you enter, but not activity that is on or before that date. For example, if you enter *05/01/01*, you would see activity from 05/02 on, but activity on 05/01 would not be included (if you want the activity from 05/01, you would have to enter *After 04/30*).

Before: This includes activity that is before the date that you enter, but not activity that is on or after that date. For example, if you enter *04/30/01*, you would see activity from 04/29 and before, but activity from 04/30 would not be included (if you want the activity from 04/30, you would have to enter *Before 05/01*).

During the past: This is useful for creating a view that lists only the most recent activity. For example, you might create a view that only listed activity during the past week. If you want to be more precise, this same option is on the *Time* screen so that you could, for example, limit a view to the last twenty-four hours.

Time

This screen controls what times activity must occur to be included.



Activity Filter

General | Date | Time | Sites | Readers | Users | Message Types | Messages

Include activity which occurred:

● At any time

○ Between 15:41 and 15:41

○ After 15:41

○ Before 15:41

○ During the past 0 hours

On any time: This includes activity from any time. This is always the initial choice when you create a new report or activity filter.

Between: This includes any activity between the times entered or exactly at those times. For example, if you chose *Between 12:00 and 13:00*, activity that happened at exactly 12:00 or 1:00, PM along with the activity in between would be included. This goes from the earliest time to the latest time, regardless of which you enter first. For example, if you enter *Between 17:00 and 8:00* (hoping to get activity that was not during normal business hours), you would get the same activity as if you had entered *Between 8:00 and 17:00* (that is, activity that occurred during normal business hours). If you really want activity that is after 5:00 PM and before 8:00 AM, you would have to create two filters: one looking for activity after 17:00 and the other looking for activity before 8:00.

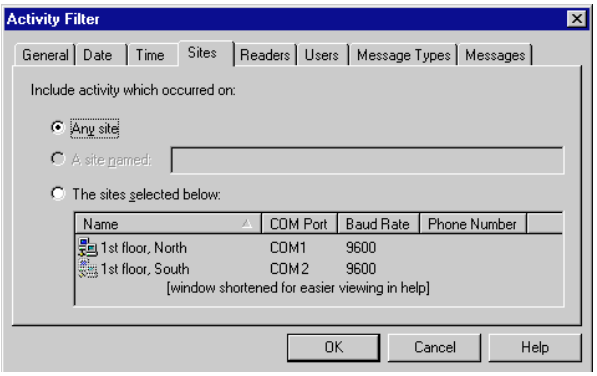
After: This includes activity that is after the time that you enter, but not activity that is exactly at that time. For example, if you enter 12:00, you would see activity from 12:00:01 (that is one second after 12) on, but activity at 12:00:00 or before would not be included.

Before: This includes activity that is before the time that you enter, but not activity that is exactly at that time. For example, if you enter 12:00, you would see activity from 11:59:59 (that is one second before 12:00) on, but activity at 12:00:00 or after would not be included.

During the past: This is useful for creating a view that lists only the most recent activity. For example, you might create a view that only listed activity during the past twenty-four or forty-eight hours (for longer periods, this same option is on the *Date* screen so that you could, for example, limit a view to the past thirty days).

Sites

This screen lets you limit the activity to certain sites.



Include activity which occurred on:

● Any site

○ A site named:

○ The sites selected below:

Name	COM Port	Baud Rate	Phone Number
1st floor, North	COM1	9600	
1st floor, South	COM2	9600	

[window shortened for easier viewing in help]

Any site: Leave this selected to not limit the activity based on site.

A site named: This option is permanently disabled. To get activity for a single site, use the following option and only click one site in the list.

The sites selected below: To limit the report/view to specific sites, click this and then select the sites to include activity from.

To select a single site: Click that site in the list.

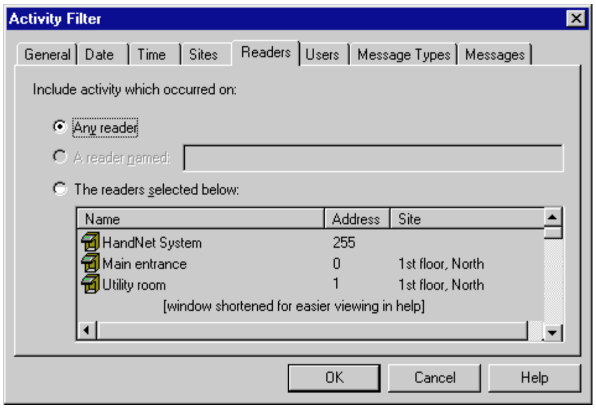
To select multiple sites that are together on the list: Click the first site in the group, hold the *SHIFT* key down, and with the *SHIFT* key down, click the last site that you want to select.

To select multiple sites that are not together on the list: Click the first site to select, hold the *CTRL* key down, and click each other site that you want to select.

If you select specific sites here, make sure you do not select readers from different sites on the *Reader* tab; if you select sites here and select readers from different sites, you will not see any activity with this filter. If you want to select specific readers, select *Any site* on this screen.

Readers

This tab lets you limit to activity that occurred at certain readers. For example, you might want to limit activity only to the readers controlling the entrances to the building so you could see who has come in. Or you might want to limit activity to the readers controlling the most secure areas so you could monitor them more closely.



Include activity which occurred on:

● Any reader

○ A reader named:

○ The readers selected below:

Name	Address	Site
HandNet System	255	
Main entrance	0	1st floor, North
Utility room	1	1st floor, North

[window shortened for easier viewing in help]

Any reader: Leave this selected to not limit the activity based on site.

A reader named: This option is permanently disabled. To get activity for a single reader, use the following option and select only that one reader in the list.

The readers selected below: To limit the report/view to specific readers, click this and then select the readers to include activity from.

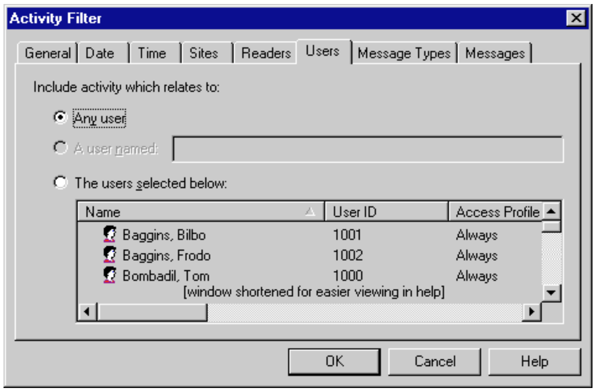
To select a single reader: Click that reader in the list.

To select multiple readers that are together on the list: Click the first reader in the group, hold the *SHIFT* key down, and click the last reader that you want to select.

To select multiple readers that are not together on the list: Click the first reader to select, hold the *CTRL* key down, and click each other reader that you want to select.

Users

This screen lets you limit to activity that occurred for certain users.



Include activity which relates to:

● Any user

○ A user named:

○ The users selected below:

Name	User ID	Access Profile
Baggins, Bilbo	1001	Always
Baggins, Frodo	1002	Always
Bombadil, Tom	1000	Always

[window shortened for easier viewing in help]

Any user: Leave this selected to not limit the activity to particular users.

A user named: This option is permanently disabled. For a single user, use the following option and select only that one user in the list.

The readers selected below: To limit the report/view to specific users, click this and then select the users to include activity for.

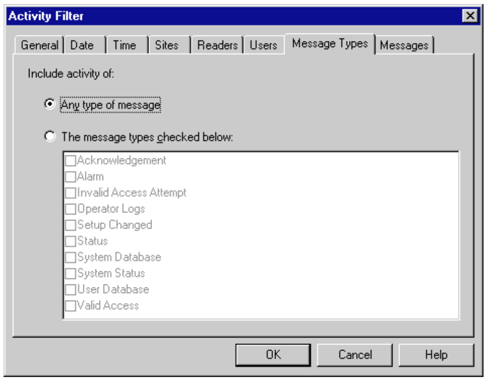
To select a single user: Click that user in the list.

To select multiple users that are together on the list: Click the first user in the group, hold the *SHIFT* key down, and click the last user that you want to select.

To select multiple users that are not together on the list: Click the first user to select, hold the *CTRL* key down, and click each other user that you want to select.

Message Types

This screen lets you limit the activity included to particular kinds of messages. If you need only specific messages within a category, use the *Messages* tab instead.



Include activity of:

● Any type of message

○ The message types checked below:

□ Acknowledgement
□ Alarm
□ Invalid Access Attempt
□ Operator Logs
□ Setup Changed
□ Status
□ System Database
□ System Status
□ User Database
□ Valid Access

Any message: This includes activity regardless of what type of message it generates.

The messages types checked below: Click this and then check any message type to include. You can check more than one box to include multiple types of messages.

Acknowledgement: This does not list anything.

Alarm: This lists any message that generates an alarm. Which messages generate alarms is controlled by your choices on the *Alarms* tab in *System Settings*. If you change which messages generate alarms, messages that did not generate an alarm when they occurred will not be listed, even if they would generate an alarm now.

Invalid Access Attempt: This lists any message where someone tries to get access and cannot. This includes the messages *Identity Unknown, Access Denied, and Access Refused, Time Zone*.

Operator Logs: This lists when operators log in or log out of HandNet, and it lists invalid login attempts. It does not list the addition of new operators or changes to the operator settings; only when each operator uses the system.

Setup Changed: This lists any setup changes made directly using command mode at the reader. For setup changes made through HandNet, use *System Database*.

Status: This lists any messages that tell whether auxiliary input and output is on or off.

System Database: This lists all setting changes made through HandNet. This includes adding or changing sites and readers, changing system settings, changing time zones, holidays and access profiles.

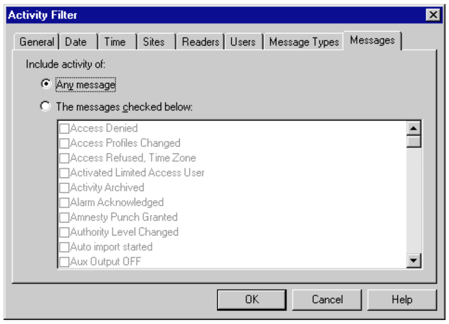
System Status: This lists messages related to when HandNet was started and exited, messages related to enrolling users, messages related to communication problems with readers, and messages related to information being downloaded/uploaded to/ from readers.

User Database: This lists messages related to users being added, deleted, or changed. It does not include messages related to users being enrolled or attempted unauthorized enrollments.

Valid Access: This lists *Identity Verified* messages.

Messages

This screen lets you limit the report or activity view to specific messages. For example, if you were trying to track who came into the building, you might select the building entrances on the *Readers* tab, and then choose only the message *Identity Verified* here. Or if you were trying to track access problems, you might limit the output to the messages *Access Denied* or *Identity Unknown*. If you want all of the messages in a particular category, you may find it easier to use the *Message Types* tab instead.



Activity Filter

Include activity of:

● Any message

○ The messages checked below:

□ Access Denied
□ Access Profiles Changed
□ Access Refused, Time Zone
□ Activated Limited Access User
□ Activity Archived
□ Alarm Acknowledged
□ Amnesty Punch Granted
□ Authority Level Changed
□ Auto import started
□ Aux Output OFF

Any message: This includes activity regardless of what message it generated.

The messages checked below: Check any message to include. See the list of activity messages starting on page 116 for an explanation of what causes each message. Not all of the messages include what you would expect. For example, the message *Authority Level Changed* does not include users whose authority level was changed on the *Security* screen in *User Properties*; it only includes users whose authority level was changed using the command menus on a reader, which is not how you would typically change a user if you use HandNet. Many of the messages are like this. If you want all of the messages in a particular category, you may find it easier to use the *Message Types* tab instead.

* * * * *

Archiving Past Activity

What Archiving Is

Archiving is moving past activity from the *Current Activity* file to a separate file. This keeps the *Activity* file smaller (and faster) while still keeping the information available for reports if needed. You can set HandNet to remind you to make archives using the *Archives* tab in the *System Settings*; see page 26.

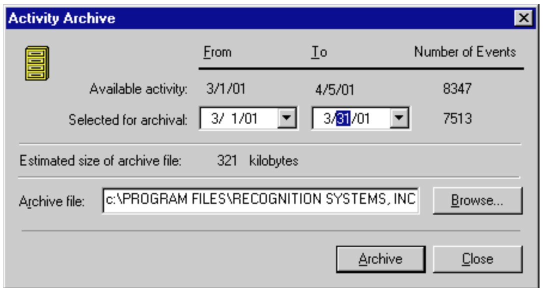
To generate an activity report on activity that is archived, you must indicate that you want to generate the report based on an activity archive (and then pick the appropriate archive).

Effect of Archiving on Reports

When you archive, HandNet removes activity from the current activity file and stores it in a different file. When you generate an activity report, you can use the current activity file OR one of your archive files, but you cannot include activity from more than one file in a single report. This means, for example, that if you make an archive once a month, you cannot generate a single report that looks at the previous year's activity; you would have to generate twelve reports, one for each monthly archive file. If you want an entire year's information in a single report, do not archive until the year is done, so all activity for the year will be in a single file.

Making the Archive

To make an archive of past activity, click the *File* menu and then click *Archive*. You see a screen like this:



Activity Archive

	From	To	Number of Events
Available activity:	3/1/01	4/5/01	8347
Selected for archival:	3/ 1/01	3/31/01	7513

Estimated size of archive file: 321 kilobytes

Archive file: c:\PROGRAM FILES\RECOGNITION SYSTEMS, INC

Available activity: This shows the date of the earliest activity in the activity file and the date of the most recent activity (usually today's date). One the right you will see the total number of events or activities currently in the file.

Selected for archival: This lets you choose the date range to include in the archive. The *From* date is initially set to the date of the earliest activity in the file; you do not normally want to change this date. The *To* date is initially set to today's date; you might sometimes want to make this earlier to keep more activity in the file. For example, suppose you make an archive on the fifth of each month for the previous month. You could change the *To* date to the last day of the previous month so that activity from the beginning of the current month would not be archived yet. Even if you leave the *To* date set to the current date, HandNet may not actually go up to that date: on the *Archives* tab in the *System Settings* there is an entry *Do not archive the latest ___ events*. The archive process keeps at least that many events in the current activity file, even if some of those events are before the date you enter here.

Estimated size of archive file: This is the approximate size that the archive file will be.

Archive file: This lists the name and location of the file that will be created. HandNet uses the location that you have entered for the *Default Archive Directory* on the *Archives* tab in the *System Settings*; see page 27. HandNet names the file using year/month/day hour/minute/seconds. For example *HN Activity Archive 20010406 094542.hna* is the default name for a file made on April 6, 2001 at 9:45 (and 42 seconds) AM. If you sometimes need to generate reports on past activity, and you do not find this naming method very clear, you can change this name. For example, if the archive contained information from the previous month, you might name it something like *Archive March, 2001.hna*. You must keep the .hna extension for HandNet to be able to find the file when you want to generate a report on it.

Once all entries are correct, click the *Archive* button to make the archive.

* * * * *

Exporting Activity

Why Export Activity

If you want to create custom activity reports using some external report tool, *Export Activity* on the *File* menu sends all of your current activity to an Access database file called *expactvt.mdb*. While the main HandNet database files are password protected for security reasons, this file is not, so you can open it (if you have Microsoft Access) and use any information in it. If you are only going to generate reports with *Activity Reports* on the *File* menu, you do not need this option; using it would only create a file that you do not need.

This option only exports current activity, not activity that you have archived, so if you plan to use this option you probably should check the *Export Transactions* box on the *Archive* tab in *System Settings*; see page 27. This causes activity to be automatically exported whenever you archive activity.

You only have access to this option if you have purchased the upgrade to full feature set of Version 2.0.

When you choose *Export Activity*, HandNet pops up a box that tells you how many activity records are going to be exported. Click *OK* to continue.

Avoiding Exporting the Same Information Twice

If you export activity and then export activity again without having archived the activity you exported last time, you will end up with duplicate records in that export file. That is, you will find the same activities listed more than once.

To avoid duplicate activity in the export file you can do one of two things:

- You can export activity and then immediately archive ALL activity. That way, the next time you export activity, the activity that was exported last time will not be in the current activity file, so it will not be exported again.
- If you do not want to archive activity after exporting (you might want to keep more activity in the current activity file so that you could see it in *custom activity* views or create reports that included a longer range of activity), delete or rename the last activity export file (*expactvt.mdb*) before exporting again. If you delete or rename this file, HandNet creates a new *expactvt.mdb* file when you export, and this new file will only contain the information from this export and not what you exported last time.

* * * * *

Activity Messages

You see activity messages in the *Activity* window. You can limit the activity in a custom activity view or in an activity report by checking the corresponding messages on the *Messages* tab in the filter/report design (see page 112). And you can control which messages cause alarms using the *Alarms* tab in the system settings (see page 25).

We have explained the messages in more detail here.

Command Menus in the Reader

Readers have built-in menus that let you change the settings in the reader. Some of the messages below can only occur if you make changes through these menus on the actual readers; you should not typically see these messages. Except for initially setting up the reader to communicate with HandNet, for recalibrating the reader, and for enrolling a user from the reader, you should NOT make changes to the reader through the reader command menus; you should control all other reader settings from within HandNet. See the HandKey manual for more about the reader menus.

Activity Messages

Access Denied: Someone repeatedly entered a valid ID at a reader, and each time the reader did NOT recognize the user's hand (at the reader, the user will see the message *ID Refused*). The number of times that a user can try before getting this message depends on the *Number of Tries* entry on the *Settings* tab in the *Reader Properties*; see page 47. If access is denied for a user, the reader will not accept that ID again until another user has successfully gained access at that reader.

Access Profiles Changed: Someone has changed one or more access profiles. During initial setup, this is a normal message. If you were not expecting access profiles to change, this could be an indication that someone was trying to give inappropriate access.

Access Refused, Time Zone: A valid ID was entered at a reader, but the user is not authorized to have access during the hours or days of the week based on the time zone associated with the reader in the access profile.

Activated Limited Access User: A user was set up with access for a limited date/time range. The computer's date and time matched the date/time the user was scheduled to start having access, so HandNet made the user active and sent the user's information to each appropriate reader so the user could can access; see page 93 for more about limited access.

Activity Archived: The operator used the *Archive* option on the *File* menu; (see page 113 for more on archiving past activity).

Alarm Acknowledged: An alarm occurred, and an operator went to the *Alarm Properties* screen and clicked one of the acknowledge buttons (following the message on the activity or alarm list, you will see *:ACK* followed by the name of the operator who acknowledged the alarm and when it was acknowledged); see page 103 for more on acknowledging alarms.

Amnesty Punch Granted: You should not see this message.

Authority Level Changed: A user's authority level was changed from the reader's command menu (typically you would change a user's authority

level from the *Security* tab in the *User Properties*; if you change the authority level there, you just see the message *User Record Changed*).

Auto Import Started: An *import.mdb* file (which contains users to import) was found, and HandNet was set up to automatically import users, so HandNet started importing them. Whether HandNet automatically imports users is controlled by the *Enable* box under *Auto Import* on the *User Import/Export* tab in *System Settings*; see page 28.

Aux Output OFF: The auxiliary output has been turned off.

Aux Unlock Via Wiegand Keypad: The auxiliary output has been turned on by a valid ID number at a remote keypad.

Auxiliary Input ON: The auxiliary input on the reader has been activated.

Auxiliary Output ON: The reader has turned on an auxiliary device (like an alarm) that is connected to the reader.

Auxiliary Output Setup Changed: The timing and clearing of an auxiliary output activation has been changed.

Baud Rate Changed: The communications baud rate has been changed using the command menus at the reader.

Command Mode Entered: Someone entered the command mode at a reader. Readers have built in menus that let you change the reader settings. These command menus are mainly needed when someone is using the readers without the HandNet program; HandNet controls most settings in the reader for you. The only tasks you should need to do through the reader command menus are setting up the reader's address and communication settings during initial setup, recalibrating the reader, and enrolling users at the reader if you are not using the *Enroll* option on the *Reader* menu.

Data Base Restored: You should not see this message.

Data Base Saved: You should not see this message.

Data Downloaded to Reader: Someone used one of the *Download* options on the *Reader* menu to send information to the reader; see page 60. Unless there was some problem with the reader that is being corrected, this is not usually necessary; HandNet usually automatically sends all information to the reader that the reader needs.

Data Log Buffer Empty: You should not see this message.

Deactivating Limited Access User: A user was set up with access for a limited date/time range. The computer's date and time matched the date/time the user's access was supposed to end, so HandNet made the user inactive and sent the appropriate information to readers so the user could no longer gain access, see page 93 for more about limited access.

Door Forced Open: A door was forced open without a valid ID and hand recognition at a reader.

Door Open Too Long: A door was kept open for longer than was allowed

based on the time entered in the *Door Switch Shunt Time* on the *Configuration* tab in the *Reader Properties*; see page 48.

Duress Alarm: A user entered the duress code, a code that indicates that the user is in trouble or that someone is forcing the user to give him/her access; see page 47 for more about duress codes.

Exit Granted: The user is permitted to exit.

Extended Datalog: Someone entered command mode on the reader and changed settings that do not have specific messages associated with them (for example, you get this message if you change the language of the reader's display or the format of the date on the reader).

HandNet Exited: Someone picked *Exit* from the *File* menu to shut HandNet down. Under normal circumstances, HandNet is left running continually so it can monitor activity and immediately process any alarm messages. If someone exited HandNet to install a new Version of the program or to perform maintenance on the computer it is on, there is probably no problem; if someone exited the program at some other point, this could be an indication of an attempt to get around security.

HandNet Started: Someone started the HandNet program. Under normal circumstances, HandNet is usually left running continually so it can monitor activity and immediately process any alarm messages. If someone exited HandNet to install a new Version of the program or to perform maintenance on the computer it is on and then restarted, then there is probably no problem. If you see the message *HandNet Started* but you do not see the message *HandNet Exited* earlier in the list, then someone exited the program and restored an older Version of the activity files; this could be an indication that someone is trying to hide activity.

HandNet+ File Converted: Someone used *Convert HandNet+* on the *File* menu to convert users from HandNet+ into HandNet for Windows (HandNet+ was an MS-DOS predecessor to HandNet for Windows); see page 98 for more on converting users from MS-DOS Versions of HandNet.

Holiday Table Changed: Someone has added, changed, or deleted a holiday with the *Holidays* option; see page 65 for more about setting up holidays.

Identity Unknown: Someone entered a valid ID at a reader, but the reader did not recognize the user's hand.

Identity Verified: At a reader, a user entered a valid ID and the reader recognized the user's hand and gave access.

Invalid Operator Login Attempt: Someone tried to log into HandNet but entered an invalid user name or password. This could occur if someone just typed the name or password incorrectly, or it could mean that an unauthorized person was trying to get into the program.

Leave Command Mode: Someone exited or left command mode at a reader. Readers have built-in menus that let you change the reader settings. These command menus are mainly needed when someone is using the readers without the HandNet program; HandNet controls most settings in the reader for you. The only tasks you should need to do through the reader command

menus are setting up the reader's address and communication settings during initial setup, recalibrating the reader, and enrolling users at the reader if you are not using the *Enroll* option on the *Reader* menu.

Lock Output OFF: Someone chose *Relock* from the *Reader* menu to relock an unlocked door; see page 128 for more about locking and unlocking doors.

Lock Output ON: Someone chose to unlock a door using one of the *Unlock* options on the *Reader* menu; see page 128 for more about locking and unlocking doors.

Lock Setup Changed: Using the command menus in the reader, someone changed the number of seconds the lock should be unlocked for or the number of seconds the door is allowed to be open (normally this is changed in HandNet on the *Configuration* tab in *Reader Properties*; if it is changed there, you just see the message *Reader Properties Changed*).

Manual Import Started: The operator selected *Import Users* to import users from the *import.mdb* file; see page 99 for more about importing users (when you must import users manually or whether HandNet imports them automatically is controlled by the *Enable* box under *Auto Import* on the *User Import/Export* tab in *System Settings*; see page 28).

Maximum ID Length Changed: Someone changed the maximum length for a user ID using the command menus in the reader (if you changed the ID length on the *Settings* tab in the *Reader Properties*, you would just see the message *Reader Properties Changed*).

Memory Cleared: Someone used the *Clear Memory* option from the *Command* menus in the reader. This erases all the users from the reader (typically you would do this if you were changing the use of the reader and wanted to make sure that those who previously had access through this reader no longer had access through it).

Messages Read: You should not see this message.

No Hand Read For Card: You should not see this message.

Operating Mode Changed: The operating mode of the reader has been changed using the command menus in the reader.

Operator Added: A new operator (someone authorized to use HandNet) was added on the *Operators* tab in *System Settings*; see page 24 for more about adding operators.

Operator Deleted: An operator (someone authorized to use HandNet) was removed from the *Operators* tab in *System Settings*; see page 24 for more about deleting operators.

Operator Login: An operator logged into HandNet.

Operator Logout: An operator logged out of HandNet.

Operator Properties Changed: Someone changed the tasks that an operator is allowed to do on the *Operators* tab in *System Settings*; see page 24 for more about controlling which options an operator can use.

Output Mode Changed: The output mode of lock output or card reader emulation has been changed using the *Command* menus in the reader.

Passwords Changed: Someone changed the passwords for the reader *Command* menus, using the command menus in the reader. Generally this setting is controlled from HandNet on the *Passwords* tab in *Reader Properties* rather than from the reader (if you change this or other settings for the reader in HandNet, you just see the message *Reader Properties Changed*).

Printer Setup Changed: If a serial printer is attached to the reader, the printer settings have been changed using the command menus in the reader.

Reader Action Failed: HandNet was unable to complete a communication attempt with the reader. This could be an indication that the connection to the reader is not set up correctly; see the *Troubleshooting* resolving this error.

Reader Added: A reader was added to HandNet.

Reader Connection Failed: HandNet was not able to establish communications with the reader. This could be an indication that the connection to the reader is not set up correctly; see *Troubleshooting* resolving this error.

Reader Connection Timeout: HandNet lost its connection with the reader. This could be an indication that the connection to the reader is not set up correctly; see the troubleshooting for help resolving this error.

Reader Data Uploaded to HandNet: Someone used *Upload Users* on the *Reader* menu to get user information from the reader; see *Getting User Information from a Reader* on page 99.

Reader Deleted: A reader was deleted from HandNet.

Reader Properties Changed: Someone went to the *Reader Properties* and changed the settings on one of the tabs there. HandNet does not keep track of which settings were changed. For more about *Reader Properties*, see page 45.

Record Imported for Creation: An new user was added to HandNet by the import process.

Record Imported for Deletion: A user that was already in HandNet was deleted based on information in the *Import* file.

Record Imported for Modification: A user that was already in HandNet was changed to match a user with the same ID in the *Import* file.

Record Imported, Empty Template Overwrote Local Enrollment: A user that was not enrolled was imported. This replaced an enrolled user, so the user is not longer enrolled in HandNet. You can prevent enrolled users by being replace by either preventing the exporting computer from exporting users that are not enrolled yet, or by changing the import settings so non-enrolled users cannot replace enrolled ones; see the explanation for the *Import/ Export* settings on page 28.

Reject Override Changed: Someone changed the reject threshold for an individual user using the command menus in the reader. Generally this setting is controlled in HandNet with the *Override* setting on the *Security* screen in *User Properties*; HandNet users would not typically change this at the reader (if you change this or other user settings in HandNet, you just see the message *User Properties Changed*).

Reject Threshold Set: Someone changed the reject threshold using the command menus in the reader. Generally this setting is controlled from HandNet using *Reject Threshold* on the *Configuration* tab in *Reader Properties* rather than from the reader (if you change this or other settings for the reader in HandNet, you just see the message *Reader Properties Changed*).

Remote Enrollment Started: A user was enrolled with the *Enroll* option on the *Reader* menu (for users enrolled from the *Command* menu on the reader, you see the message *User Enrolled*); see page 87 for more about enrolling users.

Report Engine Unavailable: You should never see this message.

Request to Exit Activated: A user has pressed the *Request to Exit* button in order to get out of the secure area.

Score Is: You should never see this message.

Site Added: A site was added to HandNet.

Site Code Changed: The site code was changed using the *Command* menus in the reader.

Site Connected: HandNet is set up to connect with the site by modem, and HandNet connected to the site.

Site Deleted: A site was deleted in HandNet.

Site Disconnected: HandNet is set up to connect with the site by modem, and HandNet disconnected from the site when it was done communicating with the site.

Site Properties Changed: In HandNet, one or more changes were made to the *Site Properties*; for more about *Site Properties*, see page 34.

Special Enrollment: The *Command* menus in the reader was used to enroll a user who does not require hand recognition to gain access.

Supervisor Override: You should not see this message.

System Re-calibrated: Someone recalibrated the reader; see page 124.

System Settings Changed: Someone changed one or more entries on one of the *System Settings* tabs that you get to with settings on the *View* menu; for more about system settings, see page 22.

Tamper Activated: Someone has shaken the reader roughly or has opened the reader. Unless someone was servicing the reader, this message generally

warrants further investigation.

Time and Date Set: Someone changed the time and date in the reader using the command menus in the reader (generally, rather than changing date and time in the reader, you would just make sure that the date and time were correct in the computer and then send the date and time to the reader using *Download Time* on the *Reader* menu).

Time Restrictions Turned On/Off For All Users: You should not see this message.

Time Zone Data Changed: Someone changed a time zone using the *Command* menus in the reader. Generally this setting is controlled with the *Time Zone* settings in HandNet and not changed at the reader (if you change time zones in HandNet, you see the message *Time Zones Changed*).

Time Zones Changed: In HandNet, someone changed *Time Zones*; see page 61 for more on setting up *Time Zones*.

Two Man Timeout: Two people were required to verify at the reader, and they have not done so within the permitted time period.

Unable to Close Communications Port: HandNet was unable to close the *Serial Communications* port.

Unable to Install Communications Port or Unable to Open Communications Port: You get this message if HandNet tries to establish communication with a reader through a serial port and it cannot. Generally this only happens if you are running another program that is already controlling that serial port. You cannot have two different devices connected to the same port, so if a reader really is connected to that port, nothing else should be. Either you have selected the wrong port on the *Connection* tab in the *Site Properties*, or the other program that you are running has the wrong port selected. If you were previously running another program (especially one trying to connect to a modem, fax, or printer), it is possible that the other program tried to use the port and did not close it properly. Make sure that other programs that might try to control the port are closed. If the problem still exists, trying shutting everything down and restarting the computer.

Unable to Retrieve Datalog: An attempt to get information from the reader failed.

Unauthorized Enrollment Attempted: Someone tried to enroll a user at a reader and the user had not been added to HandNet yet. Your settings do not allow this (to change your settings so this is allowed, check the box by *Do not delete unauthorized enrollments* on the *Security* tab in *System Settings*; see page 23).

Unit Address Changed: Someone changed the address of the reader using the command menus in the reader.

User Added From Card: You should not see this message.

User Database Field Added: Someone went to the *Custom* tab in the *User*

Database properties and added a new custom entry; see page 97.

User Database Field Deleted: Someone went to the *Custom* tab in the *User Database* properties and removed a custom entry.

User Database Import Finished: The process of importing users (from the *import.mdb* file) is done.

User Enrolled: A user was enrolled using the command menu on the reader (for users enrolled with the *Enroll* option on the *Reader* menu, you see the message *Remote Enrollment Started*); see page 87 for more about enrolling users.

User Record Added: A user was added in HandNet.

User Record Changed: *User Properties* were changed for a user in HandNet. The change could be on any of the three tabs of user information; see page 90 for more on user properties.

User Record Deleted: A user was deleted in HandNet.

User Removed: A user was removed using the command menus in the reader. A user who was removed in this way is only removed from that one reader; the user is not removed from HandNet or from any other reader. If you ever download users to a reader, the user will be added to the reader again if the user is still in HandNet (to remove a user from HandNet, click the user on the list of users and press the *DEL* key. Removing a user from HandNet generates the message *User Record Deleted*).

Users Listed: Someone listed users using the command menus in the reader (if you want a list of users, its generally much easier to just look at the list of users in HandNet or to print the *Users* report; see page 13).

Users Time Zone Changed: When a user can access the reader was changed from the command menus in the reader (typically, this is not changed at the reader; you would instead change the user's access profile on the *Security* tab in *User Properties* to change when the user has access to particular readers. If you did this, you would see the message *User Properties Changed*).

* * * * *

Other Ongoing Activities

Reader Maintenance

Cleaning Readers

You should periodically clean hand readers; if you do not, users may get rejected more often.

Spray any ordinary, non-abrasive cleaner on a clean cloth, and then use the cloth to wipe the platen, the mirror and reflector on the sides of reader, and the window above the platen. When wiping the platen, start from the back corners and wipe forward.

Never spray cleaning fluid directly onto the reader! Always spray a cloth and then wipe the reader with the cloth.

Never use an abrasive or gritty cleaner! An abrasive cleaner could scratch the reader; this would damage it.

Recalibrating Readers

If users are often being rejected at a particular reader, try recalibrating it. To do this:

1. Check the list of users to make sure you have an authority level of one or higher. If you have an authority level of *None*, you cannot do this (to change your authority level, double-click your name on the list of users, click the *Security* tab, click the *Authority Level* entry, and select the appropriate level).

2. Go to the reader to be recalibrated, and enter command mode on the reader:

   If you have a HandKey II or HandKey CR reader: Press *CLEAR*, and then press *ENTER*.

   If you have an ID3D HandKey reader: Press *#* AND *** (you can press them at the same time, or one after the other).

   The display on the reader should look like this:

```
READY
*:
```

3. Type your *User ID* number (the same one you enter to get access through the reader), and press *ENTER* or *#.* The reader asks you to place your

```
ENTER PASSWORD
```

hand. Once it recognizes your hand, this display looks like this:

4. Type *1* and press *ENTER* or *#* (this is the standard password for the *Service* menu in the reader; if you have changed this on the *Passwords* screen in the *Reader Properties*, enter the password you have set up). The display should now look like this:

```
    CALIBRATE
*  NO     YES #
```

   If the reader shows the *READY* screen again instead of this screen, either you placed your hand improperly or you do not have the rights to do this; carefully check step one again.

5. Press the *YES/#* button. This display should now look something like this:

```
 r0   c0  e100  s
RECAL  (Y#/N*)?:
```

   (The actual numbers on the first line may be different).

6. Press the *YES/#* button again. After telling you to please wait, you will see the *Calibrate No/Yes* display again. At this point, the reader should be recalibrated.

7. Press the *CLEAR* button to leave the *Service* menu and return to the reader to its normal display.

* * * * *

Making Backups

Why Make Backups

Occasionally computer hard drives fail, losing the information on them. Occasionally computer files get damaged, making the information in them unusable. And occasionally computer users make mistakes and delete information they should not. A backup is an extra copy of the information on your computer, so that if the information gets damaged or lost, you have another copy to protect you.

The information in HandNet—information about readers, access profiles, and users—represents many hours of work. The record of activity (including archived historical activity) is often an important security record. So you should protect your many hours of work by periodically making a backup copy of this information.

Making Backups a Scheduled Event

In practice, many computer users understand that backups are important, but they still go months or even years without actually making one. Then, when a problem occurs, the backup they have is so old that it does not save them all that much work. The way to avoid this is to make backing up your information a scheduled part of your routine. How often you need to make them depends on how many changes to the information you make. If you are continually adding and removing users, a weekly backup might be appropriate. If you make fewer changes and losing a month's changes would not be that hard to redo, a monthly backup might be enough. Regardless, decide how often to make a backup, and then put it on your calendar; do it every Friday morning, or every month before you print your activity reports. If you do not schedule backups, they probably will not happen. And if you do not make them, sooner or later most computer users regret it.

How to Make a Backup of Your HandNet Information

You should periodically be making backups of all the information on your computer. How to best do that is beyond the scope of these instructions. Here, we will just tell you how to make a backup of your HandNet information.

1. Use *Windows Explorer* to go to the folder HandNet is in (if you installed HandNet in the standard location, it is in *C:\Program Files\Schlage Biometrics, Inc\HandNet for Windows*).

2. Make a copy of all of the Microsoft Access Database files (**.MDB*) and all of the HandNet Activity Archive files (**.HNA*) in this directory. You can copy these files to a floppy disk or to a network drive. If the files are large, WinZip is a helpful and inexpensive utility that lets you both compress a number of files into a single archive and spread the archive over a number of disks if needed (to get WinZip, go to *www.winzip.com*. For help making an archive span several floppy disks, look up "spanning" in the index of WinZip's help).

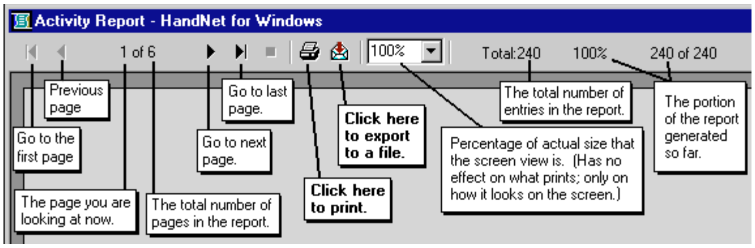
The best protection is to store the backup disks in a different place than the computer. That way, if the computer is damaged by fire or water, or if the computer equipment is stolen, there is no chance of the backup disks being damaged or taken.

* * * * *

Reporting and Exporting Information

Printing or Viewing Reports

Whenever you generate a report, HandNet shows the report in a new window. The header of that window lets you move from page to page, print the report, or export the report to a file. The header looks like this:


Activity Report - HandNet for Windows
1 of 6
100%
Total:240
100%
240 of 240
Previous page
Go to the first page
The page you are looking at now.
The total number of pages in the report.
Go to last page.
Go to next page.
Click here to export to a file.
Click here to print.
The total number of entries in the report.
Percentage of actual size that the screen view is. (Has no effect on what prints; only on how it looks on the screen.)
The portion of the report generated so far.

To print the report: Click the printer icon near the middle of the header to print the report.

If the printer icon is disabled and grayed out, you do not have a printer set up yet on this computer (to set up a printer, go to the Windows *Start* menu, highlight *Settings*, pick *Printers*, and click *Add Printer*).

To export the report to a file: Click the icon with the envelope. You can export to a variety of formats including Word, Excel, Lotus 1-2-3, ...rtf, text, and others.

To close the report window when done: Click the *X* in the upper-right corner of the window.

Getting Information from HandNet Database Files

HandNet for Windows stores information in access database files (*actions.mdb, activity.mdb,* and *HandNet.mdb*). These files are password-protected for security; we do NOT ever give these passwords out for any reason. If we did, it would put the integrity of your security at risk.

Exporting activity to an access database file

However, HandNet can export activity to an access database file that is not password protected so you can open it and access any information in it at will. If you want to create custom activity reports using some external report tool, *Export Activity* on the *File* menu sends all of your current activity to an access database file called *expactvt.mdb*.

Exporting the content of any report to various formats

To save HandNet information to a file, you can also generate any *Activity Report* or other report on the *Reports* menu and, when you see the report on the screen, click the *Export* button.

You will then be able to save the content of the report in a number of different formats so you can import it into other programs. These formats include: character-separated values, comma-separated values, Crystal Reports, Data Interchange Format (DIF), Excel (Versions 5.0, 7.0, or 8.0; either extended or not), Lotus 1-2-3 (WK1, WK3, or WKS), Access 97 database, paginated text, record style (columns of values(report definition, Rich Text Format (RTF), tab-separated, text, or Word for Windows)).

* * * * *

Locking and Unlocking Doors

Automatically Unlocking a Door on a Scheduled Basis

If you regularly want a door unlocked during certain hours:

1. If you have not already done so, set up a time zone that corresponds to the days and times you want the door unlocked.
2. Select the reader(s) in the list of readers.
3. Pick *Reader* from the main menu, and then pick *Properties* from the *Reader* menu.
4. Go to the *Configuration* tab.
5. In the *Auto Unlock Time Zone*, choose the time zone when the door should be automatically unlocked. HandNet automatically unlocks the door at the beginning of the time zone, and locks it again at the end of the time zone.

Unlocking a Door on a Non-Scheduled Basis

Unlock on the *Reader* menu lets you unlock a door without setting it up to be regularly unlocked.

1. Select the reader(s) in the list of readers.
2. Pick *Reader* from the main menu, and highlight *Unlock* on the *Reader* menu. You will see another menu with two choices: *Indefinite* and *Timed*.

   To unlock a door so that it stays unlocked until you lock it again: Choose *Indefinite*. This leaves the door unlocked until you lock it again with *Relock* on the *Reader* menu.

   To unlock the door momentarily: Choose *Timed*. This unlocks the door connected to that reader only for the number of seconds specified in *Lock Open For* on the *Configuration* tab in the *Reader Properties* (that is, it unlocks the door for the same number of seconds that the door would be unlocked if it were opened by a reader).

Locking a Door so it cannot be Opened from the Reader

Lockup on the *Reader* menu disables the lock on the door for the selected reader. The reader will still let users enter their ID numbers and still verify hands, but the door will stay locked and will not open even for valid users. No one will be able to open the door from the reader until you choose *Unlock* or *Relock* from the *Reader* menu.

Locking an Unlocked Door

If you have unlocked a door with *Unlock, Indefinite* on the *Reader* menu, *Relock* locks it again (if you unlocked the door using *Unlock, Timed* on the *Reader* menu, the door automatically relocks after the number of seconds specified in *Lock Open For* on the *Configuration* tab in the *Reader Properties* just as it would if the door were unlocked by the reader, so you do not have to anything special to relock it).

If you have disabled access through a door with *Lockup* on the *Reader* menu, *Relock* releases so the reader can open it again.

* * * * *

Turning an Auxiliary Device On or Off

HandNet can be set up to automatically turn on external auxiliary devices when certain conditions occur. For example, it might trigger an alarm, turn on lights or a security camera, and so on.

HandNet can turn an auxiliary device on automatically when certain conditions occur. When this can happen is controlled by the *Auxiliary (AUX) Settings* tab; see page 48 (the HandKey II and HandKey CR support up to three auxiliary devices; this option only controls the first of these, the same one controlled by the *Auxiliary Settings* tab in *Reader Properties*. The other two are only controlled by the *Extended Settings* tab in *Reader Properties*).

Manually Turning an Auxiliary Device On

Auxiliary Output on the *Reader* menu lets you turn manually turn an auxiliary device on or off without anything happening at the reader. For example, suppose a reader, in addition to being connected to a door, is also connected to an auxiliary light. You could use this option to turn the light on without doing anything at the reader.

To turn on an auxiliary device that is connected to a reader:

1. Click a reader in the right pane of the *Network* window (if the *Network* window is not shown, press *CTRL-N* to open it).
2. Click *Reader* from the main menu bar at the top of the screen.
3. Click *Auxiliary Output* on the *Reader* menu, and then click *On*.

Manually Turning an Auxiliary Device Off

If you have manually turned an auxiliary device on, or if an alarm condition has turned it on, you can also turn the device off from HandNet. For example, suppose an auxiliary alarm is connected to the reader, and suppose the alarm is set to sound for fifteen minutes after the condition occurs. You could use this option to turn the alarm off before the fifteen minutes was done.

To turn off an auxiliary device that is connected to a reader:

1. Click a reader in the right pane of the *Network* window (if the *Network* window is not shown, press *CTRL-N* to open it).
2. Click *Reader* from the main menu bar at the top of the screen.
3. Click *Auxiliary Output* on the *Reader* menu, and then click *Off*.

* * * * *

Troubleshooting

Answers to Common Questions

Enroll Option Disabled

If the *Enroll* option on the *Reader* menu is disabled or grayed out, there are several possible reasons. Check each of the following:

1. Make sure you are logged in. If you are not logged in, you cannot change anything.
2. Make sure that you have selected a reader on the list of readers. Since enrollment has to be done at a reader, you must pick the reader to enroll at before the enroll option will work (to see the list of readers, type *CTRL-N* or pick *Network* from the *View* menu).
3. Pick *About HandNet for Windows...* from the *Help* menu. Check the bottom of the box that pops up. To be able to use the enroll feature, the last line must say *You may use all features of this software.* If this line says *Your current license does not let you use the enroll...,* you must contact your dealer and upgrade your license before you can use this feature (once you upgrade, we will send you an access code that makes the feature available). If you do not upgrade to the full feature set, you must start the enrollment process using the command menus in the reader; see page 87.
4. Check with your supervisor to see if you are authorized to enroll users (for you to be authorized to enroll users, *Reader Data Download* must be checked in the *Access Rights* for the operator in *System Settings*).

No Current Record Message

You get the message *No Current Record* when you start HandNet if you have not added any users yet. This message stops occurring once you add a user; see page 74 and following for help adding users.

Problems Connecting to a Site by Modem

If you are having trouble getting HandNet to connect to a site by modem, check each of the following:

1. Click the site in the left pane of the *Network* window, pick *Properties* from the *Site* menu, and click the *Connection* tab.
2. Make sure you have picked the serial port that the modem is connected to; if this is set to *None*, HandNet will not connect.
3. Make sure the *Baud Rate* in *Site Properties* in HandNet matches the baud rate the reader is set up for. We recommend 9,600 for a HandKey II or HandKey CR and 2400 for a HandKey reader.
4. Make sure the phone number is entered correctly. If you have to dial some digit to get an outside line, enter this digit followed by a comma before the phone number. If the number is a long distance number, make sure you have entered the 1 and the area code as appropriate. For example, if you

have to dial *9* for an outside line, and the number was a long distance call that required by *1* and an area code, you would enter the number like this:

9, 18025551212

5. Make sure the modem is hooked up to a phone line.

6. Make sure the phone line is plugged into the right jack on the modem connected to your computer (most modems have two jacks: one labeled *Line* and one labeled *Phone*. The phone wire from the phone jack on the wall must connect to the jack on the modem labeled *Line*.

7. Make sure the phone line has a dial tone (hook up a regular phone to the modem jack labeled *Phone* to see if you hear a dial tone; if you do not, there is a problem with the jack or phone line).

8. Make sure no other phone, fax machine, or modem is trying to use the same phone line.

9. Make sure call waiting is not on for this line.

10. On the *Schedule* tab in *Site Properties*, make sure you have set up a time for this site to connect. Make sure this connection time is enabled (checked).

Program Claims to be a Demonstration Version

When HandNet for Windows is installed, it is in demonstration mode: it gives you full functionality for fourteen days, and after that it limits the use of certain features.

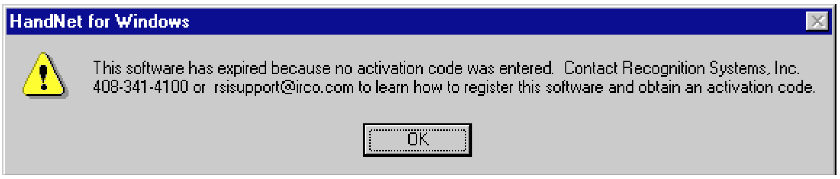
If you purchase a previous Version of HandNet for Windows, you are also authorized to use this Version, but you must register it first, even if you registered your previous Version. Once you send us your registration information, we will give you an authorization code that makes the program permanently functional.

To register this copy of HandNet, please pick *Registration* from the *File* menu and follow the instructions on that screen (we would just repeat the instructions here, but you need the unique ID number that is shown on that screen and you also need to print the registration form).

If you really do have a demonstration Version, please contact us to find out how to purchase a full Version.

Software Expired

After the first time you use this Version of HandNet, you have fourteen days to register it. You must register even if you registered your previous Version of HandNet. If you do not register within fourteen days, you will not be able to log in. When you try to log in, you see this message:



HandNet for Windows

This software has expired because no activation code was entered. Contact Recognition Systems, Inc. 408-341-4100 or rsisupport@irco.com to learn how to register this software and obtain an activation code.

If you get this message, exit HandNet and then restart. This brings up the registration screen. Send us the information requested on that screen. Once we get your information, we will send you an activation code to enter on the registration screen. This will make HandNet permanently functional.

Unable to Acknowledge an Alarm

If you have opened the detail box for an alarm and the *Acknowledge* buttons are disabled or grayed out, check the following:

1. Make sure you are logged in. If you are not logged in, you cannot change anything.
2. Make sure that you are clicking one of the *Acknowledge* buttons at the bottom left of the window; you cannot just click the checkbox by the word acknowledged; you must click one of the buttons.
3. Check with your supervisor to see if you are authorized to acknowledge alarms (for you to be authorized to acknowledge alarms, the *Alarm Acknowledgement* box must be checked in the *Access Rights* for the operator in *System Settings*; see page 24 for more on adding or changing operator settings).

User Often Rejected

If a user is often rejected at readers, you may need to teach the user the correct way to place the hand on the platen; see *Teaching Users How to Place Their Hands on Readers* on page 86.

Creating a new profile of the user's hand

If the user held his/her hand improperly while being enrolled, or if the user has lost or gained a lot of weight, the hand profile may be different enough to prevent recognition. Delete the user (this eliminates the old hand profile), and then add the user again. When you re-enroll the user, this creates a new profile of the hand. Make sure the user correctly places his/her hand. You can usually avoid this situation by allowing HandNet to update the user's hand profile each time the user gains access; see page 23.

If the user has a disability that prevents consistent hand placement

You may need to increase the tolerance for the user. To do this:

1. Double-click the user on the list of users (you could also click once to select the user and then pick *Properties* from the *User* menu).
2. Click the *Security* tab.
3. Check the *Override Reader's Threshold* box if it is not already checked.
4. Drag the pointer to the right (the *Less Sensitive* side).

If many users are rejected at a particular reader

If many users are being rejected at a particular reader, you may need to clean the reader or you may need to recalibrate it; see page 124.

* * * * *

Index

Ingersoll Rand
Security Technologies

Ingersoll Rand's Security Technologies Sector is a leading global provider of products and services that make environments safe, secure, and productive. The Sector's market-leading products include electronic and biometric access control systems; time and attendance and personnel scheduling systems; mechanical locks and portable security, door closures and exit devices, steel doors and frames, architectural hardware and technologies and services for global security markets.

408.341.4110

www.schlage.com www.ingersollrand.com

Schlage
Biometric Solutions
Ingersoll Rand Security Technologies
1520 Dell Avenue
Campbell, CA 95008
Office: 866-861-2480/512-712-1413 (international)
Fax: 866-303-1794/408-341-4111
E-mail: sbssupport@irco.com

HandNet-Lite

Terminal User's Guide

Ingersoll Rand
Security Technologies

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and, if not installed and used in accordance with the Installation Manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at the user's own expense.

This Class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numerique de la classe A respecte toutes les exigences du Reglemente sure le materiel brouilleur du Canada.

Document Part Number: 70100-6210 – Revision 3 – June, 2009

Schlage Biometrics, Inc. reserves the right to change, without notice, product offerings or specifications.

Contents

Getting Started

Introduction

What HandNet Lite Does

HandNet Lite lets you control and monitor many connected FingerKey and/or HandKey readers. In this one program, you can control who can use each reader and when. You can also monitor activity and alarms for all readers at once.

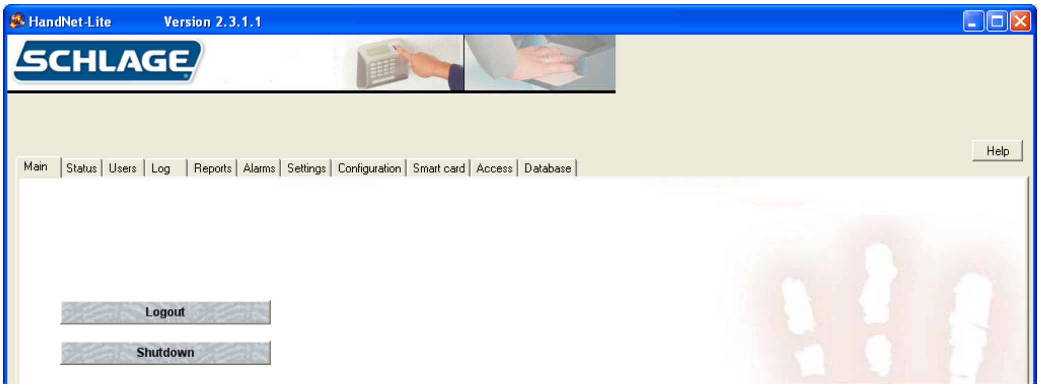
HandNet Lite System Requirements

Operating System: Windows XP SP3, Vista, Windows Server 2003 SP1 or greater, Windows 2000 Professional or Server Editions SP4, and Windows 95 & 98.

Screen Resolution: Screen resolution must be set to at least 1024 x 768; the HandNet Lite window won't fit on your screen if you use a lower resolution. The actual screen size is 1020 x 720, so if your screen resolution is 1024 x 768, your task bar must be on the top or bottom of the screen, and the task bar must be no more than two lines high; if the task bar is three lines or higher or if it is on the side of your screen, part of the HandNet Lite window will run off the screen.

Starting HandNet Lite

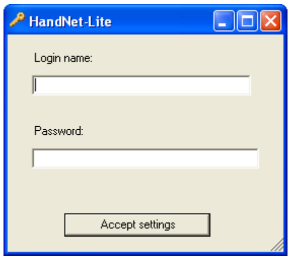
To start HandNet Lite, either double-click the HandNet Lite icon on your Windows desktop or click the Start menu on your Windows taskbar, highlight Programs, highlight Schlage Biometrics, highlight the HandNet Lite folder, and click HandNet Lite. The main window opens.



Logging into HandNet Lite

HandNet Lite requires you to log in before you can make any changes; this prevents unauthorized people from changing information. If you aren't logged in, you can look at the current status of readers and get on-line help, but you can't change any information or use any other options.

1. **Click Login on the Main window. You'll see:**



2. **Type your Login name and Password and click Accept.**

   If this is a new system: Use a Login name of "1234" and a Password of "new." (After logging in for the first time, you should add one or more new operators. See Managing Operators on page 26 for more information.)

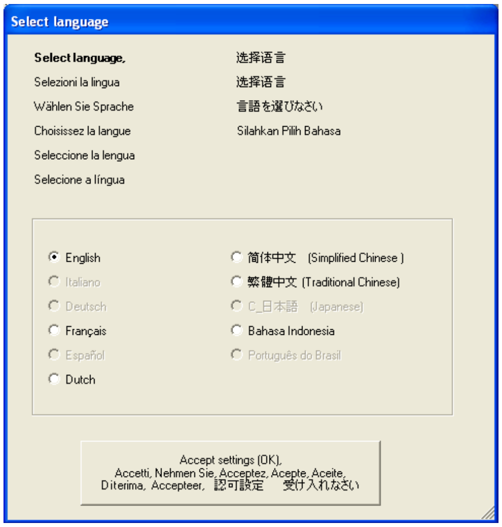
   After initial setup: If you forget your Login name or Password, see your supervisor or security administrator.

   The login name and password are case sensitive. For example, the passwords new, New, and NEW are all different.

After you are done using HandNet Lite, log out so unauthorized people won't be able to use the program.

Select Language

After HandNet-lite version 2.3 is installed, the first time it is run the following screen will be presented so that the displayed language can be selected. If you do not see the special characters on your computer, use Control Panel, Regional and Language Settings, Advanced tab and select the desired character sets.


Select language

Select language, 选择语言
Selezioni la lingua 选择语言
Wählen Sie Sprache 言語を選びなさい
Choisissez la langue Silahkan Pilih Bahasa
Seleccione la lengua
Selecione a língua

● English ○ 简体中文 (Simplified Chinese)
○ Italiano ○ 繁體中文 (Traditional Chinese)
○ Deutsch ○ C_日本語 (Japanese)
○ Français ○ Bahasa Indonesia
○ Español ○ Português do Brasil
○ Dutch

Accept settings (OK),
Accetti, Nehmen Sie, Acceptez, Acepte, Aceite,
Diterima, Accepteer, 認可設定 受け入れなさい

This is the "Select Language" screen. Current language choices are English, French, Dutch, Simplified Chinese, Traditional Chinese, and Bahasa Indonesian.

Getting Help in HandNet Lite

The on-line help has the same information as this manual. To get help in HandNet Lite, click the Help button. Use the contents, index, or search tabs at the left of the help window to find any topic.

For Basic Topics

Click the Contents tab at the top of the left pane, click a book to open, and then click a topic. Not every topic is in the Contents though, so if you don't find what you need, try the Index or Search tabs.

For Groups of Topics on a Single Theme

In addition to the contents you can also click on the pull-down list right under the Previous/Next buttons (in the bottom middle of the header). This list contains a number of important groups of topics. Once you are on one of these topics, the Next and Previous buttons work as well.

Marking a Topic to Return To

In the on-line help, to mark a topic that you want to come back to:

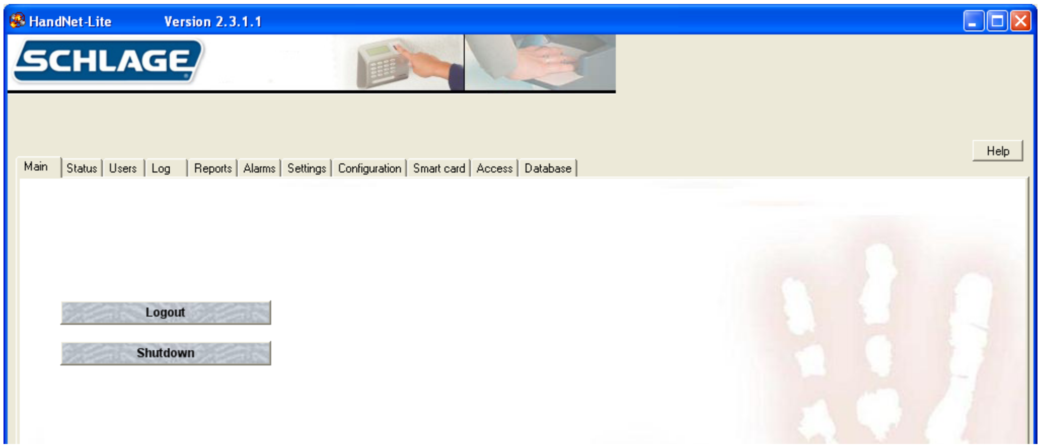
1. Go to the topic that you want to mark.
2. Click the Favorites tab at the top of the left pane.
3. Click the Add button at the bottom of the pane. This adds the topic to your favorites list.

To get back to any marked topic later:

1. Click the Favorites tab at the top of the left pane of the help window.
2. Double-click the topic.

Main HandNet Lite Window

After you log into HandNet Lite, a number of additional tabs appear that let you get to the different parts of the program. Which tabs you see depends on which operator login you used. The screen below shows all of the options.



What You Can Do On Each Tab

Each of the tabs are explained in further detail later in the following chapters.

Status: The Status tab lists every reader in HandNet Lite and the network (group of readers) the reader is connected to. It gives information about each reader and the state of its connection. See page 7 for more information.

Users: The Users tab lists every user that has been added to HandNet Lite, including the user's name, ID, access profile (the group of readers the user has access to), authority level (which reader menus the user can program), and whether the user is enrolled; see page 9. You can add, change, or delete users through the buttons in this tab.

Log: The Log window lists significant events at any connected reader. It doesn't list user accesses, but it lists user additions and enrollment, alarm conditions, and so on. It also lists significant changes made in HandNet Lite. For each event you see the date and time, network and reader, user name and IDs, a brief description of what happened, and an icon showing the type of activity. See page 17 for more information.

Reports: The Reports tab lets you generate reports on all of your users and all of your readers. See page 19 for more information

Alarms: The Alarms tab shows a subset of what you see on the Log tab; this tab lists only those events that are classified as alarm conditions. These generally require immediate attention. See page 23 for more information.

Settings: The Settings tab lets you change HandNet Lite's login name and passwords. It also lets you choose the default Access Profile for users added at a reader, that is, which readers the user has access to. See page 25 for more information.

Configuration: You may add, change, or delete networks and readers. The Configuration tab also allows you to create Wiegand output configurations which can be used for setting FingerKey output. See page 29 for more information.

Smart card: The Smart Card tab is used to manage iCLASS, DESFire and MiFare cards. See page 49 for more information.

Access: The Access tab lets you define access profiles. Access profiles control which readers different groups of people have access through. See page 61 for more information.

Database: The Database Tab is used to backup, restore, delete, detach and attach the database. See page 63 for more information.

Getting Around with the Keyboard

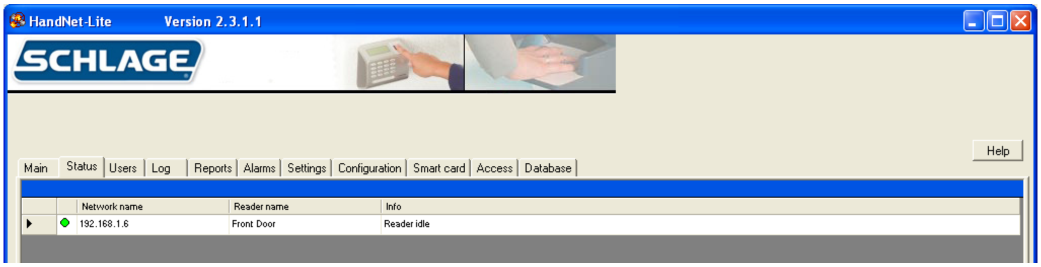
To move from tab to tab: Press ctrl tab.

To move from entry to entry with a tab: Press tab to move to the next entry, and shift tab to move to the previous entry.

Status Tab

The *Status* tab lists every network and reader that has been configured in HandNet Lite.

Figure 4-1: Status Tab



		Network name	Reader name	Info
▶	🟢	192.168.1.6	Front Door	Reader idle

Table 4-1: Reader Status

Column	Description
Status Indicator (untitled)	Indicates the current status of the reader
Network name	Name of the reader's network
Reader name	Name of the reader
Info	Details about the status of the reader's connection

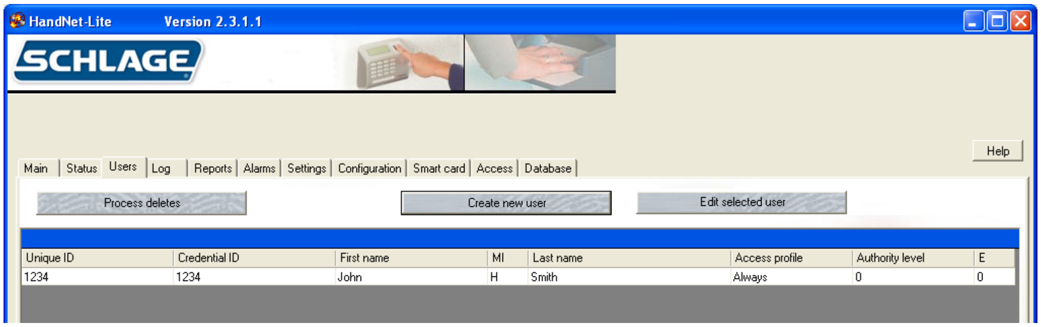
Click the heading of any row to sort the list by that heading. Click the heading again to reverse the sort order.

Table 4-2: Reader Status Indicators

Icon	Description	Additional Information
🟢	Reader is communicating	• Click the green icon to display download and conditionally upload user choices. • If the reader is a FingerKey you will have a Download (Download from PC to the reader) choice. • If the reader is a HandKey you will have both a Download (from the PC to the reader) and Upload (from the reader to the PC) choices.
○	Reader is not enabled	• Readers must be first created (see create new reader) and then enabled (see enable reader).
🔴	Reader is not communicating.	• The reader is not configured correctly, or is disconnected. • Click the red icon for further details.

Users Tab

The *Users* tab lists every user and is used to add or change users. Users are individuals who are enrolled in readers.



Unique ID	Credential ID	First name	MI	Last name	Access profile	Authority level	E
1234	1234	John	H	Smith	Always	0	0

List of Users

Table 5-3: List of Users

Column	Description
Unique ID	ID by which the user is identified in the database
Credential ID	ID the user enters at the reader in order to gain access
First Name	User’s first name
MI	User’s middle initial
Last Name	User’s last name
Access profile	Access profile that is associated with the user (See page 61 for more information.)
Authority Level	• Authority level for the user. • Zero (0) for most users, meaning the user can gain access through the reader, but not use the command menus in the reader to change settings. (See page 14 for more information.)
E	• Indicates enrollment status • Zero (0) indicates that the user is not enrolled. • One (1) indicates that a HandKey template has been captured for the user • Two (2) indicates that a FingerKey template has been captured for the user • Three(3) indicates that HandKey and FingerKey templates have been captured for the user.

Click the heading of any row to sort the list by that heading. Click the heading again to reverse the sort order.

Clicking on a user row will display actions that can be performed for that user.

Enroll Users

Users must be enrolled on a reader. For help enrolling users, see the reader’s manual.

A user may be added to HandNet Lite in one of two ways:

- **Enroll the user at a reader before entering the user in HandNet Lite.** If the reader is connected, the user is automatically added to HandNet Lite. If users are enrolled in readers before they are connected to HandNet Lite, when the reader is initially connected to HandNet Lite, all users are imported then.

  If a user is enrolled first, the user ID in the reader (the Credential ID) is used in HandNet Lite for the user’s First name, Last name, and Unique ID (an identifier used only by HandNet Lite to help distinguish users with similar names). Edit these entries by selecting the user in the Users window and clicking the Edit selected user button; see Edit Fingerprint Settings page 41.
- **Enter the user in HandNet Lite before enrolling the user in a connected reader.** Enter the user in the User edit window. See Add a User on page 11 for more information. The user will be listed as unenrolled in the Users window (denoted by a zero (0) in column E). See the User Fields table on page 13 for more information. When you enroll the user at a reader, HandNet Lite will import the finer template.

! NOTE *When enrolling users at the reader, you must completely leave the reader’s command menus before HandNet Lite will detect the enrollments.*

Problems with User Enrollment

Since bypassing finger or hand recognition gives you reduced security, it should only be used as a last resort. Try these options first:

- The user might have placed the finger or hand badly during the initial enrollment.
  1. Remove the user from the reader.
  2. Instruct the user on correct finger or hand placement. Make sure the user is placing the right finger.
  3. Add the user again.

  This creates a new template for the user.
- If using a FingerKey, Remove the user, and enroll the user again using different fingers. Try the thumb if other fingers don’t work
- If the user has a mild disability that prevents consistent finger or hand placement, change the user’s reject level. See Biometric threshold on page 13 for more information. See the reader manual for instructions on how to set the appropriate reject setting for the user.

If these options aren’t possible, or if you try them and they don’t work, then check the Verify on ID only (no biometric verification) box on the User edit screen. See Verify on ID only on page 14 for more information

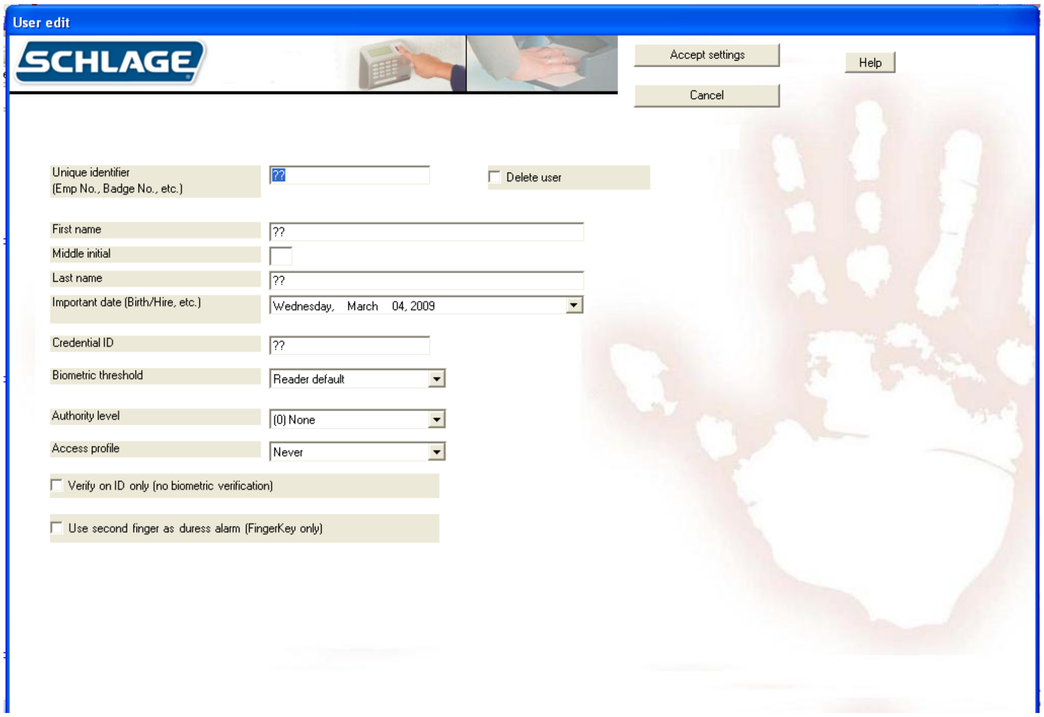
Adding a Special User

When using a FingerKey, if a user's fingerprint cannot be scanned (for any reason), the user can be added as a special user. Special users are still required to place a finger on the scanner, but the scanner does not try to match a finger template.

If a user has unrecognizable fingerprints, severe arthritis, or other conditions that keep the user's finger from being recognized, you can give the user access without finger recognition. If you choose this, the reader still asks the user to place a finger on the reader so it won't be apparent to others that finger recognition isn't required, but the reader doesn't check the finger template; it gives access regardless of whose finger is placed there.

Add a User

1. Click the *Users* tab.
2. Click the *Create new user* button.



Unique identifier (Emp No., Badge No., etc.) ??

□ Delete user

First name ??

Middle initial

Last name ??

Important date (Birth/Hire, etc.) Wednesday, March 04, 2009

Credential ID ??

Biometric threshold Reader default

Authority level (0) None

Access profile Never

□ Verify on ID only (no biometric verification)

□ Use second finger as duress alarm (FingerKey only)

3. Complete the fields on the screen. See the User Fields Table on page 13.
4. Click the *Accept Settings* button.
5. If the user has not been enrolled on a reader, do so now. See Enroll Users on page 10 for more information.

Edit a User

1. Click the *Users* tab.
2. Click to select the name of the user you want to edit.
3. Click the *Edit selected user* button.
4. Complete the fields on the screen. See the User Fields table on page 13 for more information.
5. Click the *Accept Settings* button..

Delete a User

1. Click the *Users* tab.
2. Click to select the name of the user you want to delete.
3. Click the *Edit selected user* button.
4. Click the *Delete user* check box.
5. Click the *Accept Settings* button.

Note: You can also edit, delete, and enroll an existing user by clicking on that user listed on the User’s tab and selecting the desired action from the pop-up menu.

User Fields

Table 5-4: User Fields

Field	Req'd?	Description
Unique Identifier	Yes	• Up to 30 characters (any combination of letters, numbers, spaces, or special characters) • If user was added from the reader, will initially match credential ID in the reader but can be changed.
First Name	Yes	• User's first name • If user was added at the reader, will initially match the credential ID
Middle Initial	No	• User's middle initial
Last Name	Yes	• User's last name • If user was added at the reader, will initially match the credential ID
Important Date	No	• Used to distinguish between users with similar names • Type a date directly into the entry box using the format Thursday, January 01, 2009 • Click the drop-down button to select the date from a calendar.
Credential ID	Yes	• User's credential ID • ID number from user's card (when card readers are used) or the number a user enters manually at the reader. See the reader's manual for help with designing an ID numbering system.
Biometric Threshold	Yes	• Controls how closely user's finger or hand must match the stored template in order for access to be granted. • Reader default uses the Reject Threshold from the reader's setup. See Reject Threshold on pages 36 and 38 for more information. In most cases, Reader default is the appropriate choice. • To override the reader's reject threshold, choose from values of 30-250 in the drop down list (common values of 250, 150, 75, 50, and 30 are singled out at the top). • Use a lower number for higher security. • Use a higher number if a user has trouble gaining access. See the reader's manual for more information.
Authority Level	Yes	• Determines what menus the user can access at the reader. • Each level gives access to all the lower levels. • See the Authority Levels table on page 14 for more information.
Access Profile	Yes	• Controls which readers the user can use. • Always allows access to all readers. • Never blocks access to all readers. • Additional choices correspond to the profiles configured in the Access tab. See Access Tab on page 61 for more information.

Field	Req'd?	Description
Verify on ID only (no biometric verification)	No	• Check for users who fingerprints or hand cannot be scanned • Since bypassing finger or hand recognition gives you reduced security, only use this as a last resort. See Adding a Special User on page 11 for more information.
Use Second Finger as Duress Alarm (FingerKey only)	No	• When checked, user's second finger will be used as a duress indicator.
Delete User	No	• Check to delete user from HandNet Lite. • User will be deleted from HandNet Lite and from all connected readers when you click the *Accept* button.

Authority Levels

Table 5-5: Authority Levels

Authority Level	Description
(0) None:	• Allows user to gain access through the reader, but not use the command menus in the reader to change the reader's settings. • This choice is appropriate for most users.
(1) Service:	• Allows the master reader to display the status of all readers on the network. • Not relevant on readers that are not configured as a master.
(2) Setup:	• Allows user to control reader setup • See reader's manual for more information.
(3) Management:	• Allows user to list all of the users in the reader • Allows master reader to send/acquire user databases to/from readers in a network.
(4) Enrollment:	• Allows user to add or remove users.
(5) Security:	• Allows user to modify security settings • See reader's manual for more information.

See the reader's manual for information on directly changing settings through the reader.

Process Deletes Button

When the Process Deletes button is pressed, HandNet-Lite looks for a RemoveUserXML. Xml file in the root directory of the C: Drive.   If this file is found, any users listed in that file will be removed from Handnet-lite.   Figure 3.1 provides a sample C:\RemoveUserXML. Xml file which would remove users with UserIDs of 1000, 1001, 1002, 1003, and 1004 when the Process Deletes button is pressed.

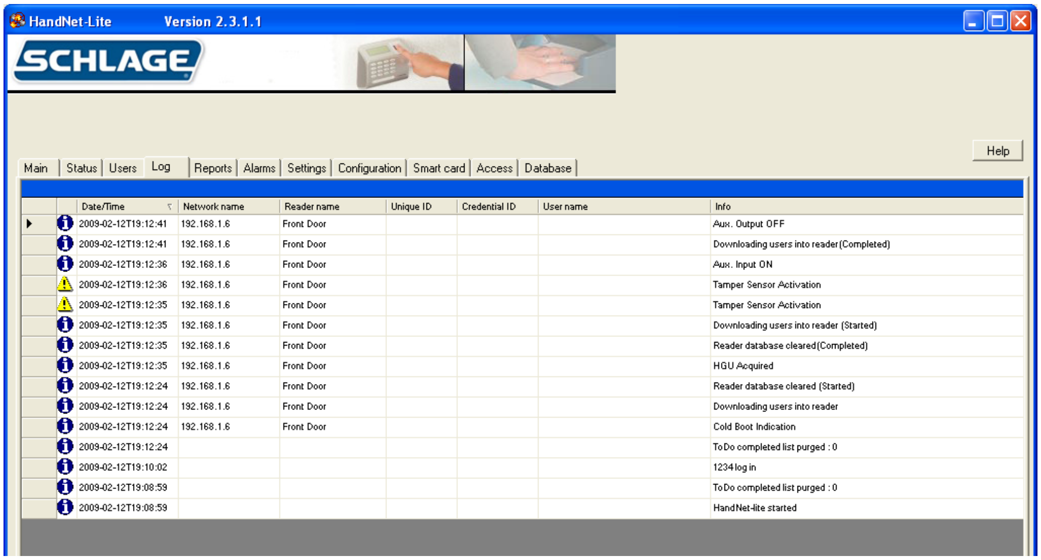
Figure 5-1: Example of RemoveUserXML.xml

```
<?xml version=”1.0” standalone=”yes”?>
<RemoveUser xmlns=”http://tempuri.org/RemoveUser.xsd”>
  <CRsiRemoveUser>
    <UserID>1000</UserID>
  </CRsiRemoveUser>
  <CRsiRemoveUser>
    <UserID>1001</UserID>
  </CRsiRemoveUser>
  <CRsiRemoveUser>
    <UserID>1002</UserID>
  </CRsiRemoveUser>
  <CRsiRemoveUser>
    <UserID>1003</UserID>
  </CRsiRemoveUser>
  <CRsiRemoveUser>
    <UserID>1004</UserID>
  </CRsiRemoveUser>
  <CRsiRemoveUser>
    <UserID>1005</UserID>
  </CRsiRemoveUser>
</RemoveUser>
```

Log Tab

The *Log* tab lists events that occur in any connected reader. It also lists any changes made in HandNet Lite.

Figure 6-1: Log Tab



	Date/Time	Network name	Reader name	Unique ID	Credential ID	User name	Info
ⓘ	2009-02-12T19:12:41	192.168.1.6	Front Door				Aux. Output OFF
ⓘ	2009-02-12T19:12:41	192.168.1.6	Front Door				Downloading users into reader(Completed)
ⓘ	2009-02-12T19:12:36	192.168.1.6	Front Door				Aux. Input ON
⚠	2009-02-12T19:12:36	192.168.1.6	Front Door				Tamper Sensor Activation
⚠	2009-02-12T19:12:35	192.168.1.6	Front Door				Tamper Sensor Activation
ⓘ	2009-02-12T19:12:35	192.168.1.6	Front Door				Downloading users into reader (Started)
ⓘ	2009-02-12T19:12:35	192.168.1.6	Front Door				Reader database cleared(Completed)
ⓘ	2009-02-12T19:12:35	192.168.1.6	Front Door				HGU Acquired
ⓘ	2009-02-12T19:12:24	192.168.1.6	Front Door				Reader database cleared (Started)
ⓘ	2009-02-12T19:12:24	192.168.1.6	Front Door				Downloading users into reader
ⓘ	2009-02-12T19:12:24	192.168.1.6	Front Door				Cold Boot Indication
ⓘ	2009-02-12T19:12:24						ToDo completed list purged : 0
ⓘ	2009-02-12T19:10:02						1234log in
ⓘ	2009-02-12T19:08:59						ToDo completed list purged : 0
ⓘ	2009-02-12T19:08:59						HandNet-lite started

Log Tab Fields

Table 6-6: Log Tab Fields

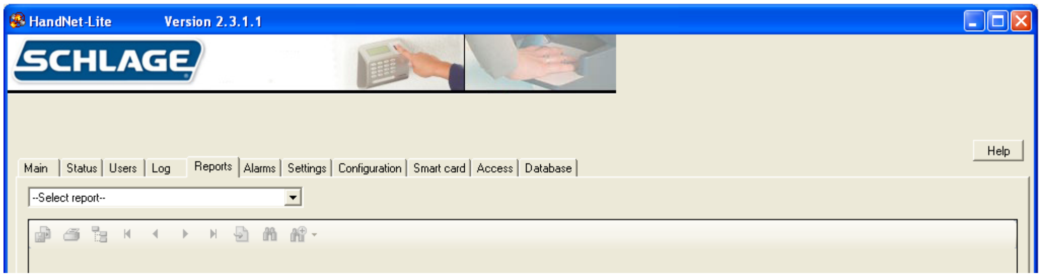
Column	Description
Event type (untitled)	One of the following icons: ⓘ: Indicates a standard informational message. ⚠: Indicates that the condition is important and warrants further investigation. These conditions are also listed on the Alarms tab.
Date/Time	Shows the date and time when the event occurred. The date is listed in year-month-day order, and the time lists hours:minutes:seconds
Network name	Network name if activity occurred at a reader
Reader name	Reader name if activity occurred at a reader
Unique ID	User's unique ID if event is associated with a particular user
Credential ID	User's credential ID if event is associated with a particular user
User name	User's name if message is event with a particular user
Info	Explanation of event

Click the heading of any row to sort the list by that heading. Click the heading again to reverse the sort order.

Reports Tab

The Reports tab is used to generate and view reports on users and readers.

Figure 7-1: Reports Tab



Generate a Report

1. Click the *Reports* tab.
2. Click the drop-down list at the top of the reports tab and choose the report you want to generate.

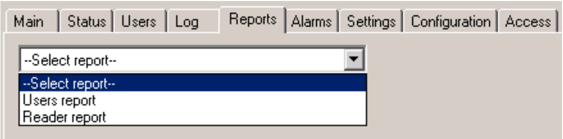
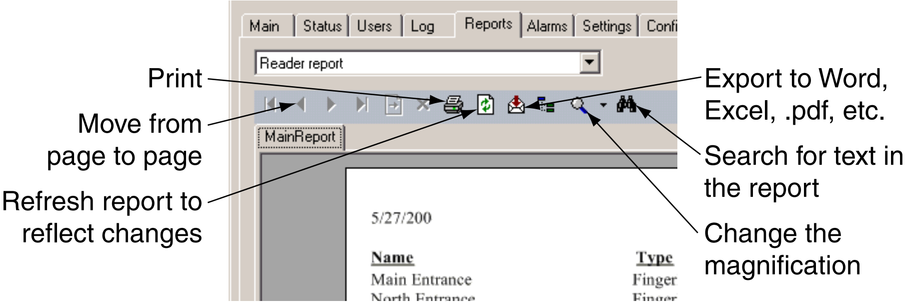


Table 7-7: Report Types

Report Type	Description
Users Report	Lists key information about every user in the system
Readers Report	Lists key information about every reader in the system

3. To print or move around in the report, click the corresponding icon in the bar above the report window.

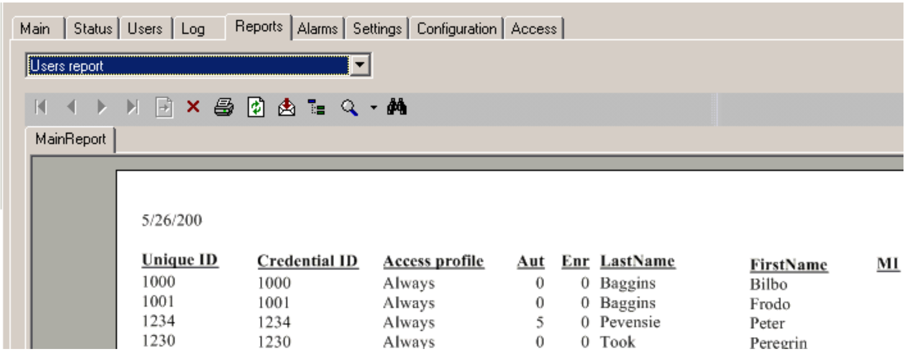


5/27/200

Name	Type
Main Entrance	Finger
North Entrance	Finger

Users Report

The Users report lists the information for each user in the program.



5/26/200

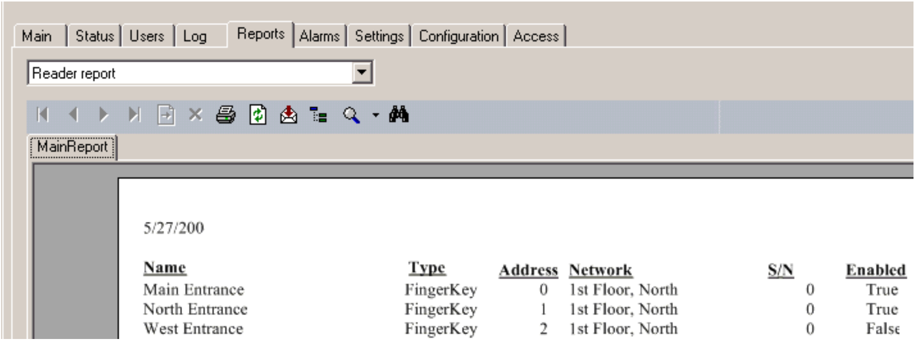
Unique ID	Credential ID	Access profile	Aut	Enr	LastName	FirstName	MI
1000	1000	Always	0	0	Baggins	Bilbo	
1001	1001	Always	0	0	Baggins	Frodo	
1234	1234	Always	5	0	Pevensie	Peter	
1230	1230	Always	0	0	Took	Peregrin	

Table 7-8: Users Report

Column	Description
Unique ID	User’s Unique identifier
Credential ID	User’s credential ID (card or manual ID)
Access Profile	Access profile associated with the user
Aut	User’s authority level
LastName	• User’s last name • If you added the user at the reader and have not changed the name, user ID is listed
FirstName	• User’s first name • If you added the user at the reader and have not changed the name, user ID is listed
MI	User’s middle initial.

Reader Report

The Reader report lists information for each reader in the program.



5/27/200

Name	Type	Address	Network	S/N	Enabled
Main Entrance	FingerKey	0	1st Floor, North	0	True
North Entrance	FingerKey	1	1st Floor, North	0	True
West Entrance	FingerKey	2	1st Floor, North	0	False

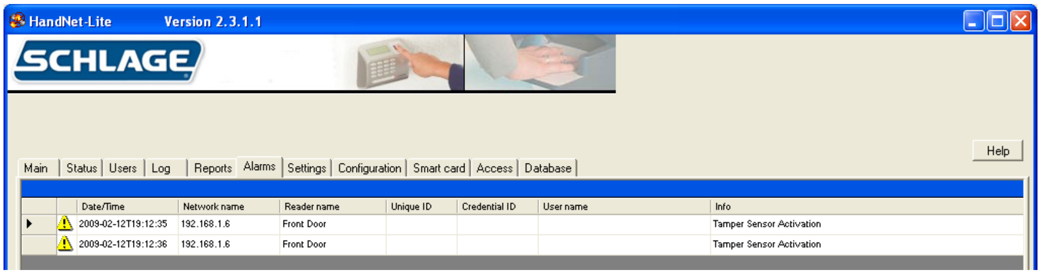
Table 7-9: Reader Report

Column	Description
Name	Reader’s name
Type	Indicates whether the reader is a hand or fingerprint reader
Address	Reader’s address
Network	Network to which reader is connected
S/N	Reader’s internal serial number
Enabled	• true: program attempts to communicate with the reader • false: program does not attempt to communicate with the reader

Alarms Tab

The *Alarms* tab shows all alarms that have been recorded in the system. Alarms are also listed with the rest of the activity in the *Log* tab

Figure 8-1: Alarms Tab



Date/Time	Network name	Reader name	Unique ID	Credential ID	User name	Info
2009-02-12T19:12:35	192.168.1.6	Front Door				Tamper Sensor Activation
2009-02-12T19:12:36	192.168.1.6	Front Door				Tamper Sensor Activation

Alarms Fields

Table 8-10: Alarms Fields

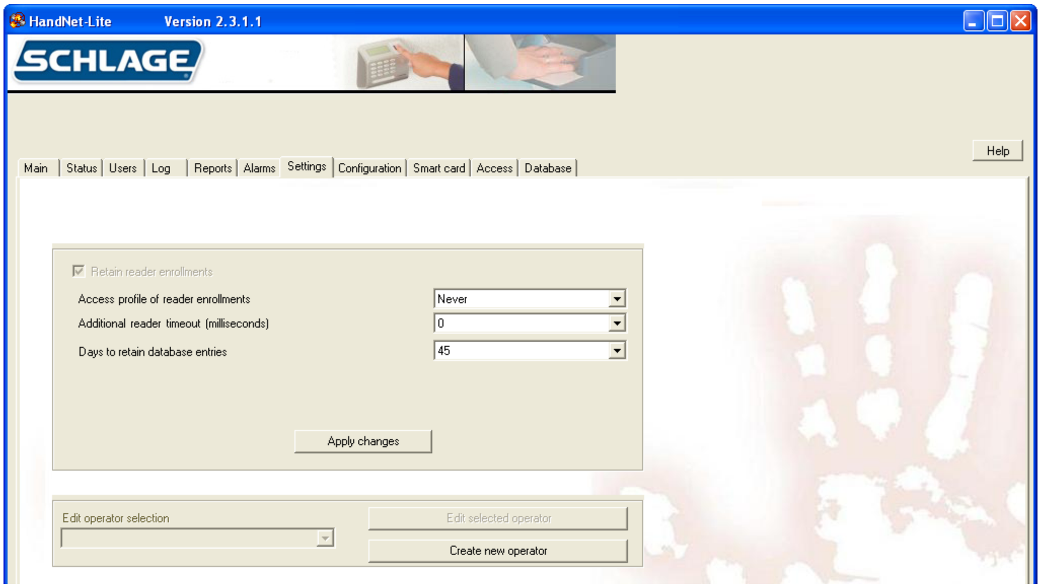
Column	Description
Date/Time	Date and time when the alarm occurred. The date is listed in year-month-day order, and the time lists hours:minutes:seconds
Network name	Network name if alarm is associated with a particular reader
Reader name	Reader name if alarm is associated with a particular reader
Unique ID	User's unique ID if alarm is associated with a particular user
Credential ID	User's credential ID if alarm is associated with a particular user
User name	User's name if alarm is associated with a particular user
Info	Description of alarm

Click the heading of any row to sort the list by that heading. Click the heading again to reverse the sort order.

Settings Tab

The *Settings* tab allows you to set default settings and add operators to the system.

Figure 9-1: Settings Tab



HandNet-Lite Version 2.3.1.1
SCHLAGE
Help
Main | Status | Users | Log | Reports | Alarms | Settings | Configuration | Smart card | Access | Database
Apply changes
Edit selected operator
Create new operator

☑ Retain reader enrollments

Access profile of reader enrollments: Never

Additional reader timeout (milliseconds): 0

Days to retain database entries: 45

Edit operator selection

Settings Fields

Table 9-11: Settings Fields

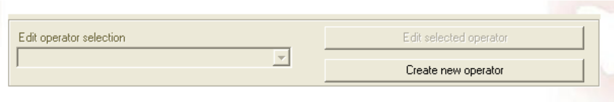
Setting	Description
Retain reader enrollments	This box is always checked and cannot be changed.
Access profile of reader enrollments	• Access profile assigned to users by default when users are added at a reader before being added in the system. • Choices are Always, Never or any custom profiles created by an operator. See Access Tab on page 61 for more informaiton.
Additional reader timeout	• Additional time that is added globally to the command timeout. • Select additional time if command timeout errors are generated on the network. These errors would be displayed on the Alarms tab. See Alarms Tab on page 23 for more information.
Days to retain expired database entries	• Number of days expired database entries are retained • Choose default of 45 days initially. If database becomes too large, make this number smaller.

Managing Operators

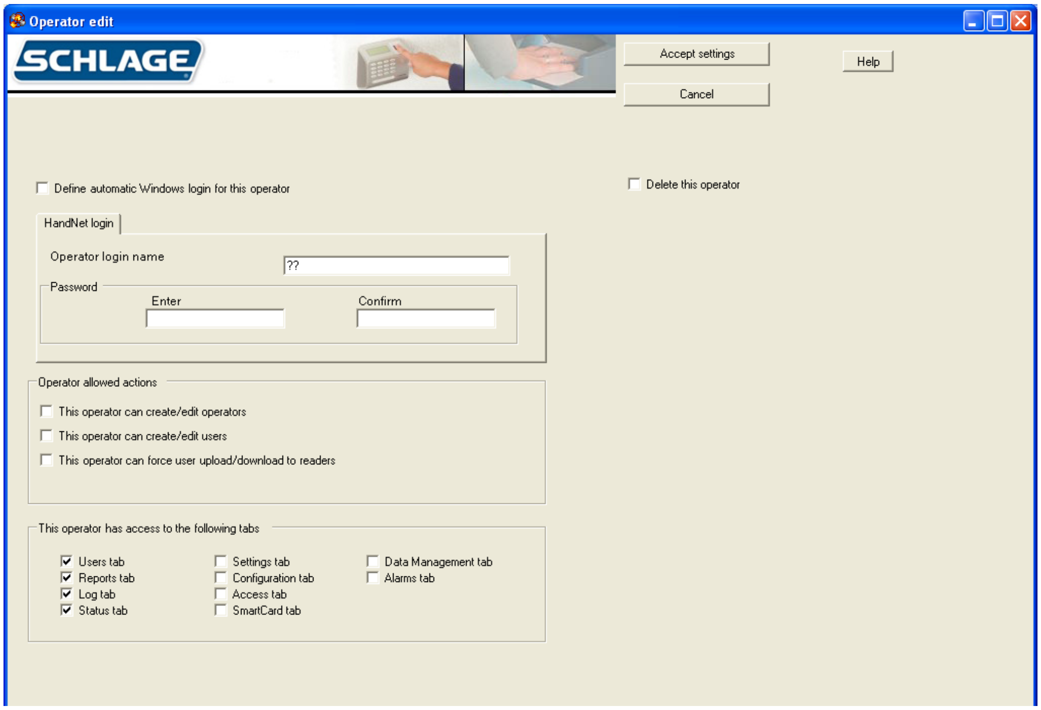
Operators are individuals who can control the system. The level of control can be set individually for each operator.

Add a New Operator

1. Click the *Settings* tab.
2. Click the *Create new operator* button.



The Operator edit screen will appear:



□ Define automatic Windows login for this operator

□ Delete this operator

HandNet login

Operator login name ??

Password

Enter

Confirm

Operator allowed actions

□ This operator can create/edit operators

□ This operator can create/edit users

□ This operator can force user upload/download to readers

This operator has access to the following tabs

☑ Users tab	□ Settings tab	□ Data Management tab
☑ Reports tab	□ Configuration tab	□ Alarms tab
☑ Log tab	□ Access tab	
☑ Status tab	□ SmartCard tab	

3. Click the *Define automatic Windows login for this operator* box to use Windows login information for this operator. See Enable Automatic Windows Login 27.
4. Enter a login name in the operator login name box. This name is case sensitive.
5. Enter the password and confirmation in the enter and confirm boxes. The password is case sensitive.
6. Choose the operator allowed actions by clicking the corresponding check box(es).
7. Choose the tabs to which the operator has access by clicking the corresponding check box(es).
8. Click the *Accept Settings* button.

Edit an Operator

1. Click the *Settings* tab.
2. Select the operator you want to edit from the *Edit operator selection* drop-down box.
3. Click *Edit selected operator* button.
4. Edit the necessary settings. See Add a New Operator on page 26 for more information.
5. Click the *Accept Settings* button.

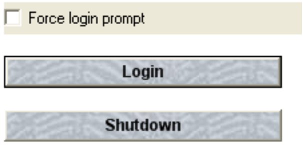
Delete an Operator

1. Click the *Settings* tab.
2. Select the operator you want to delete from the *Edit operator selection* drop-down box.
3. Click the *Delete this operator* check box.
4. Click the *Accept Settings* button.

Enable Automatic Windows Login

If you wish to allow automatic Windows login for HandNet Lite:

1. Click the *Main* tab.
2. Log off.
3. Click to un-check the *Force login prompt* checkbox.
4. Shut down HandNet Lite. The next time you start HandNet Lite, you will be automatically logged in.



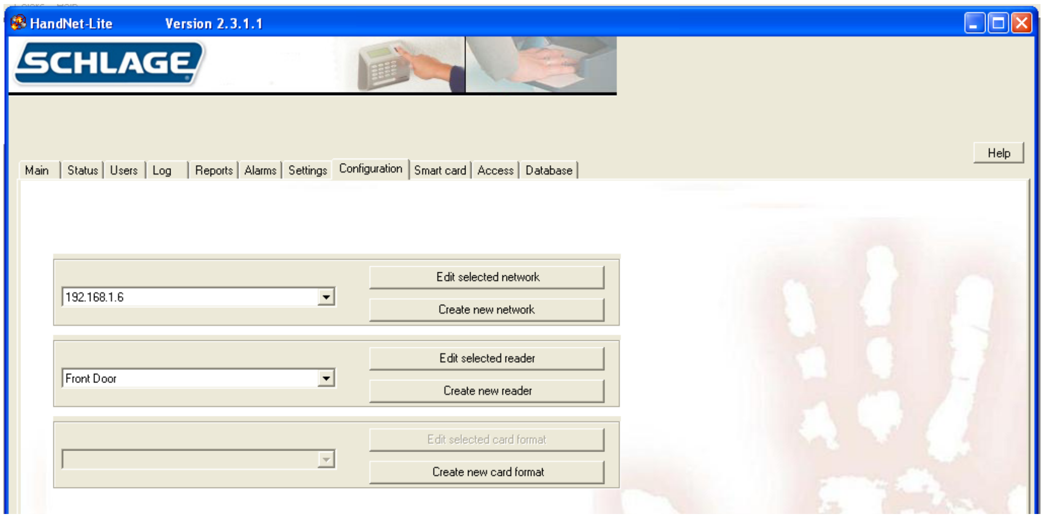
Disable Automatic Windows Login

1. Click the *Main* tab
2. Log off.
3. Click to check the *Force login prompt* checkbox.
4. Shut down HandNet Lite. The next time you start HandNet Lite, you will be prompted for login name and password.

Configuration Tab

The *Configuration* tab is used to add or edit networks, readers and card formats.

Figure 10-1: Configuration Tab



192.168.1.6

Front Door

Managing Networks

A network is a group of up to 32 daisy-chained readers connected though a single serial port using 2 wire RS485, a single reader connected to a computer with RS232, or a single TCP/IP (ethernet) reader. (See the reader manual for wiring and connection detail.)

You control access to each reader separately using HandNet Lite, so having readers with unrelated purposes in one network is fine.

There are two parts to setting up a network and readers: you must physically set the readers up and connect them to each other and to the computer, and you must add the network and readers in HandNet Lite. This manual only explains how to set up the network and readers in HandNet Lite. For help setting up and connecting the readers, see the manual that came with the readers.

Add a Network

1. Click the *Configuration* tab.
2. Click the *Create new network* button
3. Choose the Network type from the drop-down box. The remaining fields displayed will be determined by this selection.
4. Complete the fields on the screen. See page 30 for TCP/IP network. See page 32 for Serial network.
5. Click *Accept settings*.

Edit a Network

1. Click the *Configuration* tab.
2. Select the network you want to edit from the drop-down box.
3. Click the *Edit selected network* button
4. Complete the fields on the screen. See page 30 for TCP/IP network. See page 32 for Serial network.
5. Click *Accept settings*.

Delete a Network

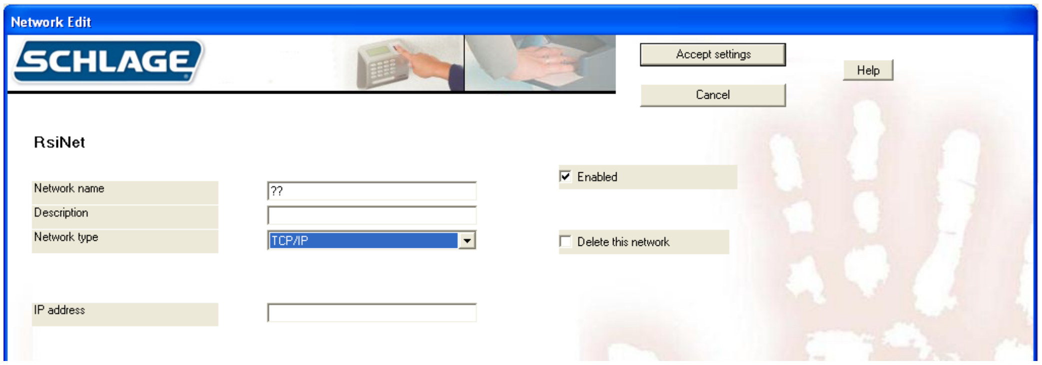
Only networks with no readers can be deleted.

1. Click the *Configuration* tab.
2. Select the network you want to delete from the drop-down box.
3. Click the *Edit selected network* button
4. Click the *Delete this network* check box.
5. Click *Accept settings*.

Connecting through a TCP/IP network

To connect to a site through the network, you must have a TCP/IP network with static IP addresses. Your computer must have a network card and be connected to the network. If the network is faster than 10baseT, you must have a switching hub. To use TCP/IP, you must have either ordered readers with the Ethernet option enabled or purchased an Ethernet upgrade.

Figure 10-2: Edit a TCP/IP Network



RsiNet

Network name: ??

Description:

Network type: TCP/IP

IP address:

☑ Enabled

□ Delete this network

Table 10-12: TCP/IP Network Fields

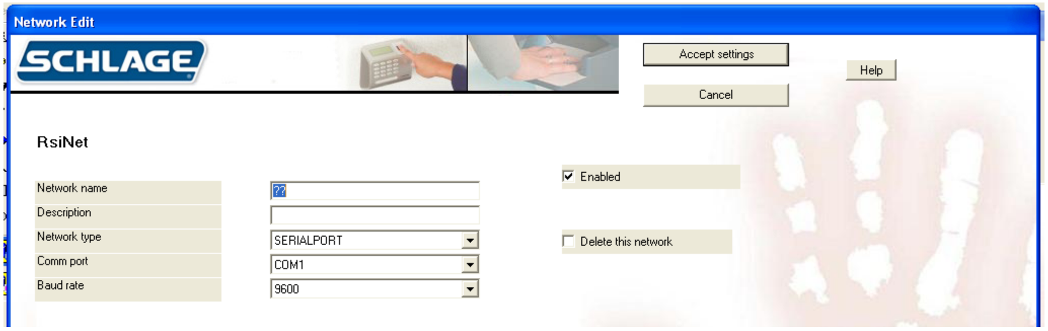
Field	Req'd?	Description
Network Name	Yes	• Name of the network • Any combination of letters, numbers, spaces, and special characters, up to 30 characters long
Description	No	Brief description of the network

Field	Req'd?	Description
Enabled	No	• Must be checked for HandNet Lite to communicate with the network and monitor any readers connected to it. • Generally you would only uncheck this if you were in the process of setting up or reconfiguring the network and didn't want the program to try to communicate • Having the Enabled box checked if the network isn't really connected to HandNet Lite causes the program to slow down significantly. Make sure that this is only checked if the network is actually set up and connected
Delete This Network	No	• Check to delete this network and remove it from the Schlage Biometrics network selection list. If there are no readers in the network, it will be deleted when you click Accept settings. • You can't delete a network with readers on it
Network Type	Yes	• Choose Serial port or TCP/IP • The remaining fields will be determined by this selection.
IP address	Yes	• Only available if TCP/IP was chosen in the Network type field. • The IP address (xxx.xxx.xxx.xxx) of the reader • Must match the IP address set in the reader. See the reader manual for more information • Ask your network administrator for an appropriate address

Connecting through a serial port

To connect to a site by running a cable from your computer to the reader, you must have a free serial port on your computer. See the reader manual for more on the requirements for the cable.

Figure 10-3: Serial Network Edit Screen



RsiNet

Network name	??
Description	
Network type	SERIALPORT
Comm port	COM1
Baud rate	9600

☑ Enabled

□ Delete this network

Table 10-13: Serial Network Fields

Field	Req'd?	Description
Network Name	Yes	• Name of the network • Any combination of letters, numbers, spaces, and special characters, up to 30 characters long
Description	No	• Brief description of the network
Enabled	No	• Must be checked for the system to communicate with the network and monitor any readers connected to it. • Uncheck when in the process of setting up or reconfiguring the network to keep the program from trying to communicate • If checked when the network is not really connected, the system will slow down significantly.
Delete This Network	No	• Check to delete this network and remove it from the network selection list. • You cannot delete a network with readers in it
Network Type	Yes	• Choose Serial port or TCP/IP • The remaining fields will be determined by this selection.
Comm Port	Yes	• Only available if Serial port was chosen in the Network type field. • Must match the serial port to which the reader is connected • Only the ports that are currently available on your computer are listed.

Field	Req'd?	Description
Baud Rate	Yes	• Only available if Serial port was chosen in the Network type filed. • Choose from values of 4800, 9600, 19200, 28800, 38400, or 57600. • Choose 9600 initially. Increase the rate after a working connection has been established. Longer wire distances require lower rates. • Must match the rate set in all readers on the network. See the reader manual for more information.

Managing Readers

There are two parts to setting up readers: physically setting up the readers and connecting them to each other and to the computer, and adding the network and readers in HandNet Lite. This manual only explains adding the network and readers in HandNet Lite. For help setting up and wiring readers, see the manual that came with the readers.

Before you add readers, you must set up the network to which they are connected. See Add a Network on page 29 for more information.

If You've Been Using Readers Already

If you've been using readers without HandNet Lite, when you add the network and readers to the system, HandNet Lite automatically gets the users from the readers and adds them to the system; see How Users Are Enrolled and Added to HandNet Lite on page 39.

Add a Reader

1. Click the *Configuration* tab.
1. Select the network in which the new reader will exist from the network drop-down box.
2. Click the *Create new reader* button.
3. Choose the *Reader type* from the drop-down box. The entries on the screen will differ depending on the reader type chosen.
4. Fill in the entries on the Reader Edit screen. See page 35 for FingerKey. See page 37 for HandKey.
5. Click the *Test reader* button. If the reader is properly configured, the reader will be able to communicate.
6. To change the security settings for the reader, click the *Security settings* button. See Security Settings Screen on page 40 for more information.
7. If you are editing a FingerKey and want to edit the fingerprint settings, click the *Fingerprint settings* button. See Fingerprint Settings Screen on page 41 for more information.
8. Click the *Accept settings* button.

Edit a Reader

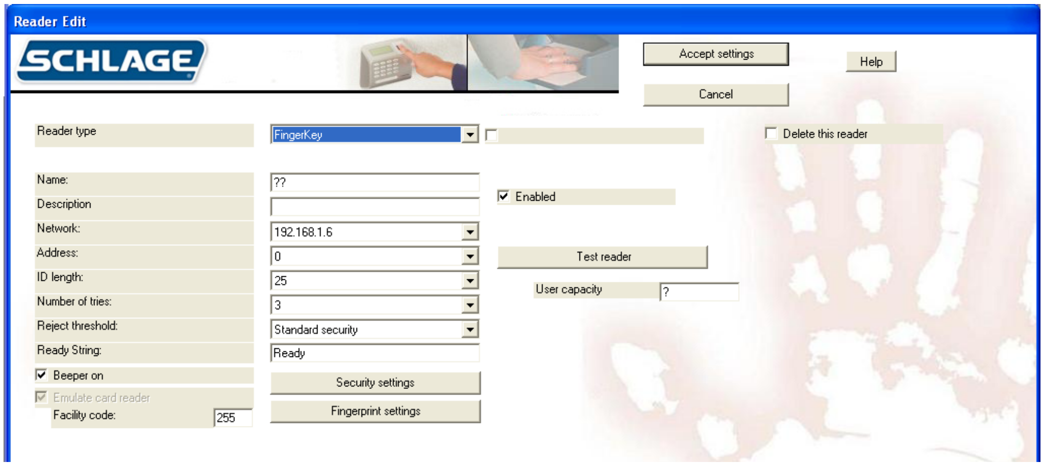
1. Click the *Configuration* tab.
1. Select the network in which the reader you want to edit exists in the network drop-down box.
2. Click the *Edit selected reader* button.
3. The entries on the screen will differ depending on the reader type chosen.
4. Fill in the entries on the Reader Edit screen. See page 35 for FingerKey. See page 37 for HandKey.
5. Click the *Test reader* button. If the reader is properly configured, the reader will be able to communicate.
6. To change the security settings for the reader, click the *Security settings* button. See Security Settings Screen on page 40 for more information.
7. If you are editing a FingerKey and want to edit the fingerprint settings, click the *Fingerprint settings* button. See Fingerprint Settings Screen on page 41 for more information.
8. Click the *Accept settings* button.

Delete a Reader

1. Click the *Configuration* tab.
1. Select the network in which the reader you want to delete exists in the network drop-down box.
2. Click the *Edit reader* button.
3. Click the *Delete this reader* check box.
4. Click the *Accept settings* button.

FingerKey Reader Edit Screen

Figure 10-4: FingerKey Reader Edit Screen



Reader type: FingerKey □

□ Delete this reader

Name: ??

Description:

Network: 192.168.1.6

Address: 0

ID length: 25

Number of tries: 3

Reject threshold: Standard security

Ready String: Ready

☑ Beeper on

☑ Emulate card reader

Facility code: 255

☑ Enabled

User capacity ?

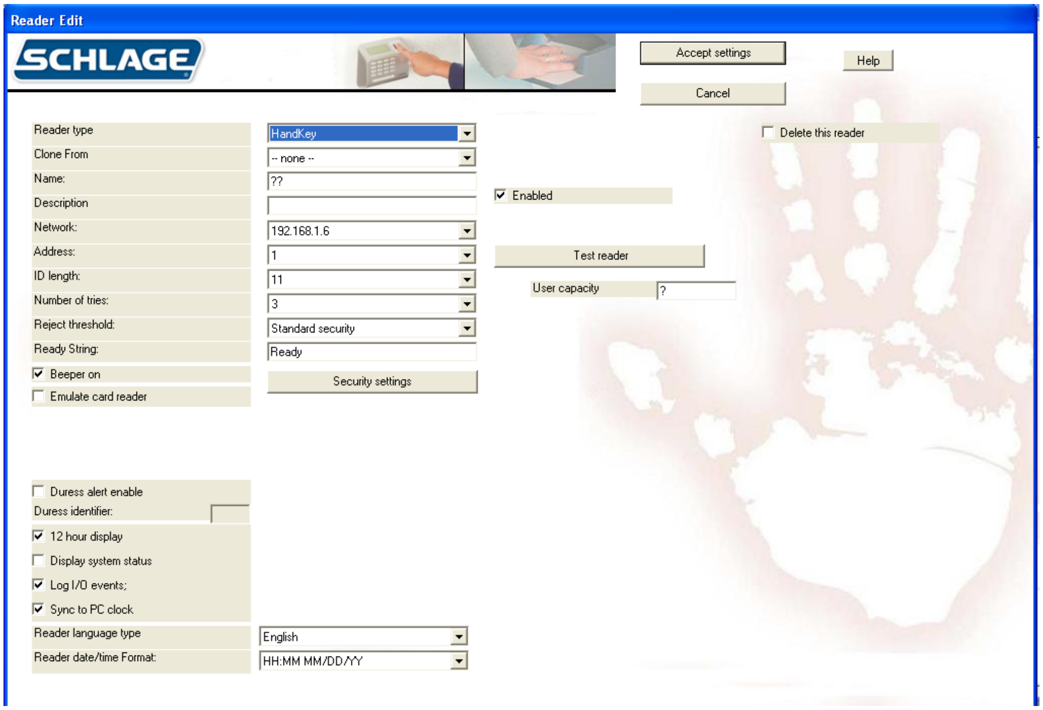
Table 10-14: FingerKey Reader Fields

Field	Req'd?	Description
Clone From	No	• Appears only after at least one reader has been configured. • Allows you copy the settings from another reader, including the underlying Fingerprint and Security Settings. • If this option is chosen, all of the following fields will be populated automatically.
Name	Yes	Any combination of letters, numbers, spaces, and special characters, up to 30 characters.
Description	No	Briefly describe the reader.
Network	Yes	• Select the network in which the reader exists. • Network must be set up before you can add the reader. See Add a Network on page 29 for more information.
Address	Yes	• Must match the address set in the reader. See the reader's manual for information on setting the address in the reader. • Field will be automatically populated with the first available address that hasn't been used. Choose another number from the pull-down list if desired. • Changing the address on this screen does NOT change the address in the physical reader. If you change an address here, you must also change the address in the reader.
ID Length	No	• If all user IDs are the same length, choose the number of digits here (any value from 1-25) so users don't have to press enter after typing the ID at the reader. • If user IDs are different lengths, choose the longest number of digits. Users with the longest IDs will not have to press ENTER after typing the ID at the reader. • Entry does not affect the length of IDs on cards. It only affects IDs entered at the keypad.

Field	Req'd?	Description
Number of Tries	Yes	• Controls how many times the user can try to get access before the reader will block the user's ID and not allow further tries. • Prevents someone from making repeated tries to gain access with someone else's ID. • Normally 3 is a good setting.
Reject threshold	Yes	• The lower this number is, the more closely the user's finger must match the template of the finger stored in the FingerKey. • 30 (the lowest possible number) requires the fingerprint to match very closely; 250 (the highest possible number) will grant access if the finger match is close but not exactly the same. • 75 is good for most contexts. Choose a lower number if you have an especially high security situation. • If particular users have trouble placing their fingers consistently, you can override the reader's setting for an individual user on the User edit screen in the Users window. See Edit a User on page 12 for more information.
Ready String	Yes	• This text appears in the reader display when the reader is ready and waiting for the user to enter an ID. • Any combination of letters, numbers, spaces, and special characters, up to 20 characters
Beeper On	No	• When checked, the reader beeps each time you press a button • In a high security setting, you might want the beeps off to make it harder for a casual observer to figure out how many digits are in the ID number.
Emulate Card Reader	Yes	• FingerKey readers always emulate a card reader, so you can't uncheck this box
Facility Code	Yes	• Facility code that should be passed to the access control panel. • Numeric value from 0 (zero) to 65535
Enabled	No	• Check if the reader is physically set up and ready to be used. • Checking the Enabled box if the reader is not really connected slows the program down significantly. Make sure this is only checked if the reader is actually set up and connected
User capacity	Yes	• Will be filled in automatically by the reader.
Delete This Reader	No	• Check ONLY to delete reader and remove it from the reader selection list.

HandKey Reader Edit Screen

Figure 10-5: HandKey Reader Edit Screen



Reader type: HandKey

Clone From: -- none --

Name: ??

Description:

Network: 192.168.1.6

Address: 1

ID length: 11

Number of tries: 3

Reject threshold: Standard security

Ready String: Ready

☑ Beeper on

☐ Emulate card reader

☐ Duress alert enable

Duress identifier:

☑ 12 hour display

☐ Display system status

☑ Log I/O events;

☑ Sync to PC clock

Reader language type: English

Reader date/time Format: HH:MM MM/DD/YY

☑ Enabled

User capacity ?

☐ Delete this reader

Table 10-15: HandKey Reader Fields

Field	Req'd?	Description
Clone From	No	• Appears only after at least one reader has been configured. • Allows you copy the settings from another reader, including the underlying Fingerprint and Security Settings. • If this option is chosen, all of the following fields will be populated automatically.
Name	Yes	Any combination of letters, numbers, spaces, and special characters, up to 30 characters.
Description	No	Briefly describe the reader. You may leave this blank if you wish
Network	Yes	• Select the network in which the reader exists. • Network must be set up before you can add the reader. See Add a Network on page 29 for more information.

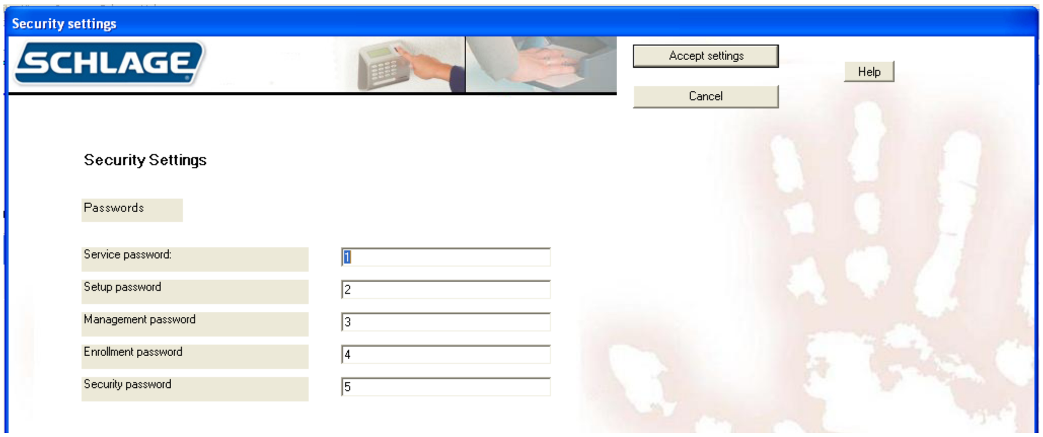
Field	Req'd?	Description
Address	Yes	• Must match the address set in the reader. See the reader's manual for information on setting the address in the reader. • Field will be automatically populated with the first available address that hasn't been used. • Choose another number from the pull-down list if desired. • Changing the address on this screen does NOT change the address in the physical reader. If you change an address here, you must set the reader to the same address or the program won't be able to communicate with the reader
ID Length	No	• If all user IDs are the same length, choose the number of digits here (any value from 1-25) so users don't have to press enter after typing the ID at the reader. • If user IDs are different lengths, choose the longest number of digits. Users with the longest IDs will not have to press ENTER after typing the ID at the reader. • Entry does not affect the length of IDs on cards. It only affects IDs entered at the keypad.
Number of Tries	Yes	• Controls how many times the user can try to get access before the reader will block the user's ID and not allow further tries. • Prevents someone from making repeated tries to gain access with someone else's ID. • Normally 3 is a good setting.
Reject threshold	Yes	• The lower this number is, the more closely the user's finger must match the template of the finger stored in the FingerKey. • 30 (the lowest possible number) requires the fingerprint to match very closely; 250 (the highest possible number) will grant access if the finger match is close but not exactly the same. • 75 is good for most contexts. Choose a lower number if you have an especially high security situation. • If particular users have trouble placing their fingers consistently, you can override the reader's setting for an individual user on the User edit screen in the Users window. See Edit a User on page 12 for more information.
Ready String	Yes	• This text appears in the reader display when the reader is ready and waiting for the user to enter an ID. • Any combination of letters, numbers, spaces, and special characters, up to 20 characters

Field	Req'd?	Description
Beeper On	No	• When checked, the reader beeps each time you press a button • In a high security setting, you might want the beeps off to make it harder for a casual observer to figure out how many digits are in the ID number.
Emulate Card Reader	Yes	• Controls the Output Mode of teh reader (Lock Output mode if unchecked, Card Reader Emulation Output if checked).
Enabled	No	• Check if the reader is physically set up and ready to be used. • Checking the Enabled box if the reader is not really connected slows the program down significantly. Make sure this is only checked if the reader is actually set up and connected
User capacity	Yes	• Contains the number of users the reader is capable of storing (this field is filled in after the Test Reader button is pressed)
Delete This Reader	No	• Check ONLY to delete reader and remove it from the reader selection list.
Duress alert enable	No	• If checked, duress activates AUX output
Duress identifier	No	• This is the key which, when pressed, will generate the DURESS event. • Must be a digit 0 through 9. Other values will disable the duress feature.
12 hour display	No	• If checked, displays terminal time in 12 hour format, otherwise 24 hour time format.
Display system status	No	• If checked, the reader's LCD will display system status on line 2. If unchecked, line 2 of the LCD will display the unit's date and time.
Log I/O events	No	• Currently ignored by HandKey units, I/O Events will always generate a DataLog
Sync to PC clock	No	• The reader's clock will be synchronized to this PC's system time.
Reader language type	No	• Selects the language used on the reader for LCD prompts.
Reader date/time Format	No	• Selects the format that the reader will display date & time on the LCD display.

Security Settings Screen

The Security Settings Screen controls the passwords needed to access the menus in the reader.

Figure 10-6: Security Settings Screen



Service password: 1

Setup password: 2

Management password: 3

Enrollment password: 4

Security password: 5

Generally the default passwords shown above are adequate since a user must be set up with the appropriate Authority level on the User edit screen in the Users window (see page 12 for more information), and the user must know how to get to these menus in the reader before the passwords below would do any good.

Edit Security Settings

1. Click the *Configuration* tab.
2. Select the network in which the reader you want to edit exists in the network drop-down box.
3. Select the reader you want to edit from the reader drop-down box.
4. Click the *Edit selected reader* button.
5. Click the *Security settings* button.
6. Edit the passwords. See the Security Settings Fields Table on page 40 for more information.
7. Click the *Accept settings* button.

Table 10-16: Security Settings Fields

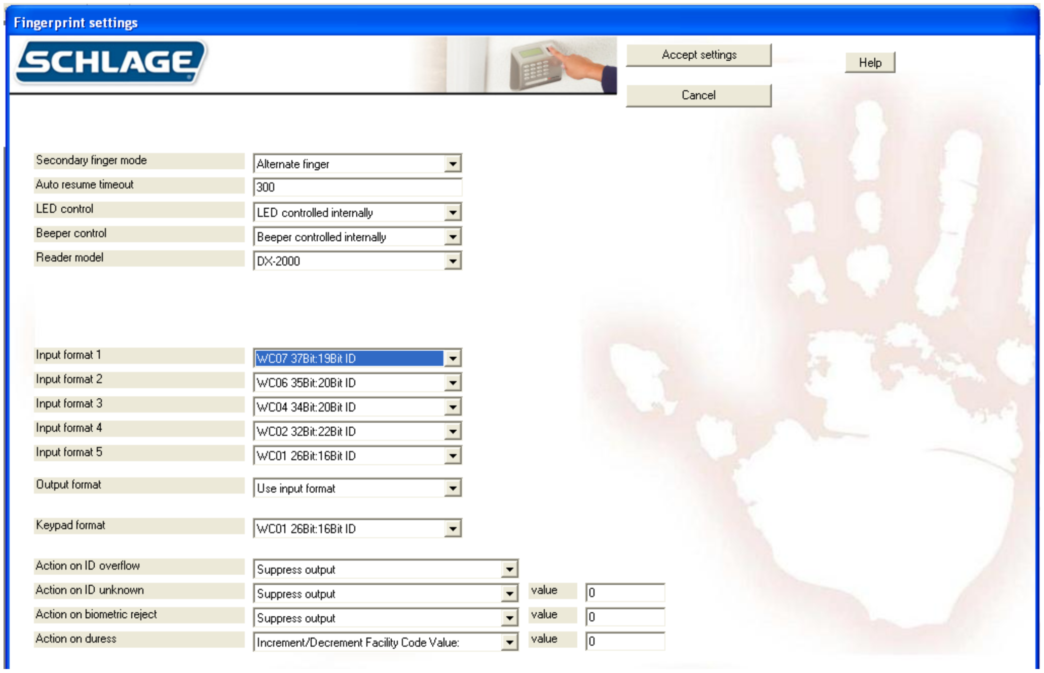
Field	Req'd	Description
Service	Yes	Allows the master reader display the status of all readers on the network
Setup	Yes	Controls reader setup including the reader's address, ID length, auxiliary output settings, facility codes, network configuration, the duress indicator, etc. It also contains an option to upgrade the maximum number of users
Management	Yes	Allows display of a list all of the users in the reader and lets the master reader send/acquire user databases to/from readers in a network
Enrollment	Yes	Allows you to add or remove users
Security	Yes	Allows you to customize user settings, control how closely user fingerprints must match templates, set the menu passwords, clear all the users from reader, etc

For more detail on the reader menus, see the reader manual.

Fingerprint Settings Screen

The Fingerprint Settings screen controls a number of the reader's internal settings.

Figure 10-7: Fingerprint Settings Screen



Secondary finger mode	Alternate finger		
Auto resume timeout	300		
LED control	LED controlled internally		
Beeper control	Beeper controlled internally		
Reader model	DX-2000		
Input format 1	WC07 37Bit:19Bit ID		
Input format 2	WC06 35Bit:20Bit ID		
Input format 3	WC04 34Bit:20Bit ID		
Input format 4	WC02 32Bit:22Bit ID		
Input format 5	WC01 26Bit:16Bit ID		
Output format	Use input format		
Keypad format	WC01 26Bit:16Bit ID		
Action on ID overflow	Suppress output		
Action on ID unknown	Suppress output	value	0
Action on biometric reject	Suppress output	value	0
Action on duress	Increment/Decrement Facility Code Value:	value	0

Edit Fingerprint Settings

1. Click the *Configuration* tab.
2. Select the network in which the reader you want to edit exists in the network drop-down box.
3. Select the reader you want to edit from the reader drop-down box.
4. Click the *Edit selected reader* button.
5. Click the *Fingerprint settings* button.
6. Edit the necessary fields. See the Fingerprint Settings Fields table on page 41 for more information.
7. Click the *Accept settings* button.

Table 10-17: Fingerprint Settings Fields

Field	Req'd?	Description
Secondary Finger Mode	Yes	• Disabled: reader collects only one finger for each user. • Alternate finger: Scan of second finger grants access exactly as the first does. If user cannot verify with one finger, the other enrolled finger can be used. • Duress finger: Scan of second finger grants access and triggers a duress alarm. (Accomplished by either sending an alternate facility code or with reverse parity, depending on how your access control panel is set up.)

Field	Req'd?	Description
Auto Resume Timeout	Yes	• Number of seconds that reader stays in idle mode after being set into idle mode by a host command. • Number between 60 and 65535 • Default value is 300. • DO NOT change this setting unless advised to by technical support
LED Control	Yes	• Determines what controls the reader's LED display. • LED controlled internally: reader controls the LED display • LED controlled externally: access control panel control the LED display • For more information on setting up the LED control, see the reader's manual.
Beeper Control	Yes	• Determines what controls the reader's beeper. • Beeper controlled internally: reader controls beeper • Beeper controlled externally: access control panel controls beeper • For more information on setting up the beeper control, see the manual that came with the readers.
Reader Model	Yes	• Select the FingerKey model type from the drop down choices which are: • DX-2000 - Select this if you are using a DX-2000 model FingerKey. • DX-2100 HID Prox - Select this if you are using a DX-2100 model FingerKey using HID Prox cards. • DX-2200 HID iClass - Select this if you are using a DX-2200 model FingerKey with HID iClass cards. • DX-2400 Philips Mifare Standard - Select this if you are using a DX-2400 model FingerKey with Mifare Standard cards and settings. • DX-2400 Philips Mifare DESFire - Select this if you are using a DX-2400 model FingerKey with Mifare DESFire cards and settings.
iCLASS Configuration	Yes	• Choose None unless you are using iCLASS readers and cards. • If using iCLASS readers and cards, choose any iCLASS configuration that you've defined. • See Add an iCLASS Definition on page 50 for more information.
Mifare standard Configuration	Yes	• Choose None unless you are using Mifare Standard readers and cards. • If using Mifare Standard readers and cards, choose any Mifare Standard definition that you've defined. • See Add a Mifare Standard Definition on page 57 for more information.

Field	Req'd?	Description
DESFire Configuration	Yes	• Choose None unless you are using Mifare DESFire readers and cards. • If using Mifare DESFire readers and cards, choose any Mifare DESFire definition that you've defined. • See Add a DESFire Definition on page 55 for more information.
Input Format 1-5	Yes	• Card formats reader will accept from an internal or external card reader. • Choose either Wiegand or Magstripe formats but not both. Most companies use only one format. See the Card Formats table on page 65 for more information. • If you change from Wiegand to Magstripe format, or from Magstripe to Wiegand, you must reboot the reader. See the reader manual for further detail
Output Format	Yes	• Format reader sends to the access control panel if you use an internal or external card reader. • Use Input Format: Passes through whatever format is received • None: Reader sends no output when the ID is entered with a card. • Formats 1-11: Choose one of the formats from the Card Formats table on page 65.
Keypad Format	Yes	• Format the reader sends to the access control panel when a user enters his ID on the keypad instead of using a card. • None: Reader sends no output when the ID is entered with the keypad. • Formats 1-11: Choose one of the formats from the Card Formats table on page 65.
Action on ID Overflow	Yes	• Indicates what reader sends to access panel when card ID is longer than maximum length permitted by selected formats. • Suppress Output: Reader sends no output • Substitute all 1 bits: All 1 (one) bits are sent instead of the ID that was entered • Substitute all 0 bits: All 0 (zero) bits are sent instead of the ID that was entered

Field	Req'd?	Description
Action on ID Unknown	Yes	• Controls what the reader sends the access panel when ID is not recognized • Suppress Output: reader sends no output • Alternate Facility Code Value: reader sends facility code entered in the value entry, instead of the normal facility code • Increment/Decrement Facility Code Value: Reader sends facility code increased or decreased by the amount in the Value entry. • Toggle All Parity Bits: reader toggles the output parity bits.
Action on Biometric Reject	Yes	• Controls what the reader sends the access panel when a valid ID is entered but the finger doesn't match the template. • Same four options here as for Action on ID Unknown
Action on Duress	Yes	• Controls what the reader sends the access panel when a user places a duress finger • Same four options here as for Action on ID Unknown
Value	Yes	• Number between 0 and 32767 • Used when either Alternate Facility Code Value, Increment/Decrement Facility Code Value is chosen in the previous three fields • Enter a minus (-) sign before the number if you want to decrement the value.

Enabling a Secondary Finger Later

If users are enrolled with Seconday finger mode disabled, only one finger will be collected. If Secondary finger mode is later changed, all users need to be removed and re-enrolled in order to obtain a template for the second finger. The first finger will still function normally, but the second finger functionality will not be available until the user is re-enolled.

Interpreting the Format Detail

In the explanation of the format detail, you'll see an elaboration on the format that looks like this:

```
         1         2
12345678901234567890123456
PFFFFFFFFIIIIIIIIIIIIIIIIP
EXXXXXXXXXXXX.............
.............XXXXXXXXXXXXO
```

The numbers at the top: Identify the bit numbers; this example has 26 bits.

F: Indicates which bits contain the facility code; in this example, bits 2-9 have the facility code.

I: Indicates which bits contain the ID; in this example, bits 10-25 contain the ID.**P/E/O/X/.:** P indicates a parity bit; the E under the first parity bit here indicates that this parity is even. The X's following indicate which bits are used to determine that parity bit; the periods following indicate that those bits are not used in determining that parity bit; in this example, bits 2-13 are used to determine parity bit 1, and bits 14-26 do not affect this parity bit. The O under the second parity bit (bit 26) indicates this parity bit is odd; the preceding X's indicate that bits 14-25 are used to determine this parity bit.

For a list of available card formats, see the Card Formats table on page 65.

Managing FingerKey Card Formats

Most users don't need to define additional formats; the predefined formats that we initially provide cover almost all situations. However, if you need some other Wiegand format, you can define any format that you want.

We don't recommend changing or deleting any of our standard card formats. If you need a format that is similar to one of our existing formats, choose to add a new format; there's an option on the screen that lets you clone (copy) an existing format; you can then change the copy rather than changing the original.

Add a Card Format

1. Click the *Configuration* tab.
2. Click the *Create new card format* button.
3. Complete the fields on the screen. See the Card Format Fields table on page 46 for more information.
4. Click the *Accept settings* button.

Edit a Card Format

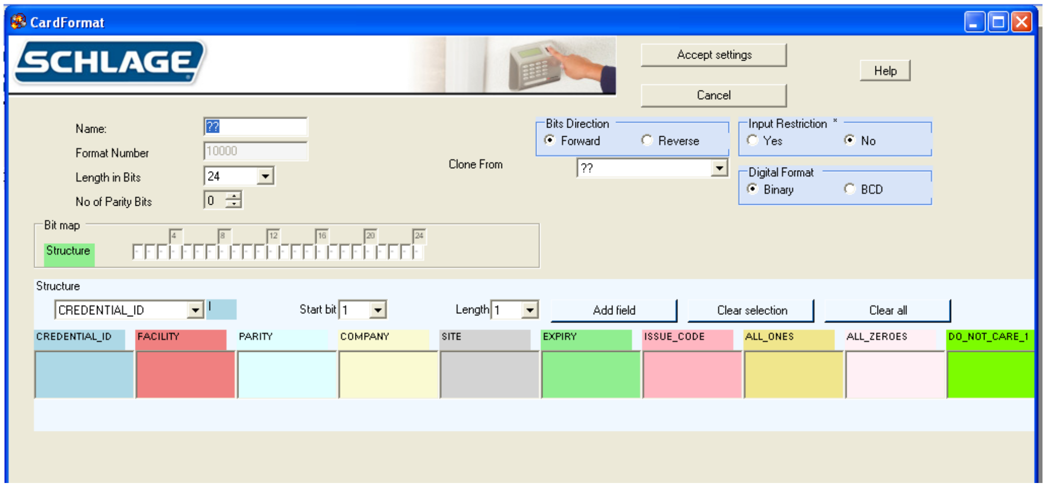
1. Click the *Configuration* tab.
2. Select the card format you want to edit from the drop-down box.
3. Click the *Edit selected card* format button.
4. Make changes to the fields on the screen. See the Card Format Fields table on page 46 for more information.
5. Click the *Accept settings* button.

Delete a Card Format

1. Click the *Configuration* tab.
2. Select the card format you want to edit from the drop-down box.
3. Click the *Edit selected card format* button.
4. Click the *delete* check box.
5. Click the *Accept settings* button.

Card Format Screen

Figure 10-8: The Card Format Screen



Name: ??

Format Number 10000

Length in Bits 24

No of Parity Bits 0

Clone From ??

Bits Direction ● Forward ○ Reverse

Input Restriction * ○ Yes ● No

Digital Format ● Binary ○ BCD

Structure

CREDENTIAL_ID

Start bit 1

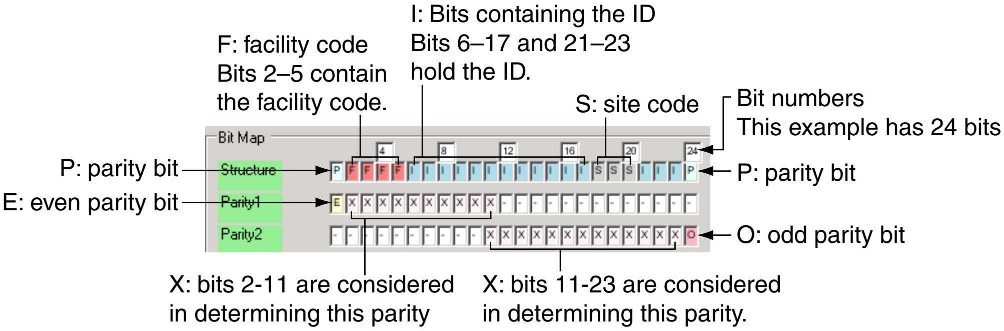
Length 1

The appearance of this screen varies depending on what you choose. The width of the Bit Map section changes based on the length you define for the ID. The Parity sections at the bottom only appear if you indicate that there are parity bits

Table 10-18: Card Format Fields

Field	Req'd?	Description
Name	Yes	Name that clearly identifies the format
Format Number	Yes	Internally generated number to identify the format. Cannot be changed.
Length in Bits	Yes	Number of bits in the format. This is the total number of bits, not just the number of bits in the ID
No of Parity Bits	No	If there are any parity bits, enter the number (1-4) here. For each parity bit specified here, a Parity section appears below
Bit Map	Yes	Structure of the format and how each bit is used. To change how different bits are used, see Card Format Structure on page 47, and the Bit Map example on page 47 for more information.
Delete	No	Deletes the current format.
Bits Direction	Yes	Forward: bits will be read in from left to right Reverse: bits will be read in from right to left
Clone From	No	Only appears if you are creating a new format. Allows you to make a copy of an existing format. Entries on the screen will be set to match the settings for the format you choose.
Input Restriction	Yes	Yes: only an exact format match will be accepted. Gives higher security since cards that are not issued by you will not be accepted. No: any input and parses will be accepted
Digital Format	Yes	Leave this set to Binary unless you understand what BCD is and have a specific reason for choosing it

Figure 10-9: Bit Map Example



Card Format Structure

1. Under Structure, choose the type of bit you want to add from the drop-down box.

   - Credential ID
   - Facility
   - Parity
   - Company
   - Site
   - Expiry
   - Issue Code
   - All Ones
   - All Zeros
   - Do Not Care 1
   - Do Not Care 0

   To add parity bits, see Set Up the Parity Bits on page 48 for more information
2. Choose the first bit you want to use for the structure from the *Start bit* drop-down box.
3. Choose the number of sequential bits from the *Length* drop-down box.
   - For example, if bits 2-11 should contain the ID, select 2 from the Start Bit drop-down box, and 10 from the Length drop-down box.
   - If a particular structure is broken up, the structure will be added in multiple steps. For example, if you have a 15 bit ID, but that ID is contained in bits 2–6, 8–12, and 14–18, add the Credential ID three times: the first time with a Start Bit of 2 and a Length of 5, the second time with a Start Bit of 8 and a Length of 5, and the third time with a Start Bit of 14 and a Length of 5.
   - Similarly, suppose a particular structure is scrambled. For example, suppose bit 2-11 are used for the ID, but instead of being in order, bit 9 is the first bit of the ID, bit 3 is the second, etc. You would simply add this one bit at a time, starting with the first bit (bit 9), then the second, etc. Bits are considered in the order they appear in the structure list. (If you add bits in the wrong order, there’s no way to rearrange them. You must delete the incorrect bits and then add them again in the correct order.)
   - If the Start Bit is disabled, then you have used all available bits; if you want to change the function of an existing bit, you must delete the incorrect bits before you can add them elsewhere.
4. Click *Add Field*.

   The bit numbers will be added in the corresponding columns in the structure table, and the bits will be reflected in the Bit Map representation above.
5. To remove an incorrect bit, check the box next to the bit and then click the *Clear Selection* button.
6. To clear (delete) the entire structure, click the *Clear All* button.

Set Up the Parity Bits

1. Add the Parity Bit to the Structure
   a. Under Structure, choose *Parity* from the drop-down box.
   b. Choose the first bit you want to use for the parity bit from the *Start bit* drop-down box.
   c. Choose the number of sequential bits (usually 1) from the *Length* drop-down box.
   d. Click the *Add Field* button.

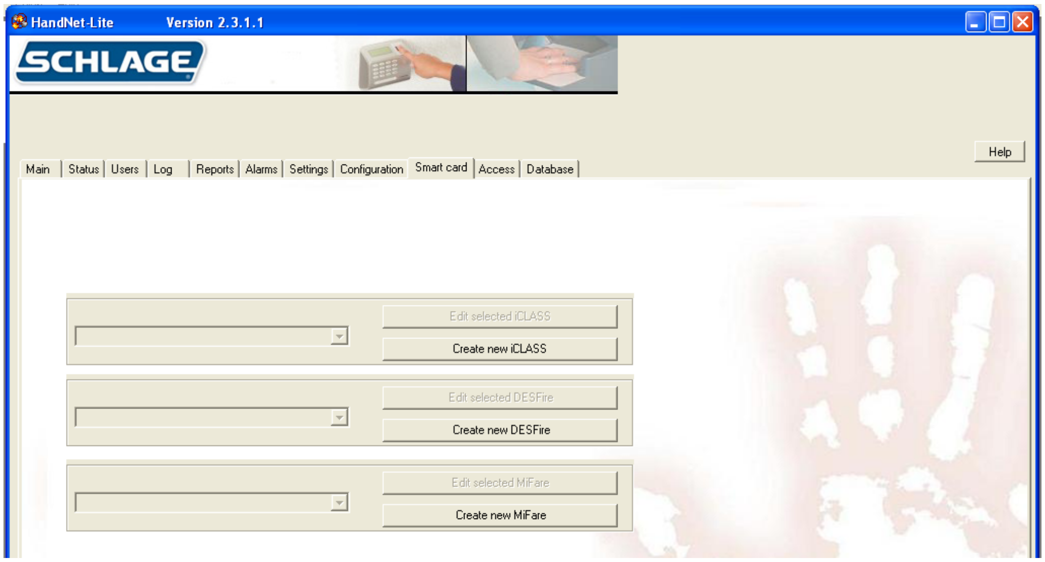
2. Indicate whether that parity bit is even or odd
   a. Under *Parity 1*, choose *Even* or *Odd* from the drop-down box.
   b. Under Start Bit, choose the bit for which you want to identify parity from the drop-down box.
   c. Click *Add Field*.

3. Identify which bits are considered to determine that parity bit
   a. Under *Parity 1*, choose *Included*
   b. Under *Start Bit*, choose the first bit that is used to determine this parity
   c. Under *Length*, indicate the number of bits to consider
   d. Click *Add Field*.
   e. If the bits to consider are broken up (for example, if you want to consider bits 2–10 and bits 14–18), simply repeat this step to add the additional bits.

Smart Card Tab

The Smart Card tab is used only with FingerKeys. It is used to manage FingerKey iCLASS, DESFire and MiFare cards.

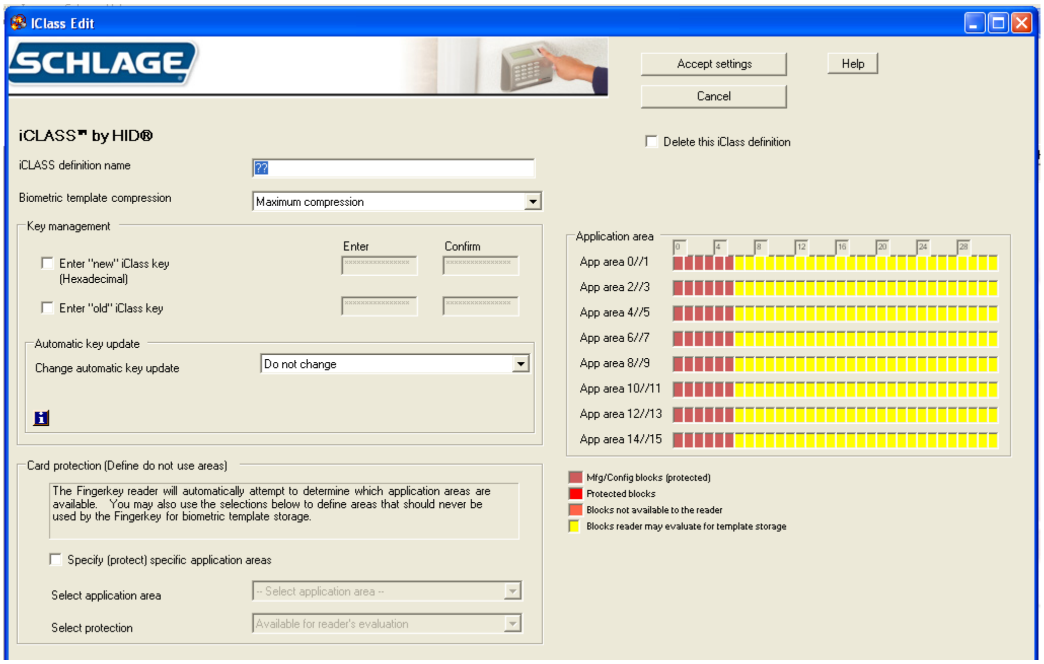
Figure 11-1: Smart Card Tab



Managing FingerKey iCLASS Definitions

iCLASS Definition Screen

Figure 11-2: iCLASS Definition Screen



iCLASS™ by HID®

□ Delete this iClass definition

iCLASS definition name: ??

Biometric template compression: Maximum compression

Key management

	Enter	Confirm
□ Enter "new" iClass key (Hexadecimal)	***************	***************
□ Enter "old" iClass key	***************	***************

Automatic key update

Change automatic key update: Do not change

Card protection (Define do not use areas)

The Fingerkey reader will automatically attempt to determine which application areas are available. You may also use the selections below to define areas that should never be used by the Fingerkey for biometric template storage.

□ Specify (protect) specific application areas

Select application area: -- Select application area --

Select protection: Available for reader's evaluation

Application area

App area 0//1
App area 2//3
App area 4//5
App area 6//7
App area 8//9
App area 10//11
App area 12//13
App area 14//15

🟥 Mfg/Config blocks (protected)
🟥 Protected blocks
🟥 Blocks not available to the reader
🟨 Blocks reader may evaluate for template storage

Add an iCLASS Definition

1. Click the *Smart Card* tab.
2. Click the *Create new iCLASS* button.
3. Complete the fields on the screen. See the iCLASS Definition Fields table on page 50 for more information.
4. Click the Accept settings button.

Edit an iCLASS Definition

1. Click the *Smart Card* tab.
2. Choose the iCLASS definition you want to edit from the drop-down box.
3. Click the *Edit selected iCLASS* button.
4. Complete the fields on the screen. See the iCLASS Definition Fields table on page 50 for more information.
5. Click the *Accept settings* button.

Delete an iCLASS Definition

1. Click the *Smart Card* tab.
2. Choose the iCLASS definition you want to delete from the drop-down box.
3. Click the *Edit selected iCLASS* button.
4. Click the *Delete this iCLASS definition* check box.
5. Click the *Accept settings* button.

iCLASS Definition Fields

Table 11-19: iClass Definition Fields

Field	Req'd?	Description
iCLASS definition name	Yes	• Name of the iCLASS definition • Any name that distinguishes this definition from others
Biometric template compression		• Controls the amount of compression of the finger template before it is written to the iCLASS card • Maximum compression should be used initially • See the iCLASS Card Compression table on page 51 for more information
Enter “new” iClass key		• A password that encrypts the areas used by the readers on iCLASS cards • Protects the fingerprint data from being read if the same cards are used with other devices. • 16 hex digits (0–9 and A–F.) • A default key is used when a new iCLASS definition is defined. Can be used permanently if desired. • For increased security, change this key periodically.
Confirm “new” iClass key		Confirmation of previous field

Field	Req'd?	Description
Enter "old" iClass key		• Old reader key, usually populated automatically. • Required for the reader to change the key. • All cards should be updated each time the key is changed, to ensure they key is always up-to-date. • See Resetting Old Card Keys on page 52 for more information.
Automatic Key Update		• Indicates whether readers using this definition can automatically change the key on a card. • Defaults to Do Not Change. Whatever setting was previously entered will continue to be used. If you're editing a previously created definition, click the ℹ button to see what the current settings are. • Options: • Do Not Change: Use the previously entered setting. • Disable Auto Key Update: Prevents the reader from changing a key. • Start Unlimited Auto Key Update: Any card with the old key will be automatically updated when used at the reader. • Start Limited Auto Key Update: Any card with the old key will be automatically updated at the reader, until the number of cards and/or date specified is reached. • See Automatic Key Update on page 53 for more information.
Specify (protect) application areas		• Only check this box if you are sharing the iCLASS card with another iCLASS device that does not automatically determine the template location on the card. • See iCLASS Card Protection on page 52 for more information.

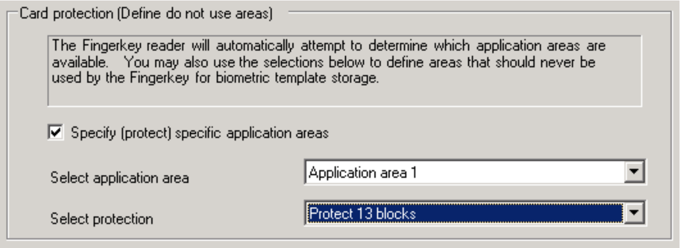
iCLASS Card Compression

Table 11-20: iCLASS Card Compression

	Number of Enrolled Fingers	
	1	2
No Compression	854 bytes	1654 bytes
Minimum Compression	566	1078
Medium Compression	454	854
Maximum Compression	310	566

iCLASS Card Protection

Figure 11-3: iCLASS Card Protection



Card protection (Define do not use areas)

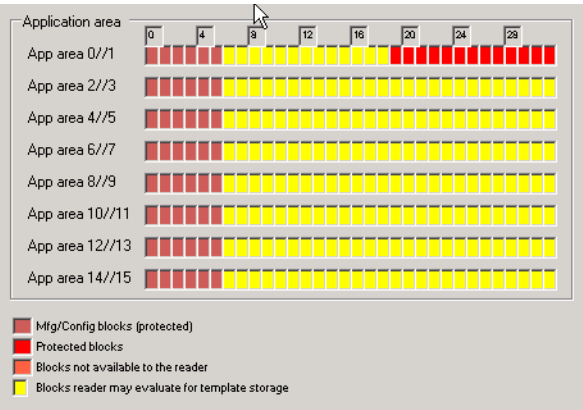
The Fingerkey reader will automatically attempt to determine which application areas are available. You may also use the selections below to define areas that should never be used by the Fingerkey for biometric template storage.

☑ Specify (protect) specific application areas

Select application area: Application area 1

Select protection: Protect 13 blocks

The grid on the right shows the protected blocks in red:



▨ Mfg/Config blocks (protected)
🟥 Protected blocks
▨ Blocks not available to the reader
🟨 Blocks reader may evaluate for template storage

You can protect multiple areas simply by choosing new values for each of these entries. You can clear any protected area by choosing the application area and choosing Available for Reader's Evaluation in the Select Protection drop down menu.

When you protect blocks in even application areas (0, 2, 4, etc.), blocks are used from the left to the right, that is, starting at block 6 and working up; when you protect areas in odd application areas (1, 3, 5, etc.), blocks are used from right to left, that is, starting at 31 and working down.

If you protect both even and odd sections in any pair (for example, if you protect parts of both area 0 area 1), then the fingerprint reader can't use that pair at all so the entire area is marked as protected.

! NOTE *Programmed iCLASS cards require application area 0 to be blocked off. To do this, click Select Application Area and pick Application Area 0 from the drop down menu. Then click Select Protection and choose Protect 26 blocks.*

Resetting Old Card Keys

To change the key for a previously used iCLASS card, the reader must know what the old key is—this prevents unauthorized people from converting other cards to work with your system. HandNet Lite keeps track of what the last key you used was, so most of the time, you don't need to change this entry.

For example, suppose you originally set the key to 1234123412341234 and then you entered a New Reader Key of 5678567856785678. HandNet Lite remembers the old key; it would automatically change cards to the new key if you set it to automatically update keys (see Automatic Key Update on page 53).

However, suppose in January you set the key to 1234123412341234, in February change it to 5678567856785678, and in March change it again to 9ABC9ABC9ABC9ABC. Cards that got used during February would have been updated to 5678567856785678; cards that didn't get used during February would still have January's key of

1234123412341234. The reader can automatically update those cards with the most recent old key (5678567856785678), but it would no longer recognize the prior old key of 1234123412341234. If you have a situation like this, to update the older cards, you must manually indicate what old key to use by checking the Reset Old Key checkbox and then entering the appropriate value in the old key entries.

If you have an older card and know that one of several keys was used on it but aren't sure which one, enter the various old keys in turn here, trying to update the card each time.

You can avoid ever having to do this if you make sure that all cards get updated each time you change your key.

Automatic Key Update

Some administrators want any reader to update the key; other administrators prefer to only let selected readers update cards. For example, for top security, you might only let a non-networked reader in a security office update cards so that was the only place they could be updated. To do this, the administrator would create one iCLASS definition for the public readers (with Automatic Key Update unchecked), and another iClass definition (Automatic Key Update checked) for the administrative reader.

If you disable automatic updates here, you can still manually update keys using the reader command menus.

If you return to this screen, this entry defaults to Do Not Change; this means that whatever setting was previously entered will continue to be used. If you're editing a previously created definition, click the ℹ button to see what the current settings are. (This button doesn't do anything when creating a new definition.)

Your choices are:

Do Not Change: Use the previously entered setting.

Disable Auto Key Update: This prevents the reader from ever changing a key. With this setting, to update cards, you would have to use a reader associated with another iCLASS definition that allowed updates, or you would have to manually update cards with the reader's command menus.

Start Unlimited Auto Key Update: If any card with the old key is used, this automatically updates the card to the new key. There's no limit to the number of cards that can be updated, and no limit on the date range.

Start Limited Auto Key Update: If any card is used that currently has this old key, this automatically updates the card to the new key until the number of cards and/or date specified in the following two entries is reached. For example, if you had 20 employees, you might set this to only automatically update 20 cards; once that was done, cards would not be automatically updated until you changed the key again. You could also specify a date; cards would then be automatically updated until that date, but would not be updated after that date.

Specify (protect) application areas

Only check this box if you are sharing the iCLASS card with another iCLASS device that doesn't automatically determine the template location on the card. If fingerprint readers are the only iCLASS device that you use with your cards, or if you use other device that also automatically choose an available space to store information, then you don't need to change this setting.

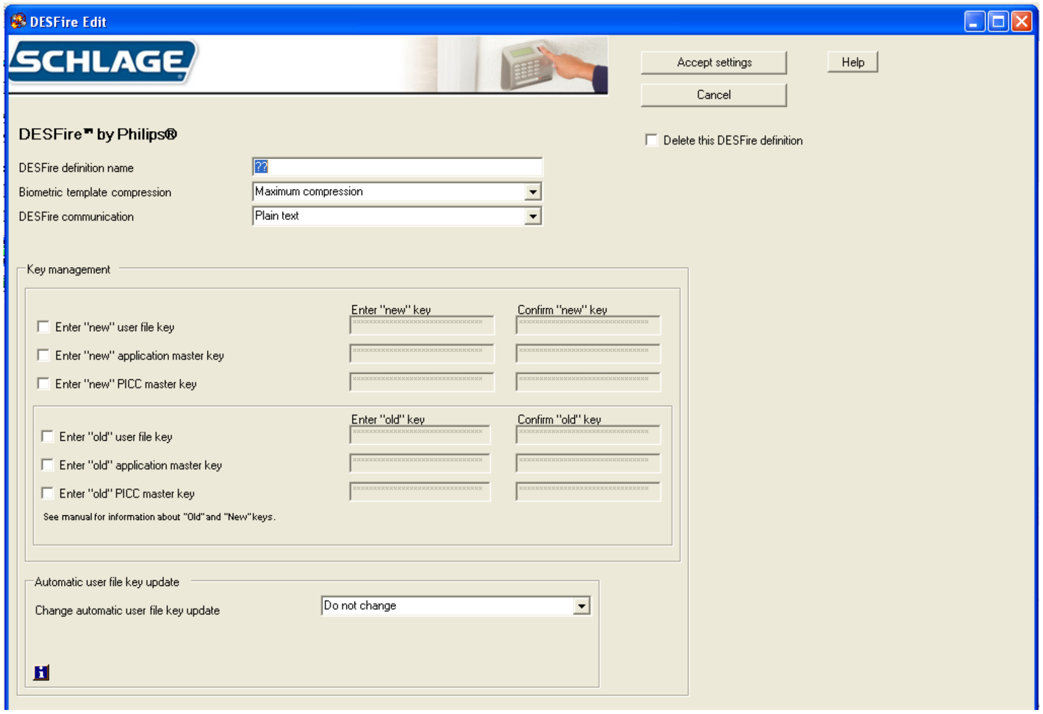
For example, Schlage Biometrics hand readers always store their templates in blocks 19–31 of area 1. If you were using the same iCLASS cards with both Schlage Biometrics hand readers and Schlage Biometrics fingerprint readers, you'd have to protect these blocks so a fingerprint template wouldn't get written in this area; if it did, the hand reader would write a template over it.

To protect these blocks, check the box by Specify (protect) application areas, click Select Application Area and pick Application Area 1 from the drop down menu, and click Select Protection and choose Protect 13 blocks from the menu:

Managing FingerKey DESFire Card Definitions

DESFire Definition Screen

Figure 11-4: DESFire Definition Screen



DESFire™ by Philips®

□ Delete this DESFire definition

DESFire definition name: ??

Biometric template compression: Maximum compression

DESFire communication: Plain text

Key management

	Enter "new" key	Confirm "new" key
□ Enter "new" user file key		
□ Enter "new" application master key		
□ Enter "new" PICC master key		

	Enter "old" key	Confirm "old" key
□ Enter "old" user file key		
□ Enter "old" application master key		
□ Enter "old" PICC master key		

See manual for information about "Old" and "New" keys.

Automatic user file key update

Change automatic user file key update: Do not change

Add a DESFire Definition

1. Click the *Smart Card* tab.
2. Click the *Create new DESFire* button.
3. Complete the fields on the screen. See the DESFire Definition Fields table on page 56 for more information.
4. Click the *Accept settings* button.

Edit a DESFire Definition

1. Click the *Smart Card* tab.
2. Choose the DESFire definition you want to edit from the drop-down box.
3. Click the *Edit selected DESFire* button.
4. Complete the fields on the screen. See the DESFire Definition Fields table on page 56 for more information.
5. Click the *Accept settings* button.

Delete a DESFire Definition

1. Click the *Smart Card* tab.
2. Choose the DESFire definition you want to delete from the drop-down box.
3. Click the *Edit selected DESFire* button.
4. Click the *Delete this DESFire* definition check box.
5. Click the *Accept settings* button.

DESFire Definition Fields

Table 11-21: DESFire Definition Fields

Field	Req'd?	Description
DESFire definition name	Yes	• Name of the DESFire definition • Any name that distinguishes this definition from others
Biometric template compression	Yes	• Controls the amount of compression of the finger template before it is written to the DESFire card • Maximum compression should be used initially • See the DESFire Card Compression table on page 56 for more information
DESFire communication	Yes	Select either *Plain Text* or *DESFire* ciphered
Enter "new" user file key	Yes	• Check the box to edit these fields. • Key entered must be exactly the same in both boxes.
Enter "new" application master key	Yes	• Check the box to edit these fields. • Key entered must be exactly the same in both boxes.
Enter "new" PICC master key	Yes	• Check the box to edit these fields. • Key entered must be exactly the same in both boxes.
Enter "old" user file key	Yes	• Check the box to edit these fields. • Key entered must be exactly the same in both boxes.
Enter "old" application master key	Yes	• Check the box to edit these fields. • Key entered must be exactly the same in both boxes.
Enter "old" PICC master key	Yes	• Check the box to edit these fields. • Key entered must be exactly the same in both boxes.
Change automatic user file key update	Yes	The automatic user key update choices are: • Do not change • Disable auto key update • Start unlimited auto key update • Start limited auto key update (displays two additional fields) • With limited auto key update the operator can select the number of cards to be updated and/or the number of cards to automatically update.

DESFire Card Compression

Table 11-22: DESFire Card Compression

	Number of Enrolled Fingers	
	1	2
No Compression	854 bytes	1654 bytes
Minimum Compression	566	1078
Medium Compression	454	854
Maximum Compression	310	566

Managing FingerKey Mifare Standard Card Formats

Add a Mifare Standard Definition

1. Click the *Smart Card* tab.
2. Click the *Create new Mifare* button.
3. Complete the fields on the screen. See the Mifare Standard Definition Fields table on page 58, and the Mifare Standard Sector Fields on page 59 for more information.
4. Click the *Accept settings* button.

Edit a Mifare Standard Definition

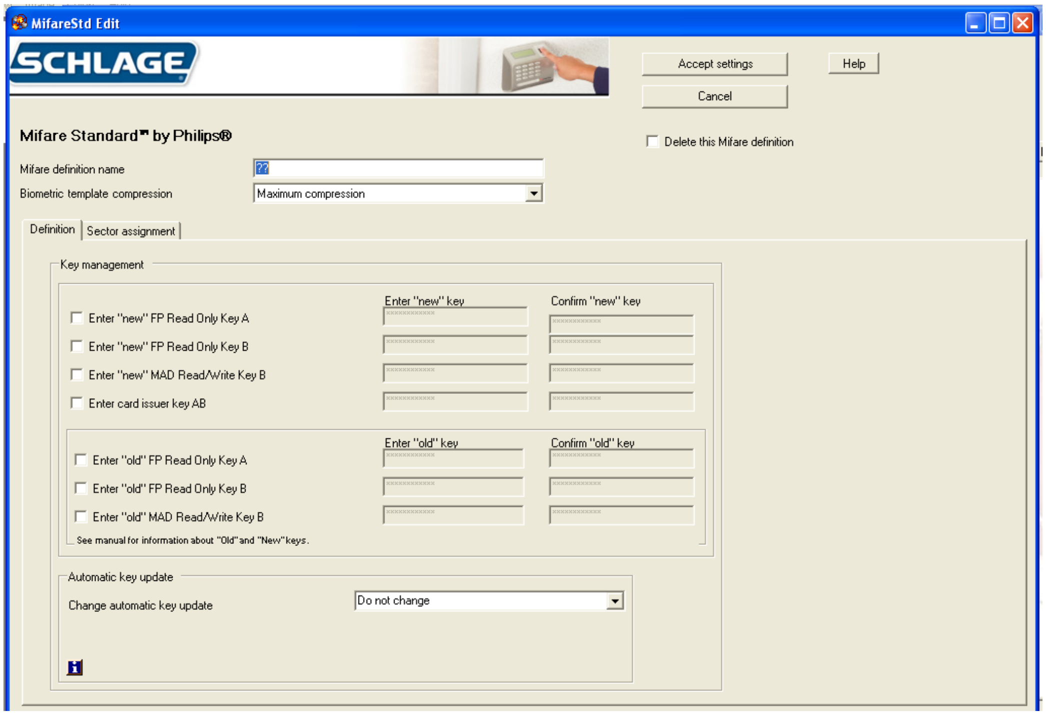
1. Click the *Smart Card* tab.
2. Choose the Mifare definition you want to edit from the drop-down box.
3. Click the *Edit selected Mifare* button.
4. Complete the fields on the screen. See the Mifare Standard Definition Fields table on page 58, and the Mifare Standard Sector Fields on page 59 for more information.
5. Click the *Accept settings* button.

Delete a Mifare Standard Definition

1. Click the *Smart Card* tab.
2. Choose the Mifare definition you want to delete from the drop-down box.
3. Click the *Edit selected Mifare* button.
4. Click the *Delete this Mifare* definition check box.
5. Click the *Accept settings* button.

Mifare Standard Definition Screen

Figure 11-5: Mifare Standard Definition Screen



Mifare Standard™ by Philips®

□ Delete this Mifare definition

Mifare definition name: ??

Biometric template compression: Maximum compression

	Enter "new" key	Confirm "new" key
□ Enter "new" FP Read Only Key A	xxxxxxxxxxxx	xxxxxxxxxxxx
□ Enter "new" FP Read Only Key B	xxxxxxxxxxxx	xxxxxxxxxxxx
□ Enter "new" MAD Read/Write Key B	xxxxxxxxxxxx	xxxxxxxxxxxx
□ Enter card issuer key AB	xxxxxxxxxxxx	xxxxxxxxxxxx

	Enter "old" key	Confirm "old" key
□ Enter "old" FP Read Only Key A	xxxxxxxxxxxx	xxxxxxxxxxxx
□ Enter "old" FP Read Only Key B	xxxxxxxxxxxx	xxxxxxxxxxxx
□ Enter "old" MAD Read/Write Key B	xxxxxxxxxxxx	xxxxxxxxxxxx

See manual for information about "Old" and "New" keys.

Change automatic key update: Do not change

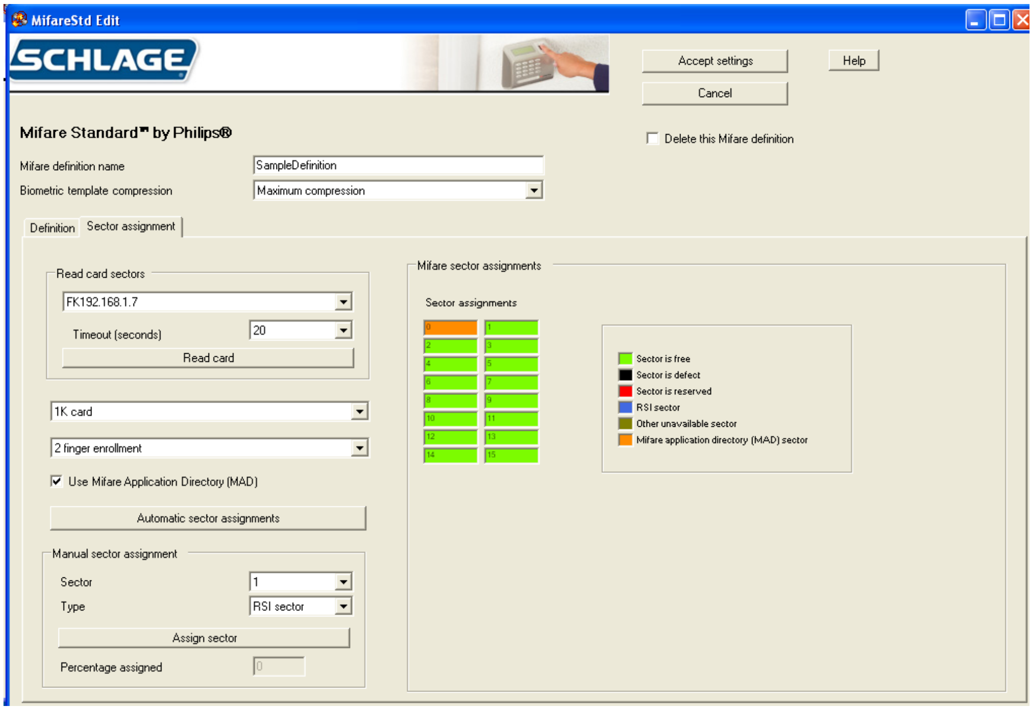
Mifare Standard Definition Fields

Table 11-23: Mifare Standard Definition Fields

Field	Req'd?	Description
Mifare definition name	Yes	• Name of the Mifare definition • Any name that distinguishes this definition from others
Biometric template compression	Yes	• Controls the amount of compression of the finger template before it is written to the Mifare card • Maximum compression should be used initially • See the Mifare Card Compression table on page 60 for more information
Enter “new” FP Read Only Key A	Yes	• Check the box to edit these fields • Key entered must be the same in both boxes
Enter “new” FP Read Only Key B	Yes	• Check the box to edit these fields • Key entered must be the same in both boxes
Enter “new” MAD Read/Write Key B	Yes	• Check the box to edit these fields • Key entered must be the same in both boxes
Enter card issuer key AB	Yes	• Check the box to edit these fields • Key entered must be the same in both boxes
Enter “old” FP Read Only Key A	Yes	• Check the box to edit these fields • Key entered must be the same in both boxes
Enter “old” FP Read Only Key B	Yes	• Check the box to edit these fields • Key entered must be the same in both boxes
Enter “old” MAD Read/Write Key B	Yes	• Check the box to edit these fields • Key entered must be the same in both boxes

Field	Req'd?	Description
Change automatic key update	Yes	The automatic key update choices are: • Diable auto key update • Start unlimited auto key update • Start limited auto key update (displays two additional fields) • With limited auto key update, the operator can select the number of cards to be updated and/or the number of cards to automatically update.

Figure 11-6: Mifare Standard Sector Assignment Screen



Mifare Standard™ by Philips®

☐ Delete this Mifare definition

Mifare definition name: SampleDefinition

Biometric template compression: Maximum compression

Read card sectors: FK192.168.1.7

Timeout (seconds): 20

1K card

2 finger enrollment

☑ Use Mifare Application Directory (MAD)

Manual sector assignment

Sector: 1

Type: RSI sector

Percentage assigned: 0

Mifare sector assignments

Sector assignments

🟧 0	🟩 1
🟩 2	🟩 3
🟩 4	🟩 5
🟩 6	🟩 7
🟩 8	🟩 9
🟩 10	🟩 11
🟩 12	🟩 13
🟩 14	🟩 15

- 🟩 Sector is free
- ⬛ Sector is defect
- 🟥 Sector is reserved
- 🟦 RSI sector
- 🟫 Other unavailable sector
- 🟧 Mifare application directory (MAD) sector

Mifare Standard Sector Fields

Table 11-24: Mifare Standard Sector Fields

Field	Req'd?	Description
Read card sectors		• Select the desired FingerKey to use in reading an existing Mifare Standard card • Select a card read timeout in seconds • Click the *Read card* button and present the Mifare Standard card to the reader • The card characteristics will be displayed • Use either Automatic Sector Assignment or Manual Sector Assignment to determine where the FingerKey will place the biometric template.
1K Card or 4K Card	Yes	• Allows you to tell HandNet Lite if the Mifare Standard cards you will be using have 1K or 4K capacity. • If you have used the *Read card* button described above, this will be filled in automatically.

Field	Req'd?	Description
Two finger enrollment or One finger enrollment	Yes	• Allows for storage of either one or two fingerprint biometric templates on the card.
Use Mifare Application Directory (MAD)	Yes	• Allows for use of a MAD (Mifare Application Directory) on the card. A MAD is stored in sector 0 (and 16 if a 4K card) and tells devices how the sectors on the card are allocated. • If unchecked, then you can assign any card sectors to fingerprint template storage.
Automatic sector assignments		• If *Use Mifare Application Directory* is checked, then clicking this button will instruct HandNet Lite to automatically assign the sectors on the card to be used for biometric template assignment (Schlage Biometrics Sector).
Manual Sector Assignment		• Allows you to manually assign the sectors for either biometric template assignment (Schlage Biometrics sector) or a free/available sector. You will need to assign sectors as Schlage Biometrics sectors until the percentage assigned is 100%.

As you use either Automatic or Manual sector assignment the display in the Mifare sector assignments group will change showing you the current assignment.

If your installation is currently using Mifare Standard cards with another device and you wish to add FingerKey biometrics to your existing cards you will wish to:

a. Determine if your current cards are formatted to use a Mifare Application Directory. Contact your existing device manufacturer. You can attempt to use the "Read card sectors" button in HandNet lite to attempt to read an existing MAD on the card.

b. If your current cards are not formatted to use a MAD, then you will need to determine which sectors your current device manufacturer uses on your card. It is normal that sector 0 will be used, but your current cards may also contain data in additional sectors. Check with your existing device manufacturer to determine which sectors on your cards are available and begin the Schlage Biometrics sector assignment at the first free sector.

Once you are satisfied with the card definition, click the "Accept settings" button to record the definition. You will then need to go back to the "Configuration" tab, and for each FingerKey to use this Mifare Standard definition you will need to "Edit selected reader", click "Fingerprint settings" and use the drop down for "Mifare standard configuration" and select the saved Mifare Standard Definition.

It is important that each FingerKey be assigned the correct Mifare standard configuration setting.

Mifare Card Compression

Table 11-25: Mifare Card Compression

	Number of Enrolled Fingers	
	1	2
No Compression	854 bytes	1654 bytes
Minimum Compression	566	1078
Medium Compression	454	854
Maximum Compression	310	566

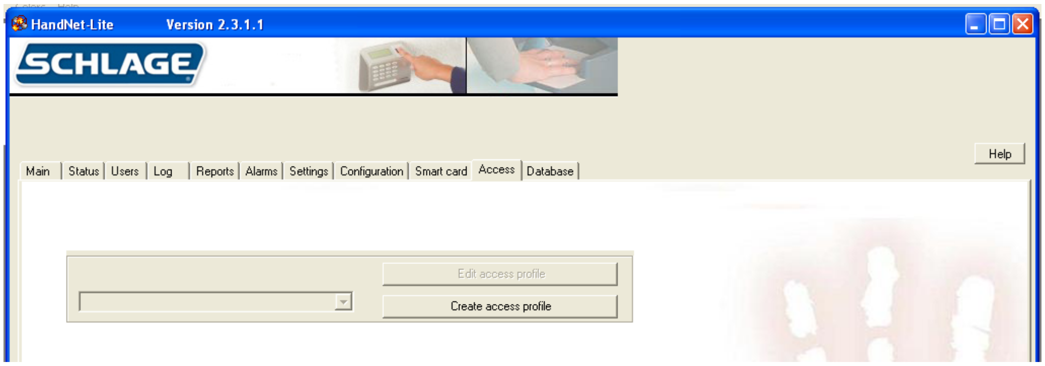
Access Tab

The Access Tab is used to add or edit access profiles. Access profiles define which type of user can use each reader.

For example, suppose your maintenance staff should have access to the maintenance rooms, your office staff should have access to the office, and your supervisors should have access to everything. You would create three access profiles: one for supervisors, one for office staff, and one for maintenance personnel. These profiles would identify which readers each group could use. After creating these profiles, whenever you added a user, you would identify which group the user was a part of, and the access profile for that group would automatically give the appropriate access.

If you want all users to be able to use every reader, you don't need to set up access profiles. HandNet Lite comes set up with an Always profile that lets users use any reader in the system. (It also has a Never profile that doesn't let the user verify at any reader.) You can't change or delete the Always or Never profile.

Figure 12-1: Access Tab



Add an Access Profile

1. Click the *Access* tab.
2. Click the *Create access profile* button.
3. Enter the access profile name.
4. Check the boxes next to the readers you want users with this access profile to be able to access.
5. Click the *Accept settings* button.

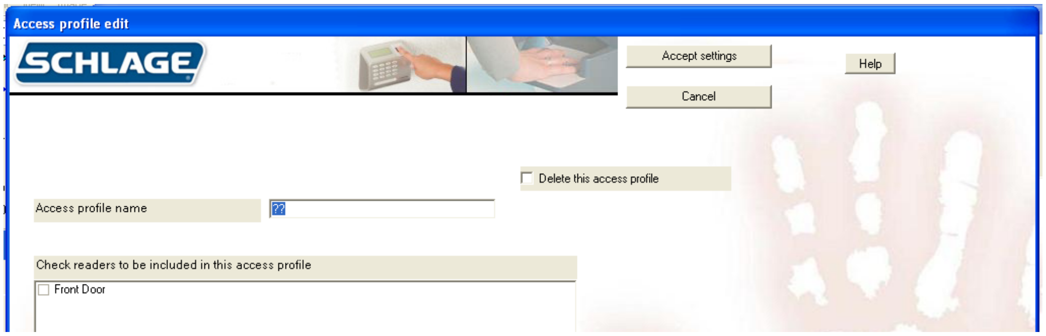
Edit an Access Profile

1. Click the *Access* tab.
2. Select the name of the access profile you want to edit from the drop-down box.
3. Click the *Edit access profile* button.
4. Edit the access profile name, if necessary.
5. Check the boxes next to the readers you want users with this access profile to be able to access.
6. Click the *Accept settings* button.

Delete an Access Profile

1. Click the *Access* tab.
2. Select the name of the access profile you want to delete from the drop-down box.
3. Check the box next to *Delete this access profile*.
4. Click the *Accept settings* button.

Figure 12-2: Access Profile Edit Screen



□ Delete this access profile

Access profile name: ??

Check readers to be included in this access profile

□ Front Door

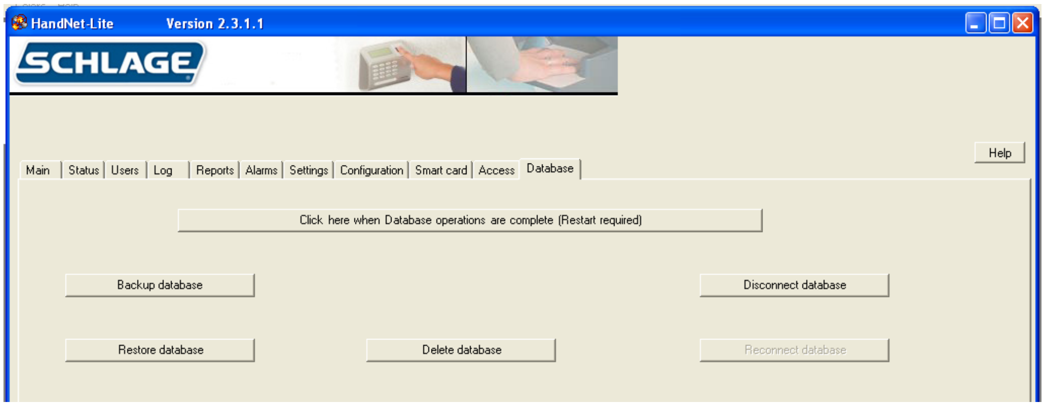
Table 12-26: Access Profile Fields

Field	Req'd?	Description
Access profile name	Yes	• Name of the access profile • Use a name that describes the group of users for which this access profile will be used. • Any combination of letters, numbers, spaces, and special characters up to 30 characters
Check readers to be included in this access profile	No	• Lists all the readers in the system • Check the box next to each reader you want users with this profile to be able to access. • Uncheck the box next to each reader you do not want users with this access profile to be able to access.
Delete this access profile	No	• Check to delete this access profile and remove it from the access profile list. • Access profiles that are assigned to users cannot be deleted. To remove an access profile from a user, see Edit a User on page 12. • If you delete the profile that is the default profile for reader enrollments, the next profile in the list will be selected. To choose a different default profile, go to the Settings window and choose the correct profile; see Settings Fields on page 25 for more information..

Database Tab

The Database Tab is used to backup, restore, delete, detach and attach the database.

Figure 13-1: Database Tab



Back Up the Database

The Backup database button is used to create a backup of the HandNet-lite database. The location of the backup will be displayed at the bottom of the screen:

1. Click the *Database* tab.
2. Click the *Backup database* button.
3. If you have completed all database operations you want to perform at this time, click the *Click here when Database operations are complete* button. See Finish Database Operations and Restart on page 64 for more information.

Restore the Database

The Restore database button is used to restore a backup file of the database.

1. Click the *Database* tab.
2. Click the *Restore database* button.
3. Select the backup file you want to use from the pop-up window and click the *Open* button.
4. If you have completed all database operations you want to perform at this time, click the *Click here when Database operations are complete* button. See Finish Database Operations and Restart on page 64 for more information..

Delete the Database

The Delete database button is used to delete the working copy of the database.

1. Click the *Database* tab.
2. Click the *Delete database* button.
3. Click the *Yes* button on the pop-up window.

   If you delete the database, you will lose all configuration and user information in the system. A new, empty database will replace the current database.

4. If you have completed all database operations you want to perform at this time, click the *Click here when Database operations are complete* button. See Finish Database Operations and Restart on page 64 for more information..

Disconnect the Database

The Disconnect database button is used to disconnect the database from the MS SQL Server Express database engine.

1. Click the *Database* tab.
2. Click the *Disconnect database* button.
3. If you have completed all database operations you want to perform at this time, click the *Click here when Database operations are complete* button. See Finish Database Operations and Restart on page 64 for more information..

Reconnect the Database

The Connect database button is used to reconnect the database to the MS SQL Server Express database engine.

1. Click the *Database* tab.
2. Click the *Reconnect database* button.
3. If you have completed all database operations you want to perform at this time, click the *Click here when Database operations are complete* button. See Finish Database Operations and Restart on page 64 for more information..

Finish Database Operations and Restart

Once you have completed all database operations you want to perform at this time, click the Click here when Database operations are complete button. This will cause HandNet-lite to exit. When you restart HandNet-lite it will take the following actions:

1. If a database is currently attached, HandNet Lite will use that database.
2. If a database is not currently attached, but database files exist, HandNet Lite will reattach the database files and continue.
3. If a database is not currently attached, and there is no database file, HandNet Lite will create a new database.

Appendix A

Table A-27: Card Formats

Type	Format	Description	Format detail
Wiegand formats	1	WC01 26 bit: 16 bit ID	Facility code: 8 bits, bit 2-9 ID: 16 bits, bit 10-25 1 2 12345678901234567890123456 PFFFFFFFFIIIIIIIIIIIIIIIIP EXXXXXXXXXXXX............. .............XXXXXXXXXXXXO
	2	WC02 32 bit: 22 bit ID	Facility code: 8 bits, bit 2-9 ID: 22 bits, bit 10-31 1 2 3 12345678901234567890123456789012 PFFFFFFFFIIIIIIIIIIIIIIIIIIIIIIP EXXXXXXXXXXXXXXX................ ................XXXXXXXXXXXXXXXO
	3	WC03 34 bit: 16 bit ID	Facility code: 16 bits, bit 2-17 ID: 16 bits, bit 18-33 1 2 3 1234567890123456789012345678901234 PFFFFFFFFFFFFFFFFIIIIIIIIIIIIIIIIP EXXXXXXXXXXXXXXXX................. .................XXXXXXXXXXXXXXXXA
	4	WC04 34 bit: 20 bit ID	Facility code: 12 bits, bit 2-13 ID: 20 bits, bit 14-33 1 2 3 1234567890123456789012345678901234 PFFFFFFFFFFFFIIIIIIIIIIIIIIIIIIIIP EXXXXXXXXXXXXXXXX................. .................XXXXXXXXXXXXXXXXO
	5	WC05 34 bit: 32 bit ID	ID: 32 bits, bit 2-33 1 2 3 1234567890123456789012345678901234 PIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIP EXXXXXXXXXXXXXXXX................. .................XXXXXXXXXXXXXXXXO
	6	WC06 35 bit: 20 bit ID	Facility code: 12 bits, bit 3-14 ID: 20 bits, bit 15-34 1 2 3 12345678901234567890123456789012345 PPFFFFFFFFFFFFIIIIIIIIIIIIIIIIIIIIP .EXX.XX.XX.XX.XX.XX.XX.XX.XX.XX.XX. .XX.XX.XX.XX.XX.XX.XX.XX.XX.XX.XX.O OXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
	7	WC07 37 bit: 19 bit ID	Facility code: 16 bits, bit 2-17 ID: 19 bits, bit 18-36 1 2 3 1234567890123456789012345678901234567 PFFFFFFFFFFFFFFFFIIIIIIIIIIIIIIIIIIIP EXXXXXXXXXXXXXXXXXX.................. ..................XXXXXXXXXXXXXXXXXXO
	8	WC08 37 bit: 35 bit ID	ID: 35 bits, bit 2-36 1 2 3 1234567890123456789012345678901234567 PIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIP EXXXXXXXXXXXXXXXXXX.................. ..................XXXXXXXXXXXXXXXXXXO

Type	Format	Description	Format detail
MagStripe formats	9	MS09 MAG1	ABA Track 2 Input ID len 25 Output min len 1 Output max len 25 Do trim leading zeroes Oriented right, no offset
	10	MS10 MAG2	ABA Track 2 Input ID len 25 Output min len 1 Output max len 25 Do trim leading zeroes Oriented left, no offset
	11	MS11 MAG3 Octal 7	ABA Track 2 Input ID len 7 Output min len 1 Output max len 25 Do trim leading zeroes Oriented right, no offset MS11 MAG3 Octal 7 is the format used for FingerKeys with a ProxIF reader.
	12	MS12 MAG 6 AT 5	ABA Track 2 Input ID len 6 Output min len 1 Output max len 25 Do trim leading zeroes Oriented left, offset 5

While these are the most common formats, you can define any additional formats that you need; see Managing Card Formats starting on page 45 for more information.

Custom Splash Screen

1. Shut down HandNet Lite
2. Create a bitmap (.bmp) image that is 100 x 100 pixels.
3. Save the image to the program directory: C:\Program Files\Schlage\HandNet_Lite\Splash100x100.bmp. This path may vary depending on your individual installation.
4. Restart HandNet Lite. The image should appear on the splash screen.

Index

Ingersoll Rand
Security Technologies

Ingersoll Rand's Security Technologies Sector is a leading global provider of products and services that make environments safe, secure, and productive. The Sector's market-leading products include electronic and biometric access control systems; time and attendance and personnel scheduling systems; mechanical locks and portable security, door closures and exit devices, steel doors and frames, architectural hardware and technologies and services for global security markets.

408.341.4110

www.schlage.com www.ingersollrand.com

Schlage
Biometric Solutions
Ingersoll Rand Security Technologies
1520 Dell Avenue
Campbell, CA 95008
Office: 866-861-2480/512-712-1413 (international)
Fax: 866-303-1794/408-341-4111
E-mail: sbssupport@irco.com

SCHLAGE®

HP-1000

Terminal User's Guide

Ingersoll Rand
Security Technologies

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and, if not installed and used in accordance with the Installation Manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at the user's own expense.

This Class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numerique de la classe A respecte toutes les exigences du Reglemente sure le materiel brouilleur du Canada.

Document Part Number: 70100-6009 – Revision 3.3 – July, 2011

Schlage Biometrics, Inc. reserves the right to change, without notice, product offerings or specifications.

Table of Contents

Introduction

The HandPunch 1000 is a member of the Schlage Biometrics' line of biometric hand geometry Time and Attendance Terminals[1]. The HandPunch records and stores the three-dimensional shape of the human hand for comparison and identity verification. Upon verification, the HandPunch records the time, date, user ID number, and collected time and attendance data for collection by a host computer. The HandPunch can communicate with a host computer.

The HandPunch provides proof-positive employee identification combined with the sophisticated operating features one expects in a modern Time and Attendance Terminal. Because of this unique combination of capabilities, the HandPunch provides the most accurate Time and Attendance data collection terminal available. The key features of the HandPunch include:

- Transaction Buffer
    - 5,120 event capacity
- Programmable Clock and Date Formats and Daylight Savings Switch-over

Biometrics

Biometrics is a term describing the automatic measurement and comparison of human characteristics. While its origins are ancient, the evolution of advanced scanning and microprocessor technology brought biometrics into everyday life. Electronic hand geometry technology first appeared in the 1970s. Schlage Biometrics Inc., founded in 1986, built the first mass-produced hand geometry readers and made biometric technology affordable for the commercial market. Today, Schlage Biometrics' products are in use in every imaginable application from protecting cash vaults to verifying employee attendance in hospitals.

[1] For the sake of using a consistent name throughout the manual, the HandPunch 1000 terminal is referred to as the HandPunch for the remainder of this manual.

Principle of Operation

The HandPunch uses low-level infrared light, optics, and a CMOS (IC chip) camera to capture a three-dimensional image of the hand. Using advanced microprocessor technology, the HandPunch converts the image to an electronic template. It stores the template in a database with the user's ID number.

To gain punch, the user enters his or her ID number at the HandPunch's keypad or uses an external card reader. The HandPunch prompts the user to place his or her hand on the HandPunch's platen[2]. The HandPunch compares the hand on the platen with the user's unique template. If the images match, the HandPunch records the transaction for processing.

The HandPunch Terminal

The HandPunch is a time and attendance terminal designed for use with time and attendance software. Refer to Figure 1-1 on page 5 when reviewing the information in this section.

The HandPunch has an integrated keypad for ID entry (see "Figure 1-1"). The CLEAR and ENTER keys are used for data entry and programming.

Four different features assist the user with hand placement and read verification.

1. A light emitting diode (LED) hand placement display on the HandPunch's top panel assists users with hand placement on the platen.
2. A liquid crystal display (LCD) shows operational data and programming menus.
3. "Red light/Green light" verification LEDs quickly inform users if their verification attempts were rejected or accepted.
4. An internal beeper provides audible feedback during keypad data entry and user verification.

[2] The Platen is the flat surface at the base of the HandPunch (see Figure 1-1). This is where users place their hands for enrollment and verification. It has guide pins to assist positioning the fingers during use.

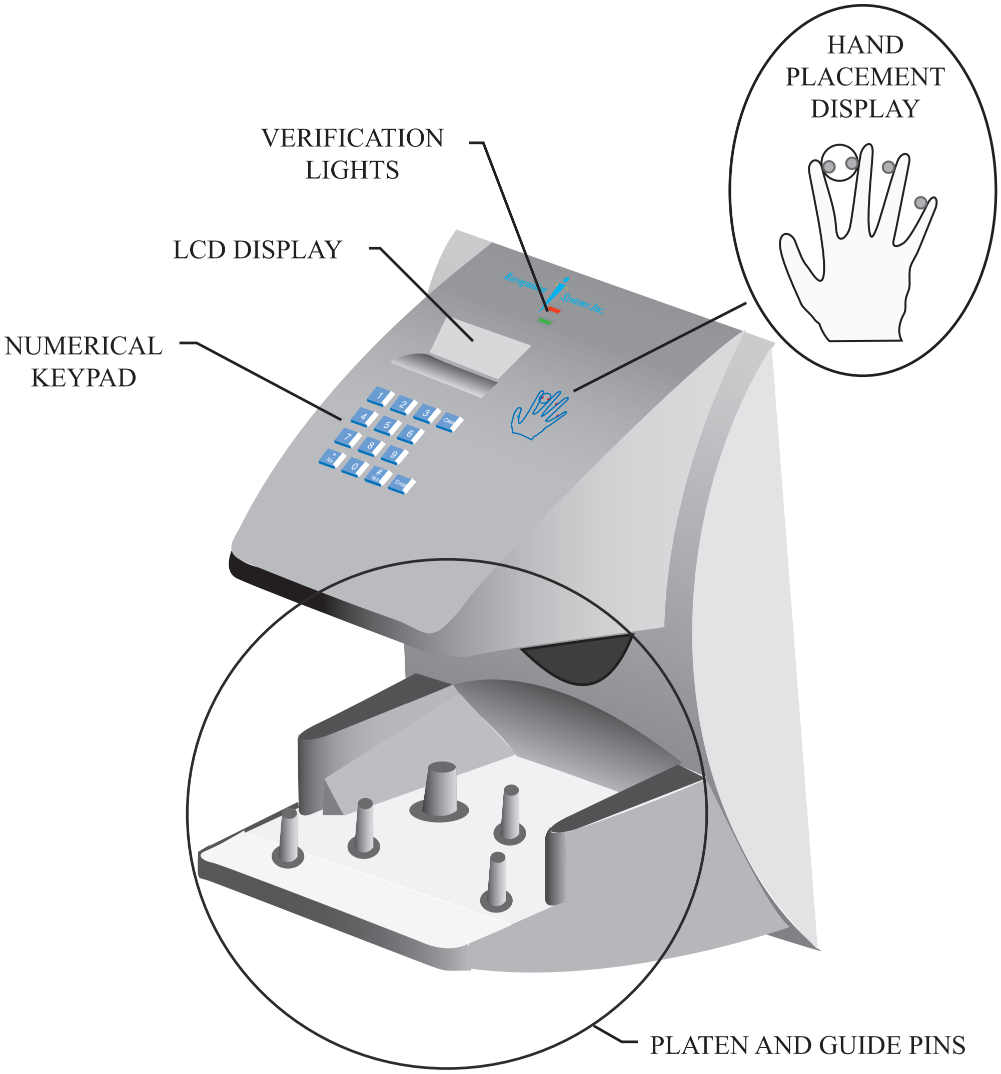


Figure 1-1: The HandPunch 1000

Specifications

Table 1: Specifications

Size:	8.85 inches wide by 11.65 inches high by 8.55 inches deep 22.3 cm wide by 29.6 cm high by 21.7 cm deep
Power:	12 to 24 VDC or 12 to 24 VAC 50-60 Hz, 7 watts
Weight:	6 lbs (2.7 kg) – 7 lbs (3.2 kg) with optional backup battery
Temperature:	-10°C to +60°C – non-operating/storage (14°F to 140°F) 5°C to 40°C – operating (40°F to 110°F)
Relative Humidity Non-Condensing:	5% to 95% – non-operating/storage (non-condensing) 20% to 80% – operating
Verification Time:	1 second or less
Memory Retention:	5 years using a standard internal lithium battery
Transaction Buffer:	5,120 transactions
ID Number Length:	1 to 10 digits
Baud Rate:	300 to 28.8 K bps
Communications:	RS-232, optional Modem
User Capacity:	HP-1000 50 - 512 users HP-1000-E 100 users only

Options

The HandPunch has the following options available.

• Backup Battery Support	See Technical Note 70200-0012 rev C
• Modem Communication	See Technical Note 70200-0013 rev C

UL Compliance

Hand Readers are UL Listed as stand alone units only (i.e. the card reader function has not been evaluated by UL).

The HandKey II has not been tested for UL 294 in an Outdoor configuration.

CE
approved

recyclable

Planning an Installation

Site Preparation

Before you begin installation, check the site blueprints, riser diagrams, and specifications for important information about HandPunch location and for other systems that connect to the HandPunch. Look for any existing wall preparations and wiring that other contractors may have installed for the HandPunch. A wire routing layout diagram (see Figure 3-2 on page 14) is provided to assist in planning wire routing.

HandPunch Placement

The recommended height for the HandPunch platen is 40 inches (102 cm) from the finished floor. The HandPunch should be out of the path of pedestrian and vehicular traffic, and convenient to the door it is controlling. Avoid placing the HandPunch where users must cross the swing path of the door. The HandPunch should be in an area where it is not exposed to excessive airborne dust, direct sunlight, water, or chemicals.

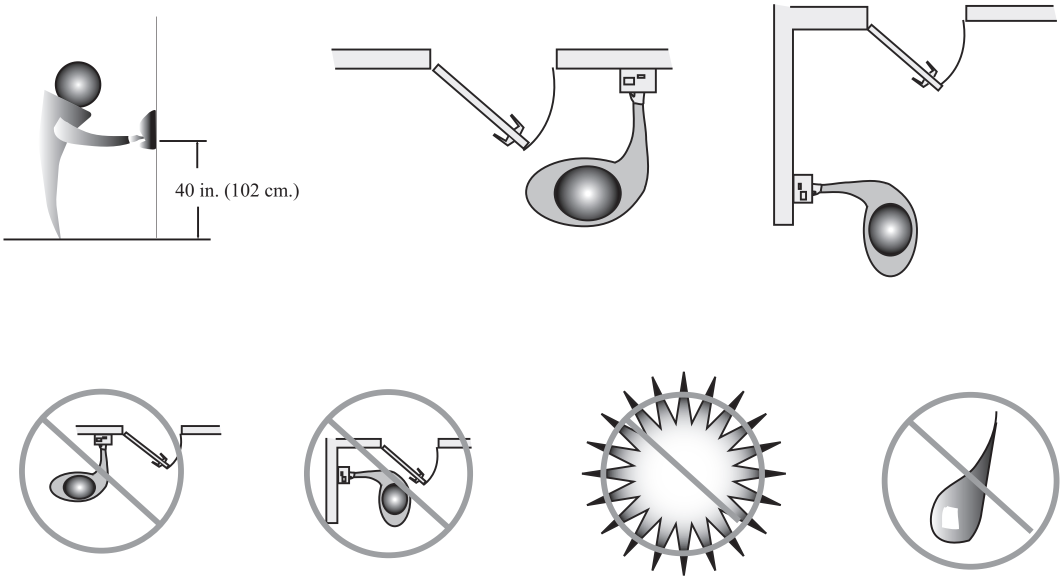


Figure 2-1: HandPunch Placement Rules

NOTE *For the following sections, Schlage Biometrics does not supply hardware items such as power or communications wiring.*

Wiring

Two basic circuits typically connect to the HandPunch:

- Power Input
- HandPunch to Host Computer
  - RS-232
  - modem

The minimum wire size for these circuits is AWG 22; the maximum is AWG 18.

Power Input

The HandPunch uses an internal switching regulator to obtain internal operational power. It accepts input voltages from 12 to 24 VDC or 12 to 24 VAC at 50 to 60 Hz. The HandPunch comes with a 120 VAC to 13.5 VDC power supply (Class 2, Model No. P48131000A010G – 120 VAC, 60 Hz, 21 W, 13.5 VDC output @ 1000mA). An optional 220 VAC to 13.5 VDC power supply is also available.

To power the HandPunch with this power supply, a 120 VAC (or 220 VAC as applicable) duplex outlet must be within 5 feet of the HandPunch. The power supply has a 6-foot cable to provide a comfortable reach between power outlet and HandPunch. The barrel jack at the end of the power supply's cable is connected to J12 on the HandPunch PCB.

! NOTE *Do not connect a HandPunch's power supply to a switched duplex outlet. The HandPunch must have a constant source of power for proper operation.*

Battery Backup Operation

An optional power-fail protection circuit board can be attached to the main circuit board to provide and control battery backup. The battery backup option uses a 12 volt 800 ma/ hour sealed lead acid battery to provide backup battery power. This battery is located immediately inside the rear panel of the HandPunch and plugs into jack J4 on the keypad control circuit board located in the top of the chassis.

The design of the HandPunch's internal power supply is such that any range of the above input voltages may be used and still provide proper battery charge voltage and battery backup operation. Switch-over to battery power is automatic and occurs when the input voltage falls to approximately 10.5 volts. At that time the backup battery charger is disabled to save power, and uninterrupted operation continues on battery power.

When input power is restored, the HandPunch switches off of battery operation and the battery charger is re-enabled to recharge the battery. Battery charge voltage is set at approximately 13.65 volts, and battery charge current is limited to approximately 50 mA. A fully discharged battery requires approximately 12 hours of charge to fully recover.

Additional options installed and specific configurations within the HandPunch make it difficult to predict precisely how long battery support will last, but in general two hours of battery operation can be expected. While operating on battery backup due to loss of main input power, the battery output voltage is constantly monitored by internal circuitry. If the battery voltage reaches approximately 9.5 volts the HandPunch automatically shuts down. This is done to prevent full exhaustion of the battery. A yellow indicator on the top panel illuminates to indicate that the HandPunch is running on battery power. This indicator turns off when main input power is restored.

Shunt J7, which is located immediately in front of the DIP switches on the main logic board (see Figure 4-1 on page 16), enables or disables battery operation on those HandPunches equipped with optional battery backup. If a HandPunch does not have the optional battery backup package installed, J7 is not used. On HandPunches equipped with the battery backup option, J7 allows service personnel a mechanism for disabling battery backup operation before removal of main input power.

To fully power down a HandPunch equipped with battery backup, remove or reposition shunt J7 so that the two pins protruding up from the main logic board are not connected to each other. This effectively opens the circuit, removing the battery from any internal circuitry. Main input power can then be removed and the HandPunch will fully shut down. Once the HandPunch has fully shut down, shunt J7 may be reinstalled.

The design of the power supply is such that main input power must be reapplied to re-enable the battery protection mechanism. If shunt J7 is not properly installed, the internal backup battery will not be charged, and in the event of a main input power loss, the HandPunch will shut down.

HandPunch to Host Computer Connection

HandPunch/host computer communications can be configured in one of two ways:

- via a direct RS-232 connection
- via an optional Modem connection

RS-232 Host Computer Connection

A direct HandPunch connection to a host computer can be made through an 4- conductor cable in an RS-232 serial configuration. A 6’ or 50’ cable may be purchased through RSI or a wiring diagram for the RS-232 to host computer connection is found on Table 2 on page 17.

Modem Host Computer Connection

The HandPunch is also available with an optional modem module for telephone line communications between the HandPunch network and the host computer. When connecting via modem, one HandPunch terminal must be configured with the modem option. This terminal will communicate with the host computer.

To make the modem connection, a telephone jack must be installed on or in the wall behind the modem HandPunch terminal. Position the RJ-11 jack location using the template provided in this manual (see Figure 3-2 on page 14). The short black cable provided with the modem HandPunch connects the terminal to the telephone jack. Figure 4-4 on page 18 a wiring diagram for a modem to host computer connection.

Mechanical Installation

Select an installation location based on the guidelines provided in the Planning an Installation section beginning on page 8.

Wall Plate Installation

Wall Preparation

NOTE *For the following procedure protect the HandPunch from the dust and debris generated during the wall plate installation process.*

1. Remove the wall plate from the packing carton. Refer to Figure 3-1 for all wall plate references in the following section.

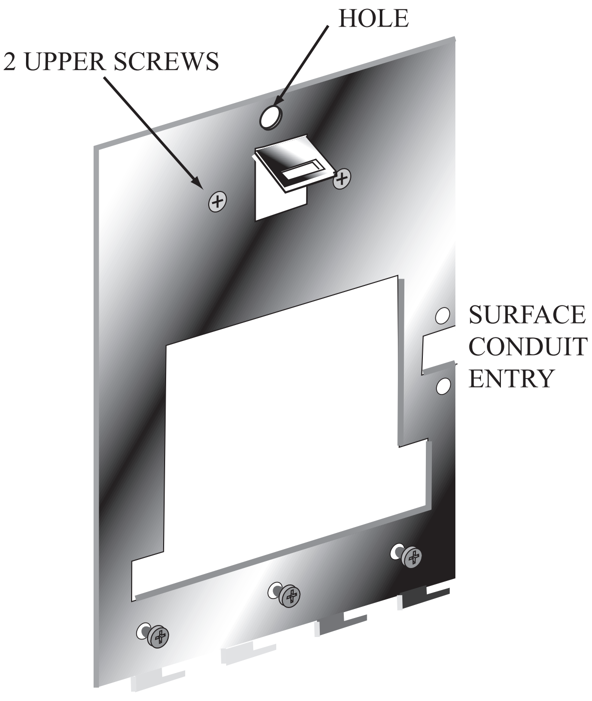


Figure 3-1: Wall Plate

2. Measure and mark a point 48 1/2 inches (123 cm) from the surface of the finished floor. This point will correspond to the Leveling Hole where the top-center point of the HandPunch should be mounted.
3. For a hollow wall, drive a small nail into the wall at the mark and hang the wall plate from the Leveling Hole located near the top of the wall plate.
4. For a solid wall, hold the wall plate against the wall, centering the Leveling Hole over the mark in the wall.

5. Align a bubble level with the top edge of the wall plate and gently rotate the wall plate until the bubble level shows that the top edge of the wall plate is level.
6. Secure the plate to the wall using heavy masking tape.
7. Using the wall plate as a template, mark the locations of the two upper screw holes and the three lower screw holes.
8. For a concealed wiring connection, trace the outline of the open area in the center of the wall plate. Identify and mark a 1/2 inch hole through which the HandPunch's wiring will be mounted.
9. For a surface conduit wiring connection, mark the two conduit clamp holes at the right side of the wall plate.
10. Remove the wall plate, masking tape, and the nail (if used).

Mounting the Wall Plate

1. For a hollow wall, use the provided hardware to mount the wall plate. Use the two auger style fasteners for the upper two mounting holes. Use the toggle bolts for the three lower mounting holes.
2. For a solid wall, use expansion bolts to mount the wall plate. For all five mounting holes, drill a 1/4 inch diameter hole, 1/4 of an inch deeper than the length of the expansion anchor.

Routing the Wire

1. Refer to Figure 3-2 on page 14 for a template diagram to assist in routing wiring.
2. For a concealed wiring connection, drill a 1/2 inch hole in a convenient location within the open area of the wall plate. Pull the wiring to enter the HandPunch through this hole in the open area.
3. For a surface conduit wiring connection, drill a 1/4 inch diameter hole, 1/4 of an inch deeper than the length of the expansion anchor for each of the two conduit clamp holes. Route 1/2 inch, flexible conduit to the HandPunch, ending the conduit between the two conduit clamp holes. Pull the wiring to enter the HandPunch through the conduit. Pull 18 inches of wire past the end of the conduit to allow enough space for final connection to the HandPunch.
4. Clear all dust and debris away from the HandPunch mounting location.

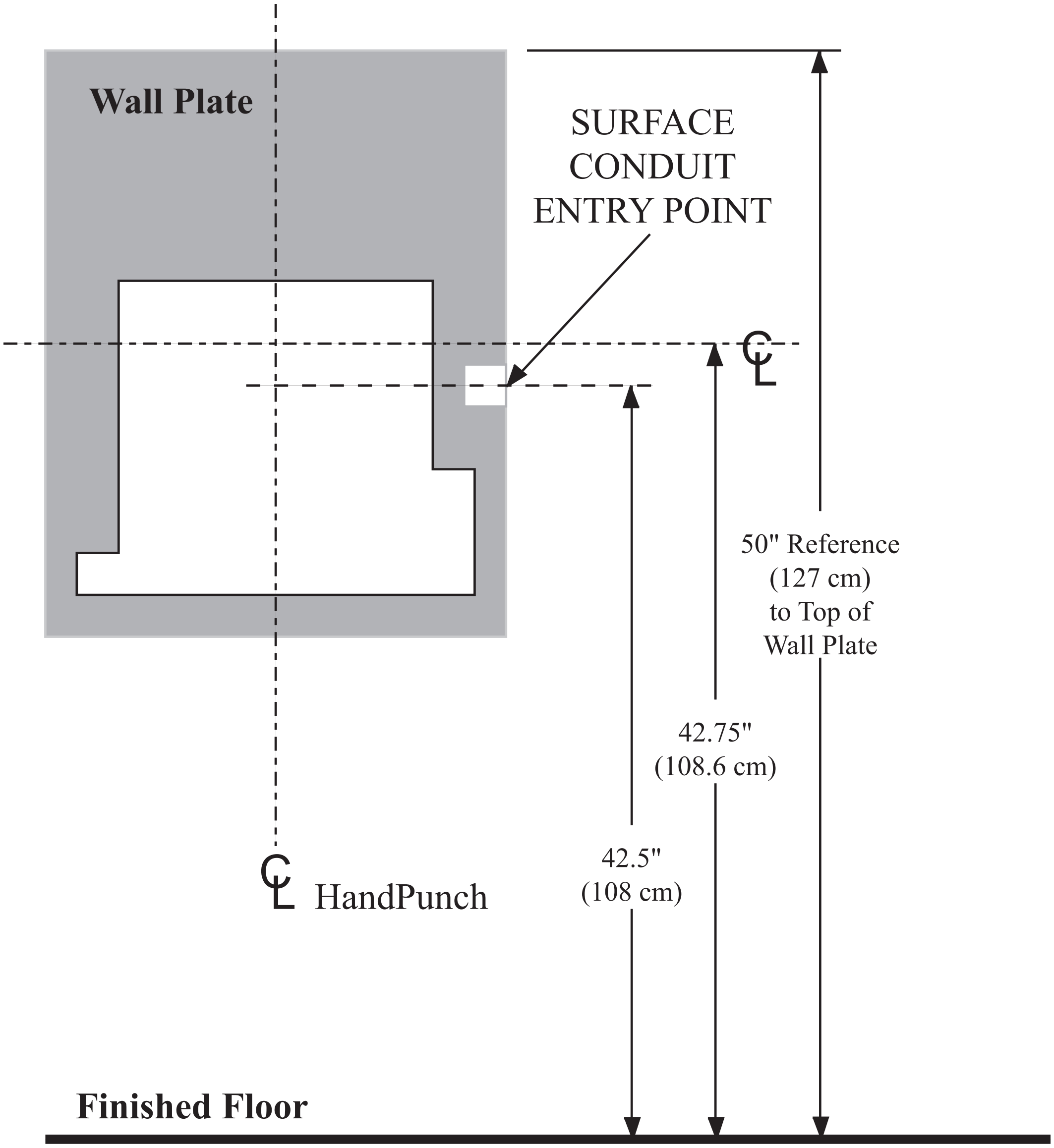

Wall Plate
SURFACE CONDUIT ENTRY POINT
CL
50" Reference (127 cm) to Top of Wall Plate
42.75" (108.6 cm)
42.5" (108 cm)
CL HandPunch
Finished Floor

Figure 3-2: HandPunch Wire Routing Layout

NOTE *Dust and debris surrounding the HandPunch can drastically affect the terminal's operation. It is important to ensure the HandPunch mounting location is free from dust and debris.*

Attaching the HandPunch

1. Remove the HandPunch from its carton.
2. Align the sleeves of the back plate with the pins of the wall plate and slide the HandPunch to the left as shown in "Figure 3-3".

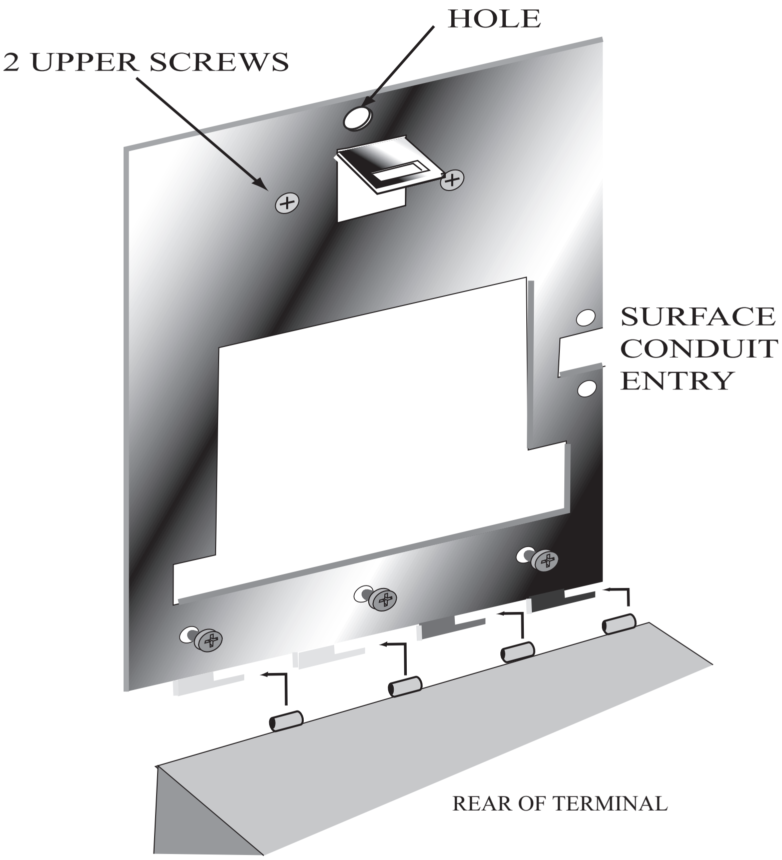


Figure 3-3: Attaching the HandPunch to the Wall Plate

Wiring Connections

Once the HandPunch is attached to the wall plate the wiring connections to the HandPunch can be made (see Figure 4-1).

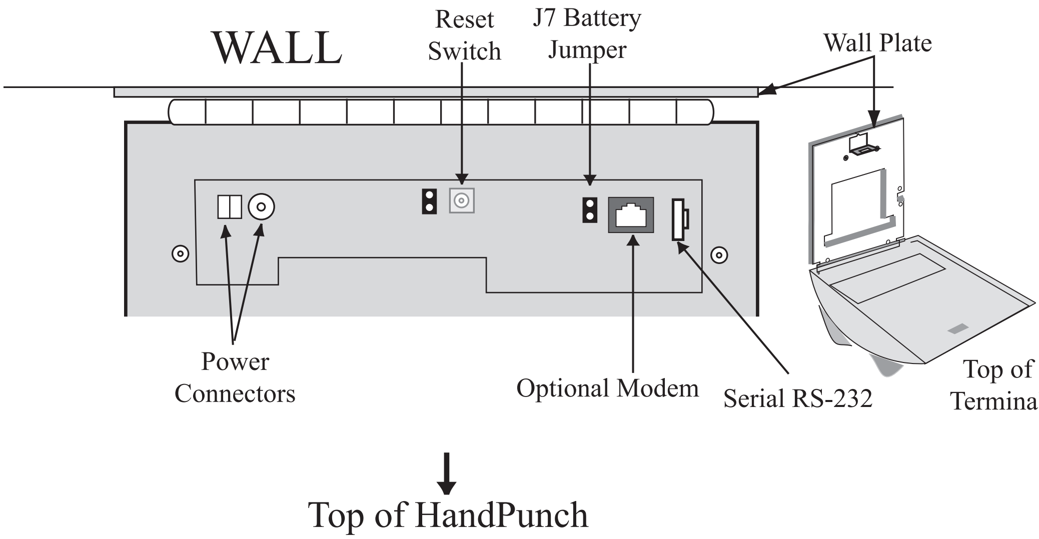


Figure 4-1: Board Layout

Wiring Examples

Table 2 on page 17 provides the pinouts for the RS-232 Serial Host Computer Connection.

Figure 4-2 on page 17 provides a diagram of the RS-232 Connector.

Figure 4-3 on page 18 provides a Serial Connection diagram

Figure 4-4 on page 18 provides a Host PC to HandPunch Modem Network wiring diagram (Modem wiring is a HandPunch option).

Table 2: RS-232 Serial Connection

J8 Pin	Signal	Connection
1	GND	Ground
2	RXD	Receive Data Input (from external device)
3	TXD	Transmit Data Output (to external device)
4	RTS	Ready to Send Output (to external device)

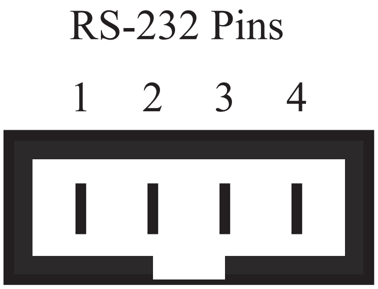


Figure 4-2: J4 - RS-232 Jack Pinout

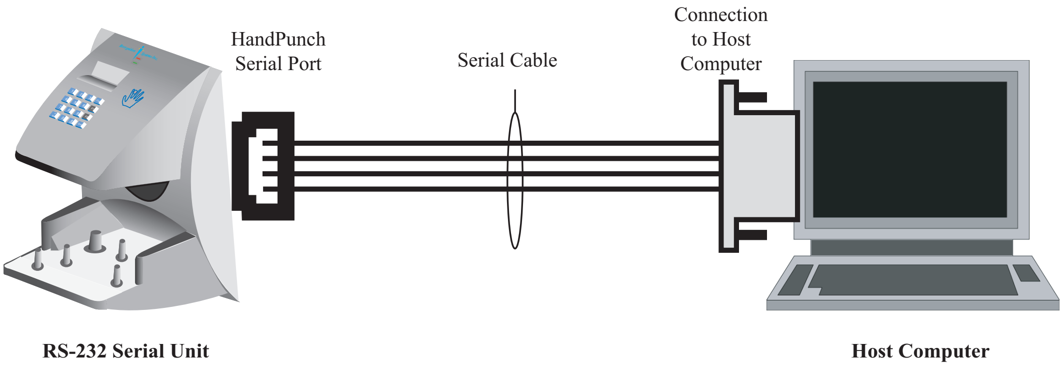


Figure 4-3: Host PC to RS-232 Connection

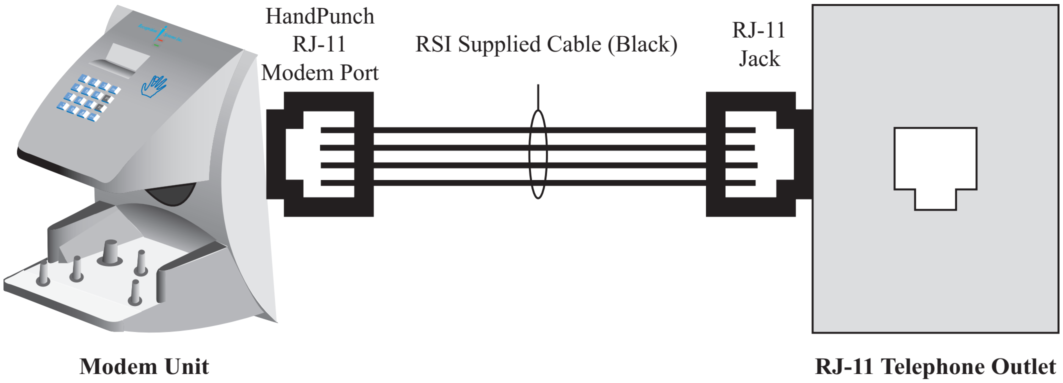


Figure 4-4: Host PC to HandPunch Modem Connection

Erasing the Memory

There are two options when erasing the memory of the HandPunch.

1. Setup
2. All

The erasing of the setup will set the HandPunch's address, passwords, etc. back to factory defaults.

Choosing the All option will take the HandPunch's setup back to factory defaults plus erase all user databases and datalogs. This action can not be undone. If there is a software that is managing the system then the users can be downloaded back to the HandPunch if needed.

Erasing HandPunch Memory

The erase memory function allows a HandPunch's setup and/or user database to be erased.

Perform the following steps to erase the setup programs but retain the user database.

1. With system power OFF, depress reset switch.
2. Turn system power ON and wait 5 seconds.
3. LCD screen will display

```
ERASE                :1 SETUP
                     :9 ALL!!!
```

Closing the HandPunch

Before closing the HandPunch clear all dust and debris away from the HandPunch. With the wall mount latch in the unlocked position, swing the body of the HandPunch up and lock the latch into place with the key provided with the HandPunch (see Figure 6-1).

NOTE *Dust and debris surrounding the HandPunch can drastically affect the terminal’s operation. It is important to ensure the HandPunch is free from dust and debris before closing the terminal.*

NOTE *Do not force the HandPunch onto the wall mount latch when the latch is in the locked position.*

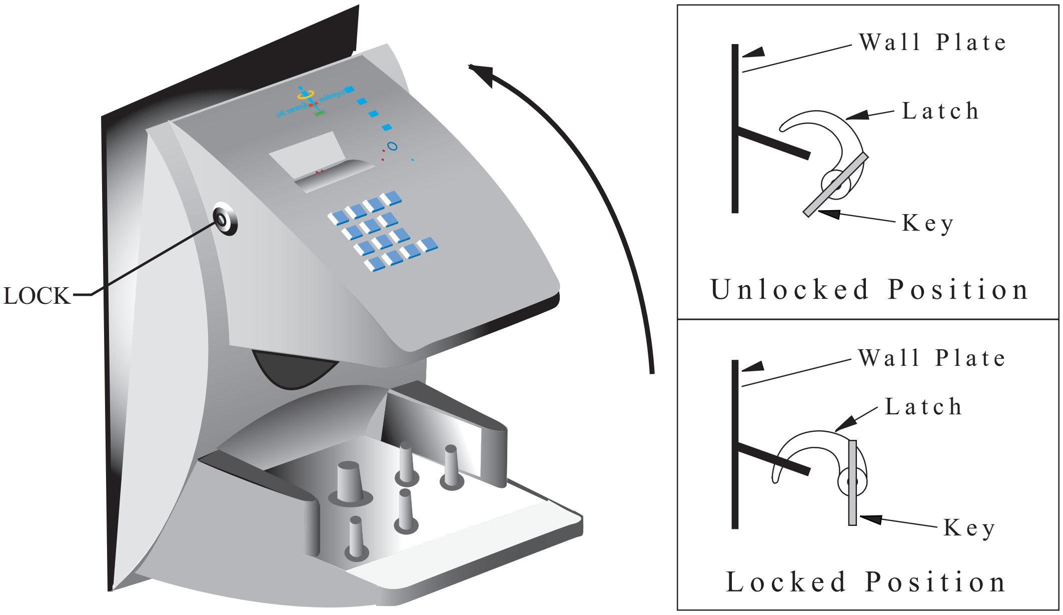


Figure 6-1: Closing the Handpunch

Enter Command Menu

If No One is Enrolled in the HandPunch

Press the CLEAR and ENTER keys simultaneously to enter a command menu.

1. The display appears as follows.

```
ENTER PASSWORD
```

2. Press the default password for the menu you wish to enter.

Press 1 for the Service Menu.

Press 2 for the Setup Menu.

Press 3 for the Management Menu.

Press 4 for the Enrollment Menu.

Press 5 for the Security Menu.

3. Press ENTER and the first command option in the selected menu appears.

If Users are Enrolled in the HandPunch

1. The display appears as follows.

```
ENTER ID
  *:
```

2. Enter your ID number on the keypad and place your hand on the platen for verification.
3. If verification is successful, the display appears as follows.

```
ENTER PASSWORD
```

4. Press the default password for the menu you wish to enter.

Press 1 for the Service Menu.

Press 2 for the Setup Menu.

Press 3 for the Management Menu.

Press 4 for the Enrollment Menu.

Press 5 for the Security Menu.

5. Press ENTER
6. If you are authorized to use this command the first command option in the selected menu appears.
7. If you are not authorized to enter this command the display appears as follows.

```
ENTER
 *:
```

NOTE *To access these menus you must be the first person enrolled in a new system installation or you must have been enrolled as a supervisor. If you are blocked from the supervisory menus, verify your access rights with management personnel. If enrollment information has been incorrectly changed and you must have supervisory access to all menus, make these changes through software.*

NOTE *It is possible to physically reset the HandPunch's memory, however resetting memory sets all unit parameters back to the factory default values. Resetting memory allows access to all menus by the first person enrolled (as if it is a new system installation), but this means that all employee information programmed into the HandPunch is lost and must be re-entered manually. Be sure you need to reset memory before performing this function. To reset memory, refer to the Erasing HandPunch Memory section on page 19.*

Navigating Command Menus

Once you have entered a command menu, there are three options available for navigating the command menu system.

1. Press # to enter the command shown on the display.
2. Press * to step to the next command in the menu.
3. Press CLEAR to exit the command menu (pressing any numeric key also exits the command menu). If you are in a command's sub-menu, you may have to press ENTER multiple times to completely exit the command menu.

Programming the HandPunch

The HandPunch is programmed via a series of command menus. A summary of the menus and commands is given in Table 3.

Table 3: Basic Command Mode Structure

Service Menu	Setup Menu	Management Menu	Enrollment Menu	Security Menu
Password 1	Password 2	Password 3	Password 4	Password 5
Calibrate	Set Language	List Users	Add Employee	Special Enroll
Status Display	Set Date Format	Set User Data	Add Supervisor	
	Set Time and Date		Remove User	
	Set Address			
	Set ID Length			
	Set Serial			
	Upgrade			

To control access to the command menus, each menu has a unique password. This password is requested as a part of the process for accessing each menu. A supervisor must enter the correct password for that menu to access that menu. The default menu passwords are given in Table 3.

To increase the security of the HandPunch, Schlage Biometrics recommends changing the passwords for the command menus to new numbers. These password numbers can be up to 10 digits long. This is done with the Set Passwords command described on.

Autority Level

A second method for controlling access to the command menus is through the use of Authority Levels. Authority Levels control whether or not a user has access to the command menus.

- Level 0 is for a user who does not need access to any of the command menus.
- Level 5 is assigned to Supervisors who need access to all of the command menus.

The HandPunch automatically assigns Authority Level 0 to users enrolled by the Add Employee command. Authority Level 5 is automatically assigned to users enrolled by the Add Supervisor command.

NOTE *Until a user has been assigned to Supervisor, every user can access every menu. Once a user has been enrolled using the Add Supervisor (designated as a supervisor), all further user authority levels are assigned. The first person enrolled should be enrolled using the Add Supervisor command. This protects the integrity of the system.* Schlage Biometrics *strongly recommends enrolling at least two users as supervisors to ensure that more than one person has the authority to access all menus and all commands.*

Programming Order

When setting up HandPunch operations there is a general programming/operations order that should be followed.

Set HandPunch Site Parameters – Set the HandPunch site parameters to meet site-specific needs and usage: change the language used by the display, set the HandPunch's address, and set the serial communication baud rate (used if you have installed a serial printer – see page 30).

Enroll Supervisory Staff – Enroll yourself and the supervisors who will have responsibility for HandPunch management. This is done through the Enrollment Menu (see Supervisor Enrollment on page 37).

NOTE *The time, date, and ID number length are normally set by the host computer. However, a supervisor can change these parameters at a HandPunch after setup information has been downloaded from the host computer.*

These tasks are done through the Setup Menu. The instructions for reader setup parameters begin on page 30.

Train and Enroll Users – Train each user regarding HandPunch usage and then Enroll each user. This is done through the Enrollment Menu. The instructions for employee enrollment begin on page 37. Special enrollment allows you to enroll people with disabilities that prevent them from using the HandPunch properly. Employees with special enrollment ID numbers can punch in without biometric verification.

NOTE *This means that anyone who knows a special enrollment ID number can punch in. This function should only be used if absolutely necessary. The instructions for special enrollment begin on page 38*

System Management

Once a HandPunch system is in operation the following commands are used for system management.

List Users – List the Users authorized to use a HandPunch. This is done through the Management Menu. The instructions for listing employees begin on page 33.

Set User Data – Set a user's reject threshold (adjusting the sensitivity applied when a HandPunch reads a hand) this task is done through the Management Menu. The instructions for setting user data begin on page 33.

Remove User – Remove employees (and supervisors) from a HandPunch. This is done through the Enrollment Menu. The instructions for removing employees begin on page 37.

Service Menu

The Service menu commands provide information that help you determine if the HandPunch is performing within normal operating parameters and identify the status of the unit's inputs and outputs. The following section provides a brief summary of the Service Menu commands.

NOTE *There are no user serviceable parts inside the HandPunch.*

Navigating the Service Command Menu

Enter the appropriate password to enter the Service command menu. Once you have entered the command menu, there are three options available for navigating the command menu system.

- Press # to enter the command shown on the display.
- Press * to step to the next command in the menu.
- Press CLEAR to exit the command menu (pressing any numeric key also exits the command menu). If you are in a command's sub-menu, press ENTER multiple times to completely exit the command menu.

Service Commands

There are two commands available from the Service command menu.

- Calibrate
- Status Display

Refer to Table 4 and identify the command you need to perform. Step through all previous commands until you reach the desired command.

Table 4: Service Command Menu

Service Menu
Password = 1
Calibrate
Recal (Y/N)
Status Display
On/Off (Y/N)

Calibrate

The Calibrate command displays the HandPunch’s exposure values, allowing you to verify these values are within normal operating parameters. The standard operating parameters are shown in Table 5

.

Table 5: Normal Operating Parameters

Parameter	Normal Range
Row “r”	0 +/- 2
Column “c”	0 +/- 2
Exposure “e”	100 +/- 20

Status Display

The status display command allow you to enable or disable the displaying of the following information.

- the status values of HandPunch inputs and outputs
- the hand read score of the last user to verify on the system

When the status display is enabled, Figure 8-1 identifies each status display field value

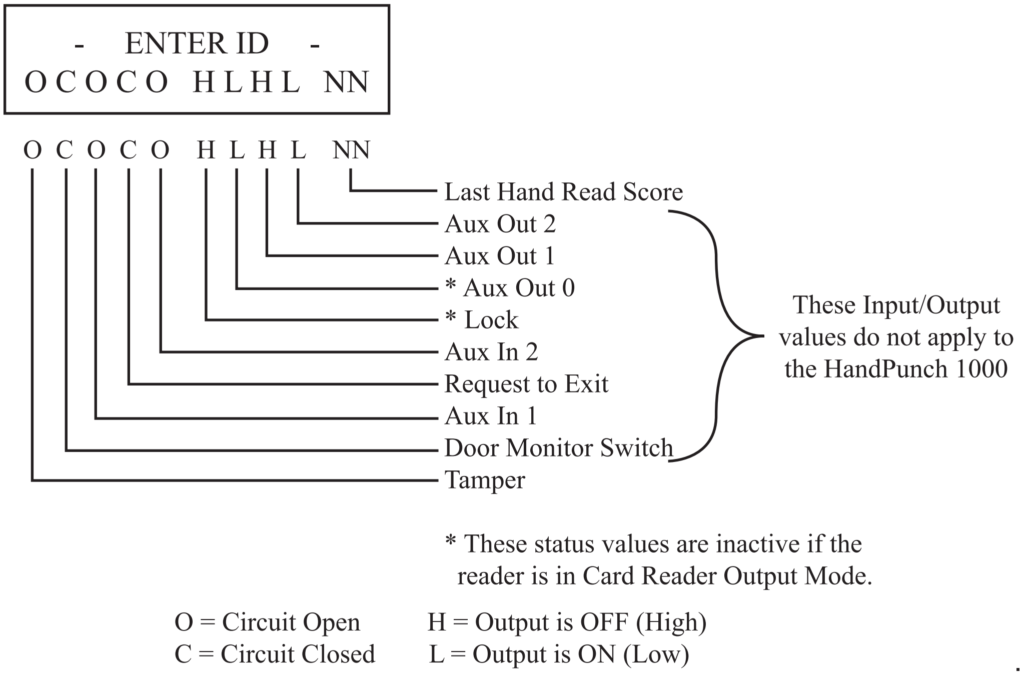


Figure 8-1: Status Display Chart

Setup Menu

The Setup menu commands allow you to set the basic operating parameters for the HandPunch unit. The following section provides a brief summary of all the parameters that may be set on a HandPunch unit.

!NOTE *Once in the Command Menu, you can step through and set the parameters for each command sequentially. You do not have to exit command mode after setting any individual command.*

Navigating the Setup Command Menu

Enter the appropriate password to enter the Setup command menu. Once you have entered the command menu, there are three options available for navigating the command menu system.

- Press # to enter the command shown on the display.
- Press * to step to the next command in the menu.
- Press CLEAR to exit the command menu (pressing any numeric key also exits the command menu). If you are in a command's sub-menu, press CLEAR multiple times to completely exit the command menu.

Setup Commands

There are six commands available from the Setup command menu.

- Set Language
- Set Date Format
- Set Date and Time
- Set Address
- Set ID Length
- Set Serial

Refer to Table 6 on page 30 and identify the command you need to perform. Step through all previous commands until you reach the desired command.

Table 6: Setup Command Menu

Setup Menu
Password = 2
Set Language
Select Language
Set Date Format
Select Date Format
Set Time and Date
Month (MM)
Day (DD)
Year (YY)
Hour (HH)
Minute (MM)
Set Address
New Address
Set ID Length
New ID Length
Set T & A Mode
Set Serial
RS-232
Select Baud Rate
Upgrade
Code

Set Language

The Set Language command allows the language shown on the HandPunch’s display to be “localized” for a variety of countries.

- English
- Japanese
- French
- Italian
- Spanish
- German
- Russian
- Indonesian
- Portuguese
- Polish

Set Date Format

The Set Date Format command allows the date format shown on the HandPunch’s display to be “localized” for a variety of countries.

mm/dd/yy

dd-MMM-yy

dd-mm-yy

dd/mm/yy

-mm-dd-yy

-MMM dd,yy

-ddMMMyyyy

Set Time and Date

The Set Time and Date command allows the HandPunch’s time and date to be set. This is normally not necessary as the HandPunch’s time and date are set by the host computer.

Set Address

The Set Address command allows a unique address to be set for each HandPunch in a network. For proper operation, each HandPunch in the network must have a unique address. All units may use any address from 0 to 254. All units are sent with the address set to 1.

Set ID Length

The Set ID Length command allows you to reduce the number of keystrokes required to enter the ID number by eliminating the use of the ENTER key to complete an ID number entry. Once the ID Length is set, the HandPunch will automatically accept an ID number entry once the correct number of characters have been entered.

Set ID Length does not apply when ID entry is made from a card reader. Once the ID Length is set, the T & A Mode Set command appears, allowing you to configure the HandPunch to prepare punch data for time and attendance software.

Set Serial

The Set Serial command allows you to set the baud rate communication parameters.

Upgrade

This Upgrade Menu is where the HandPunch code gets input to allow for a Memory Upgrade

Management Menu

The Management menu commands allow you to manage employee data stored in a HandPunch unit. The following section provides a brief summary of the employee data that may be manipulated on a HandPunch unit.

Navigating the Setup Command Menu

Enter the appropriate password to enter the Setup command menu. Once you have entered the command menu, there are three options available for navigating the command menu system.

- Press # to enter the command shown on the display.
- Press * to step to the next command in the menu.
- Press CLEAR to exit the command menu (pressing any numeric key also exits the command menu). If you are in a command's sub-menu, press CLEAR multiple times to completely exit the command menu.

Management Commands

There are four commands available from the Management command menu.

- List Users
- Set User Data

Refer to Table 7 and identify the command you need to perform. Step through all previous commands until you reach the desired command.

Table 7: Setup Command Menu

Setup Menu
Password = 3
List Users
Display
Print
Set User Data
User Reject

List Users

The List Users command allows you to display or print a list of all the employees enrolled in a HandPunch.

Set User Data

The Set User Data command allows you to set an employee's Reject Threshold, adjusting the hand read threshold for one employee without affecting the threshold of other employees. This task should be done through your user software, however it can be done through the Management Menu.

Enrollment Menu

Enrollment is the process of recording a hand image and associating it with an ID number. The first person to enroll in the HandPunch has access to all command menus. This person should enroll using the Add Supervisor command (see page 37). Once a supervisor has been enrolled, all further enrollments use the following rules:

- A user enrolled through the Add Employee command (page 37) is assigned Authority Level 0. This allows the user to punch in and/or gain access through a door secured by the HandPunch.
- A user enrolled through the Add Supervisor command (see page 37) is assigned Authority Level 5. This allows the supervisor to punch in and gain access through a door secured by the HandPunch, and it allows the supervisor to access all command menus.

!NOTE *Until a user has been assigned to Authority Level 5 using the Add Supervisor command, every user with Authority Level 0 can access every menu. This is done to ensure that the first person enrolled is able to access all the menus to perform all the programming required to support the HandPunch. Once a user has been enrolled using the Add Supervisor command, all further user authority levels are assigned as per the list above. This protects the integrity of the system by enacting the Authority Level rules described above. Schlage Biometrics strongly recommends enrolling at least two users as supervisors to ensure that more than one person has the authority to access all menus and all commands.*

Advance planning and training make enrollment fast and easy. Users should be informed on what to expect and how to place their hands on the HandPunch before you enroll them.

Navigating the Setup Command Menu

Enter the appropriate password to enter the Setup command menu. Once you have entered the command menu, there are three options available for navigating the command menu system.

- Press # to enter the command shown on the display.
- Press * to step to the next command in the menu.
- Press CLEAR to exit the command menu (pressing any numeric key also exits the command menu). If you are in a command's sub-menu, press CLEAR multiple times to completely exit the command menu.

Preparation

Here are a few guidelines to help you prepare for an enrollment session.

- You can enroll one person or a group of people during an enrollment session.
- Each user must have a unique personal identification (ID) number. It will save you considerable time if you assign the ID numbers in advance.
- The HandPunch will not accept two people with the same ID number.
- If you enroll people using the last four digits of their phone numbers or social security numbers, you may get duplicate numbers.
- If you are enrolling large groups of people you may consider using an enrollment trainer. It is a replica of a platen that is available through your Schlage Biometrics reseller.

User Education

The HandPunch is easy to use and non-threatening. However, most people have never used a biometric HandPunch. Training users on how the HandPunch works and how to use it will eliminate most fears and concerns before they occur. Inform the users of these facts.

- The HandPunch reads the shape of the hand, not the fingerprints or palmprints.
- It does not identify people. It confirms people's identity.
- It scans with an invisible light of the type used in TV remote controls.
- It does not transfer germs any more than a doorknob or money.
- It does not invade privacy; it guarantees it.
- The enrollment process requires three or more reads to collect enough information to create a template.

Proper Hand Placement

For correct, consistent hand reads it is very important that your hand is placed on the platen in the same manner every time. The following rules apply for proper hand placement on the platen also refer to Figure 8-2 bellow.

- If you are wearing a ring, rotate the ring so the stone faces up in its normal position.
- Slide your right hand onto the platen rather like an airplane landing at the airport.
- Slide your hand forward until the web between your index and middle finger stops against the Web Pin.
- Keep your hand flat. You should feel the surface of the platen on your palm and the underside of your fingers.
- Close your fingers together until they touch the Finger Pins and watch the hand diagram light display on the top panel.
- The lights go out when you have properly placed your fingers. If a light remains on, a finger is not in proper contact with its Finger Pin.

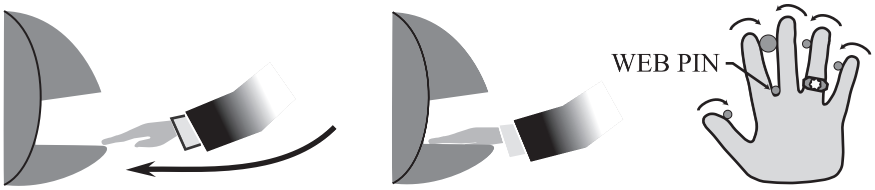


Figure 8-2: Placing Your Hand on the Platen

Left Hand Enrollment

Some right hands cannot be used in the HandPunch due to disabilities such as missing fingers. You can enroll a user with the left hand facing palm side up. The techniques for left hand enrollment are the same as for standard enrollment. The user should keep the back of the hand flat against the platen and move the fingers against the web pin and the finger pins in the same manner as in standard enrollment. Users enrolled with the left hand must always verify with the left hand. Extra practice on placing the hand on the platen may be required to ensure correct, consistent hand reads.

Read Score

When a user uses the HandPunch the display appears as follows.

```
    OKAY (USER ID)
SCORE IS: (SCORE NUMBER)
```

The score number on the display reflects how accurately the user's hand is placed on the platen. Scores that vary greatly between low and high numbers are indicative of inconsistent hand placement. Scores above 50 are indicative of improper hand placement or of a drastic change in the physical appearance of the hand.

When this occurs, emphasize the importance of sliding the hand onto the platen and keeping the hand flat. Re-training and practice should lower a user's score. It might be necessary to change a user's reject threshold if the user has a mild disability. Re-enrollment might be necessary to create a new user template.

Enrollment Commands

There are three commands available from the Enrollment command menu.

- Add Employee
- Add Supervisor
- Remove User

Refer to Table 12 to identify the command you need to perform. Step through all previous commands until you reach the desired command.

Table 8: Enrollment Command Menu

Service Menu
Password = 4
Add Employee
ID #
Add Supervisor
ID
Remove User
ID

Add Employee

The Add Employee command allows you to enroll a new employee into the HandPunch.

Add Supervisor

The Add Supervisor command allows you to enroll a new supervisor into the HandPunch.

Remove User

The Remove User command allows you to remove an employee or supervisor from the HandPunch.

Special Menu

The Special menu has one command – Special Enroll. This command accommodates users with disabilities that make it difficult or impossible to use a HandPunch in its standard way. The following section provides a brief description of the Special Menu command.

Navigating the Special Command Menu

Enter the appropriate password to enter the Special command menu. Once you have entered the command menu, there are three options available for navigating the command menu system.

- Press # to enter the command shown on the display.
- Press * to step to the next command in the menu.
- Press CLEAR to exit the command menu (pressing any numeric key also exits the command menu). If you are in a command's sub-menu, press CLEAR multiple times to completely exit the command menu.

Special Command

There is one command available from the Special command menu.

- Special Enroll

Refer to Table 9 and identify the command you need to perform. Step through all previous commands until you reach the desired command.

Table 9: Special Command Menu

Special Menu
Password = 5
Special Enroll
ID
On/Off (Y/N)

Special Enroll

The Special Enroll command allows a user to be enrolled such that the ID number is the primary criteria for determining access. A hand read is required, but is not verified against any stored identification data. A time zone value can be applied to the Special Enrollment ID number to limit access times. The HandPunch default is for no time zone to be applied.

NOTE *Special Enrollment affects the integrity of the HandPunch terminal and should only be used as a last resort. Anyone who knows a Special Enroll ID number is granted access when the ID number is used. Before specially enrolling a user, try to alleviate verification problems by adjusting the individual user's reject threshold (see page 36) or by using left hand enrollment (see page 36).*

HandPunch Maintenance

A minimum amount of system maintenance is required to keep HandPunchs fully functional. HandPunchs should be cleaned periodically to prevent an accumulation of dust from affecting the HandPunch's readability. User Scores should be reviewed periodically to ensure the HandPunch is performing properly.

!NOTE *There are NO user serviceable parts inside the HandPunch.*

Once a HandPunch system is in operation there are two HandPunch commands that can assist with system maintenance. These commands are performed through the Service Menu. The instructions for these commands begin on page 24.

- Calibrate – View HandPunch exposure values.
- Status Display – Display HandPunch input/output status, the hand read score of the last user to verify on the system.

Cleaning the HandPunch

Inspect and clean the HandPunch regularly to maintain optimum performance. Clean the platen, side mirror, reflector, and the window above the platen using a clean cloth dampened with ordinary, non-abrasive window cleaner (see Figure 9-1). Start at the rear corners of the platen and work your way forward.

!NOTE *DO NOT SPRAY CLEANING FLUID DIRECTLY INTO OR ON THE HandPunch.*

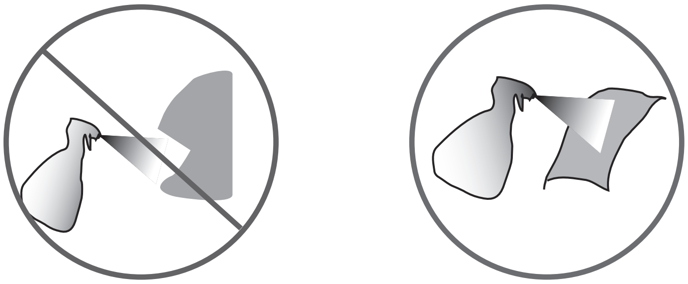


Figure 9-1: HandPunch Cleaning

User Score

Periodically check users' scores (refer to the Read Score section on page 36). Scores should average under 30. Occasionally a user will score above 30. This is not necessarily an indication of poor performance. If a number of scores average over 30, clean the HandPunch and check scores again. If scores remain high, or if users are experiencing frequent rejections, run the Calibration command (see page 28).

Appendix A

Tips for a successful Installation

HandPunch

- Think of the HandPunch as a camera
- Clean the HandPunch before it gets dirty
- Use non-abrasive cleaners such as glass cleaners and non-abrasive and clean cloths
- Make cleaning the HandPunch part of Janitorial program
- Do not remove the foam backing from the wall mounting plate
- Seal any holes made in the wall for wire routing, so that dust will not blow into the HandPunch

Location

- Mount all HandPunchs in a network so that the top of the platen is 40" off of the floor
- If an enrollment HandPunch is used make sure that it is placed with the top platen 40" off of the floor and not sitting directly on top of a desk, this will help to eliminate "bad enrollments"
- Mount the HandPunch so that it is not difficult or dangerous to verify then open the door
- It is not recommended to mount the HandPunch in an area where there is airborne dust, in the path of direct sunlight, or where the HandPunch can be exposed to water or corrosive gasses

Enrollment

- Educate the Enrollee on Hand Geometry
- Explain enrollment process
- Train Enrollee on hand placement
    - Practice placing hand on platen
    - Rotate rings to be stone-up
    - Make sure hand is flat on platen
    - Close finger towards the center of hand
    - Fingers gently touch finger pins
- Let the enrollee enter in their own ID number during the enrollment process, this forces the Enroller to step aside allowing the Enrollee to stand in front of the HandPunch helping to eliminate "bad enrollments"
- If an enrollment transaction fails:
    - Retrain the user on correct placement and ensure that rings are rotated to be stone-up then Rotate rings to be stone-up
    - Try again to enroll the same handClose finger towards the center of hand
    - try to enroll the other hand (with the hand placed upside-down so the thumb still contacts the thumb-pin on the platen)
- After enrollment, it is a good idea to let the enrollee enter their ID number and practice a verification transaction to ensure that the enrollment was high-quality
- If a user consistently fails during verifications days/months/years later, re-enroll the user to ensure a high quality and up-to-date enrollment record

Appendix B

Noted Board Configuration Differences

Because of Schlage Biometrics' camera retrofit of the HandPunch some changes have been made to the main PCB and they are listed as follows:

- Dipswitches have been removed
  - memory is reset with a push-button reset and user interface with keypad and LCD
- Power has moved to the right side of the PCB
- The RS-232 RJ-45 receptacle has been replaced with a 4 pin Molex connector on the left side of the PCB
- A 2 pin Molex connector (J5) has been added to the board, next to the reset button, to supply power for the LEDs. This connector should never be unplugged. unless a modem or Ethernet is added to the PCB
- The upgrading of the memory is now handled through software codes at the HandPunch. Contact Order Entry for memory upgrades

Memory Reset

To reset the memory of the HandPunch follow these steps-

1. Remove power and battery jumper, if a back up battery is installed
2. Press down on reset button and apply power
3. Release button
4. Reader will boot to

```
ERASE              :1 SETUP
                    :9 ALL!!!
```

- Press 1 to erase setup i.e. address, outputs, passwords, but retain user database and datalogs
- Press 9 to erase everything i.e. HandPunch goes back to factory defaults

Appendix C

Mechanical Installation

Select an installation location based on the guidelines provided in the Planning an Installation section beginning on page 8.

Wall Plate Installation

Wall Preparation

For the following procedure protect the HandPunch from the dust and debris generated during the wall plate installation process.

1. Remove the wall plate from the packing carton. Refer to Figure 12-1 for all wall plate references in the following section.

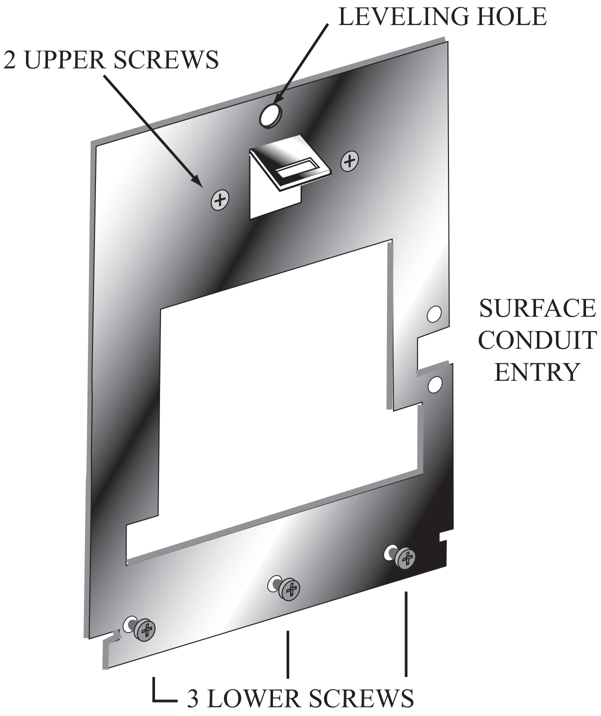


Figure 12-1: Wall Plate

2. Measure and mark a point 48 1/2 inches (123 cm) from the surface of the finished floor. This point will correspond to the Leveling Hole where the top-center point of the HandPunch should be mounted.
3. For a hollow wall, drive a small nail into the wall at the mark and hang the wall plate from the Leveling Hole located near the top of the wall plate.
4. For a solid wall, hold the wall plate against the wall, centering the Leveling Hole over the mark in the wall.Mechanical Installation

5.
6. Align a bubble level with the top edge of the wall plate and gently rotate the wall plate until the bubble level shows that the top edge of the wall plate is level.
7. Secure the plate to the wall using heavy masking tape.
8. Using the wall plate as a template, mark the locations of the two upper screw holes and the three lower screw holes.
9. For a concealed wiring connection, trace the outline of the open area in the center of the wall plate. Identify and mark a 1/2 inch hole through which the HandPunch's wiring will be mounted.
10. For a surface conduit wiring connection, mark the two conduit clamp holes at the right side of the wall plate.
11. Remove the wall plate, masking tape, and the nail (if used).

Mounting the Wall Plate

1. For a hollow wall, use the provided hardware to mount the wall plate. Use the two auger style fasteners for the upper two mounting holes. Use the toggle bolts for the three lower mounting holes.
2. For a solid wall, use expansion bolts to mount the wall plate. For all five mounting holes, drill a 1/4 inch diameter hole, 1/4 of an inch deeper than the length of the expansion anchor.

Routing the Wiring

1. Refer to Figure 12-2 on page 45 for a template diagram to assist in routing wiring.
2. For a concealed wiring connection, drill a 1/2 inch hole in a convenient location within the open area of the wall plate. Pull the wiring to enter the HandPunch through this hole in the open area.
3. For a surface conduit wiring connection, drill a 1/4 inch diameter hole, 1/4 of an inch deeper than the length of the expansion anchor for each of the two conduit clamp holes. Route 1/2 inch, flexible conduit to the HandPunch, ending the conduit between the two conduit clamp holes. Pull the wiring to enter the HandPunch through the conduit. Pull 18 inches of wire past the end of the conduit to allow enough space for final connection to the HandPunch.
4. Clear all dust and debris away from the HandPunch mounting location.

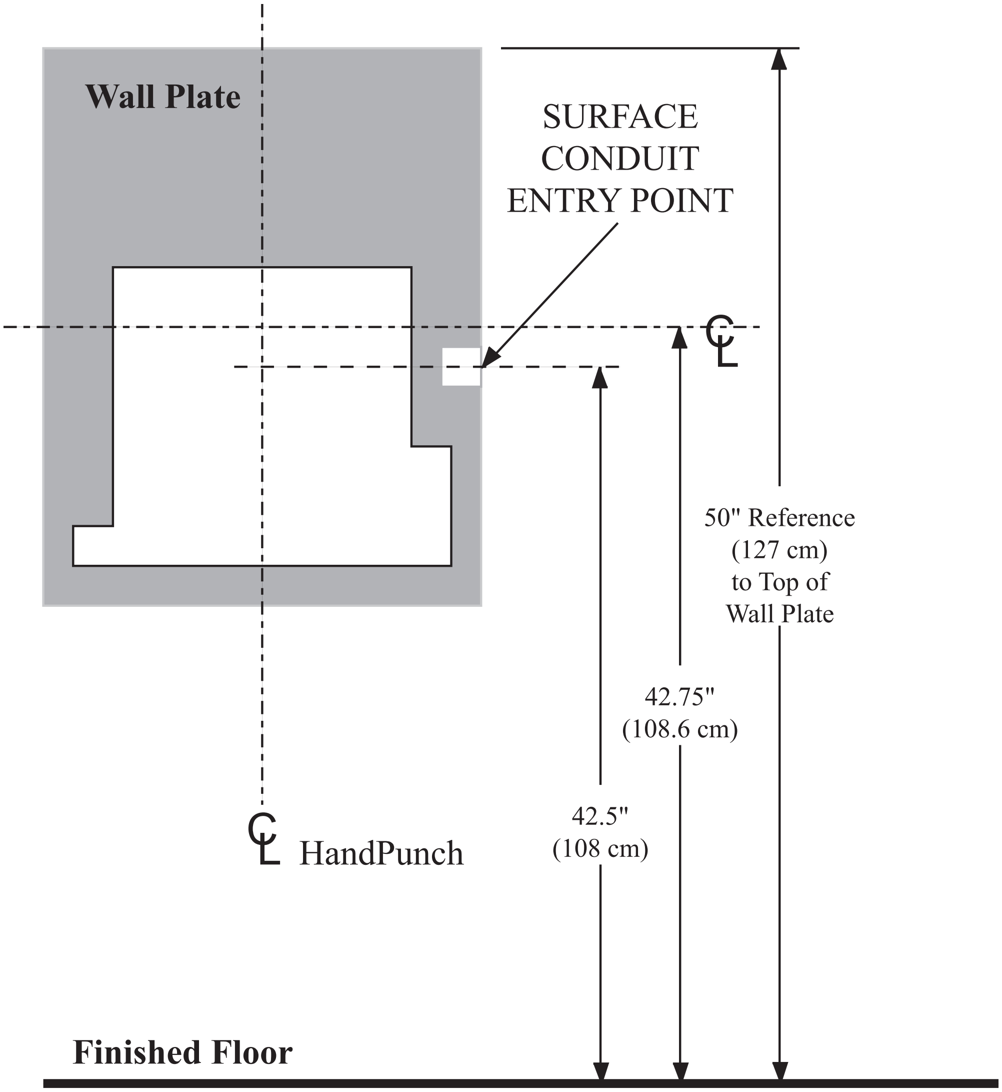

Wall Plate
SURFACE CONDUIT ENTRY POINT
℄
50" Reference (127 cm) to Top of Wall Plate
42.75" (108.6 cm)
42.5" (108 cm)
℄ HandPunch
Finished Floor

Figure 12-2: HandPunch Wire Routing Layout

NOTE *Dust and debris surrounding the HandPunch can drastically affect the terminal's operation. It is important to ensure the HandPunch mounting location is free from dust and debris.*

Attaching the HandPunch

1. Loosen the three bottom mounting screws until there is approximately 1/8 inch (3 mm) clearance between the screw head and the wall plate.
2. Remove the HandPunch from its carton.
3. At the base of the HandPunch is a piano hinge with three keyhole shaped slots that correspond with the three lower mounting screws. Align and hang the HandPunch from the three lower mounting screws (see Figure 12-3 on page 46).
4. Tighten all three lower mounting screws.
5. The HandPunch is now ready for its wiring connections.

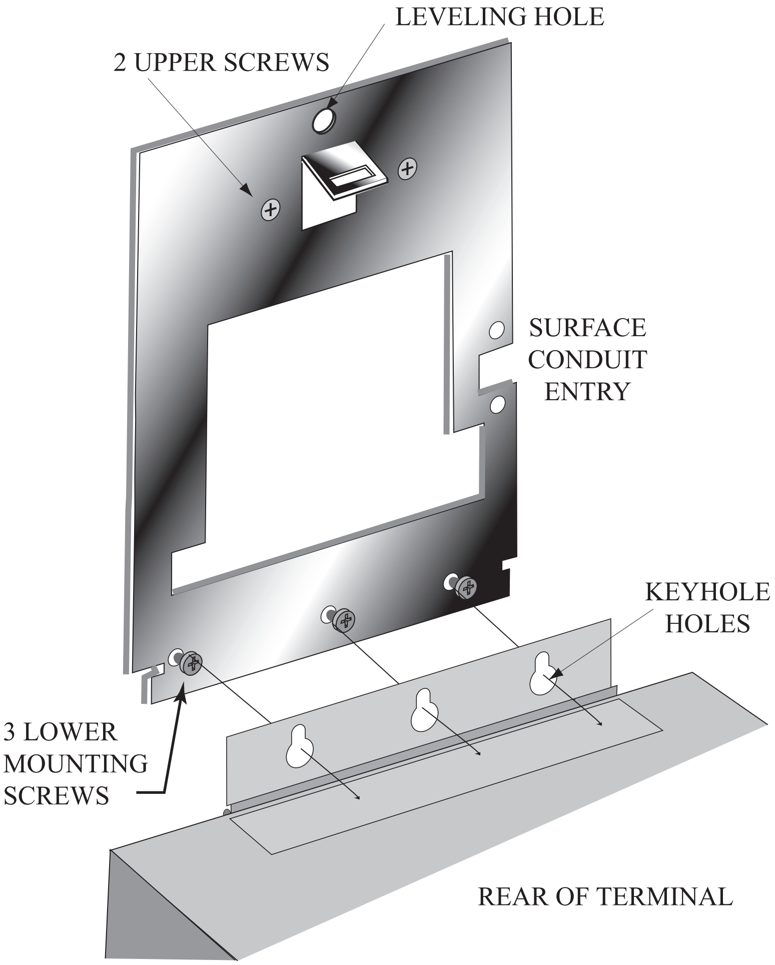


Figure 12-3: Attaching the HandPunch to the Wall Plate

Wiring Connections

Once the HandPunch is attached to the wall plate the wiring connections to the HandPunch can be made (see Figure 12-4).

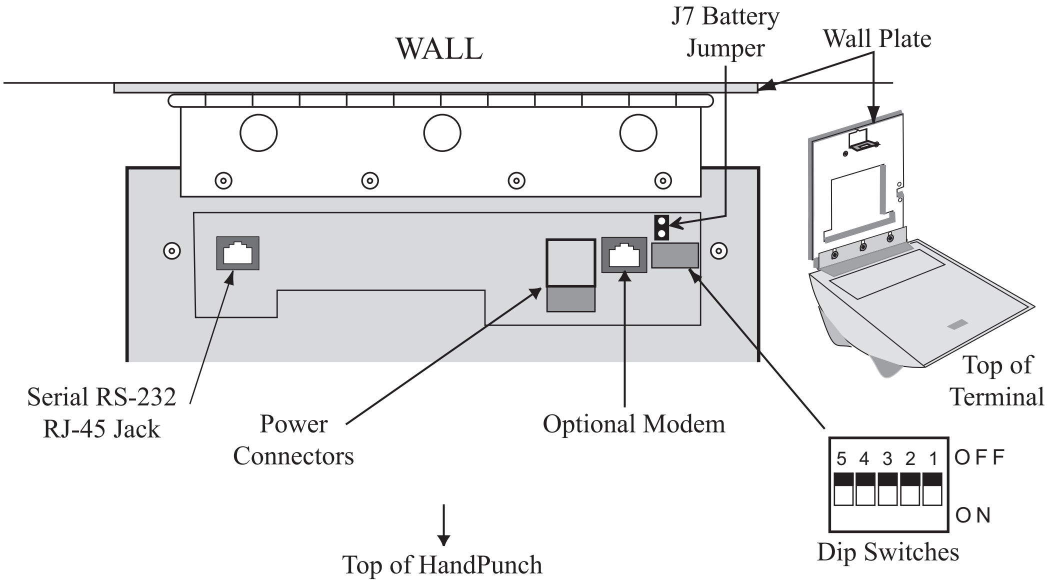


Figure 12-4: Wiring Connections and Dip Switches

Wiring Examples

Table 10 on page 48 provides the pinouts for the RJ-45/RS-232 Serial Host Computer Connection.

Figure 12-5 on page 48 provides a diagram of the RJ-45/RS-232 Connector.

Figure 12-7 on page 49 provides a Host PC to HandPunch Modem Network wiring diagram (Modem wiring is a HandPunch option).

Table 10: RJ-45/RS-232 Serial Connection

J8 Pin	Signal	Connection
1	RJ	- not used -
2	CD	- not used -
3	DTR	- not used -
4	GND	Ground
5	Rx Data	Receive Data Input (from external device)
6	Tx Data	Transmit Data Output (to external device)
7	CTS	- not used -
8	RTS	- not used -

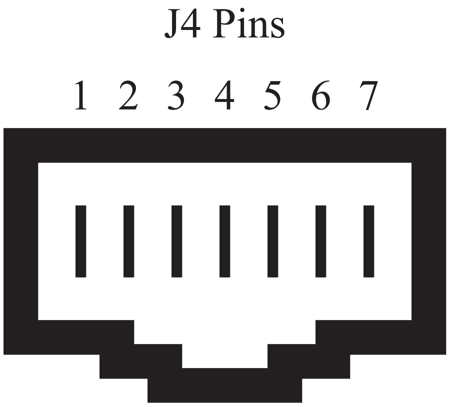


Figure 12-5: J4 - RJ-45/RS-232 Jack Pinout

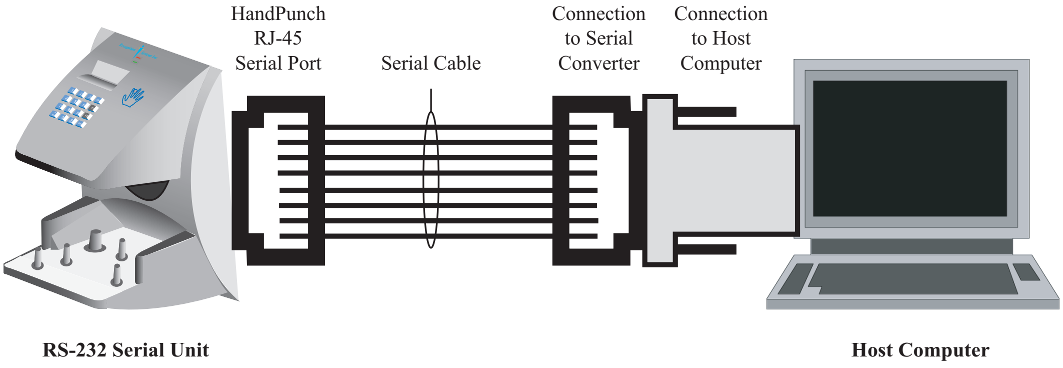


Figure 12-6: Host PC to RS-232 Connection

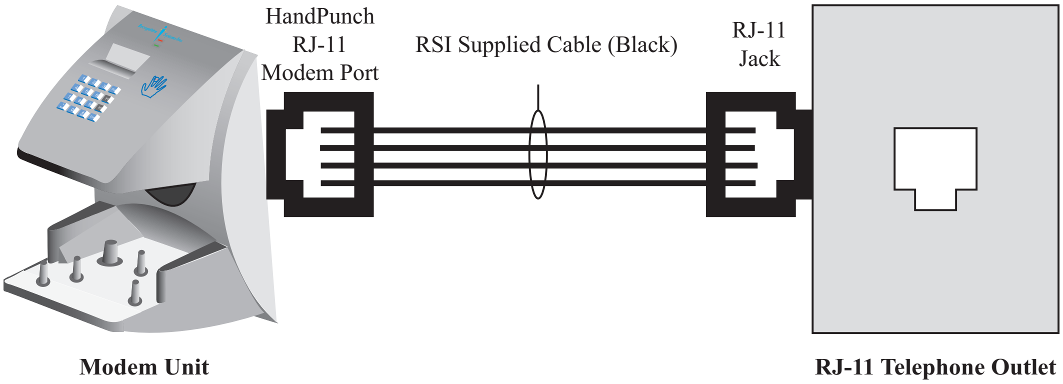


Figure 12-7: Host PC to HandPunch Modem Connection

Setting the DIP Switches

The DIP Switch settings perform three tasks for the HandPunch (see Figure 12-8).

- Set End of Line (EOL) Termination to match the type of termination needed by the network.
- Set the Communication Method to match the type of network used.
- Erase Memory to clear HandPunch memory to all factory default values and also clear all user memory.

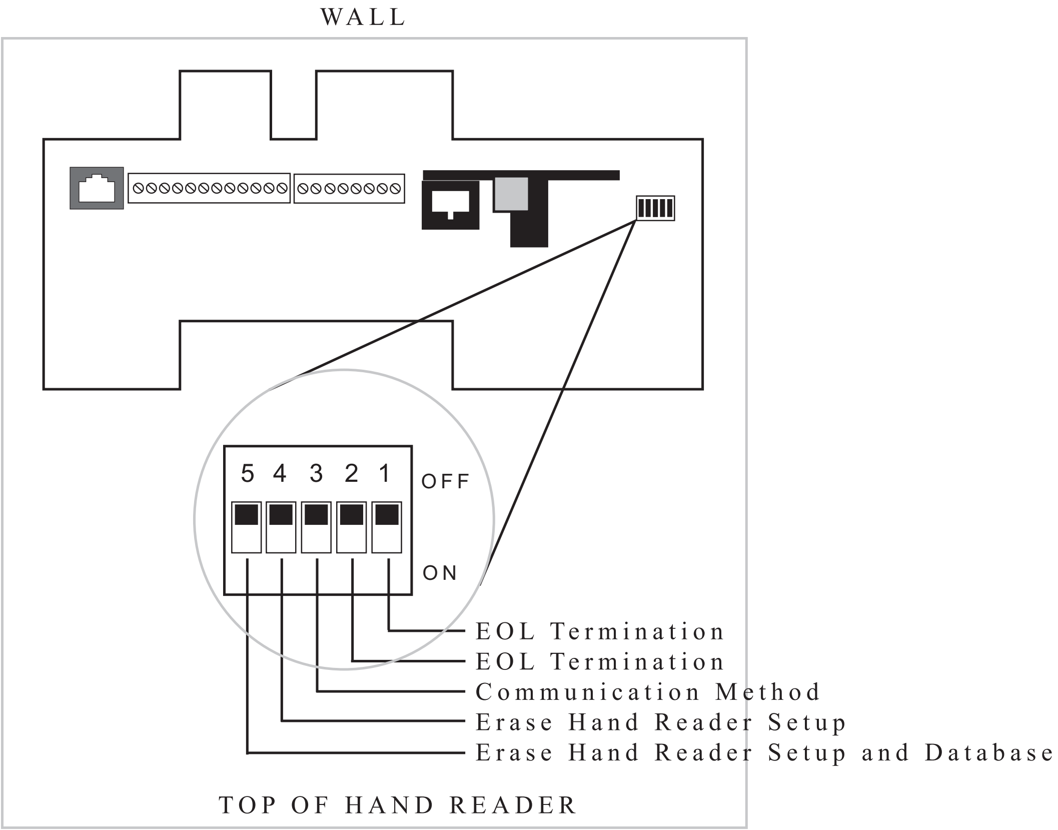


Figure 12-8: HandPunch Dip Switches

End of Line Termination

Termination helps to ensure clean data signals are transmitted through the network wiring. Termination is applied to the end-of-line (EOL) HandPunch in the network daisy-chain. The factory default setting is for EOL termination to be disabled – switches 1 and 2 OFF. Refer to Figure 12-8 on page 50 for switch ON/OFF positioning.

- To enable EOL termination at a HandPunch, both switches 1 and 2 must be ON.
- To disable EOL termination at a HandPunch, both switches 1 and 2 must be OFF.

EOL Termination must be enabled for:

- A single HandPunch terminal installation.
- In a Modem to PC network the HandPunch terminal with the Modem option (for communication with the host computer).

Communication Method

The factory default setting and for standard operation, switch 3 must be OFF.

- Switch 3 must always be OFF.

Erasing HandPunch Memory

The erase memory function can perform either or both of the following:

- Erase a HandPunch's configuration data.
- Erase a HandPunch's user database and transaction buffer.

The factory default setting (and normal operation setting) is for switches 4 and 5 to be OFF, retaining memory.

If the HandPunch is equipped with the battery backup option, remove shunt J7 in front of the DIP switch array (see Figure 12-4 on page 47) before proceeding. Replace shunt J7 after completion of the following steps.

Erasing the HandPunch Setup

Perform the following steps to erase the configuration data but retain the user database.

With system power OFF, set switch 4 ON.

Turn system power ON and wait for HandPunch boot information to appear on the display.

Turn switch 4 OFF.

Erasing the HandPunch Setup and User Database

Perform the following steps to erase both the configuration data and the user database.

1. With system power OFF, set both switches 4 and 5 ON.
2. Turn system power ON and wait 5 seconds.
3. Turn both switches 4 and 5 OFF.

! **NOTE** *Before putting the HandPunch into service ensure DIP switches 4 and 5 are both OFF. If switches 4 and 5 are not off, the next time the HandPunch's power is cycled the HandPunch's memory will be erased.*

Closing the HandPunch

Before closing the HandPunch, ensure dip switches 4 and 5 are OFF (refer to Figure 12-8 on page 50). Clear all dust and debris away from the HandPunch. With the wall mount latch in the unlocked position, swing the body of the HandPunch up and lock the latch into place with the key provided with the HandPunch (see Figure 12-9).

NOTE *Dust and debris surrounding the HandPunch can drastically affect the terminal's operation. It is important to ensure the HandPunch is free from dust and debris before closing the terminal.*

NOTE *Do not force the HandPunch onto the wall mount latch when the latch is in the locked position.*

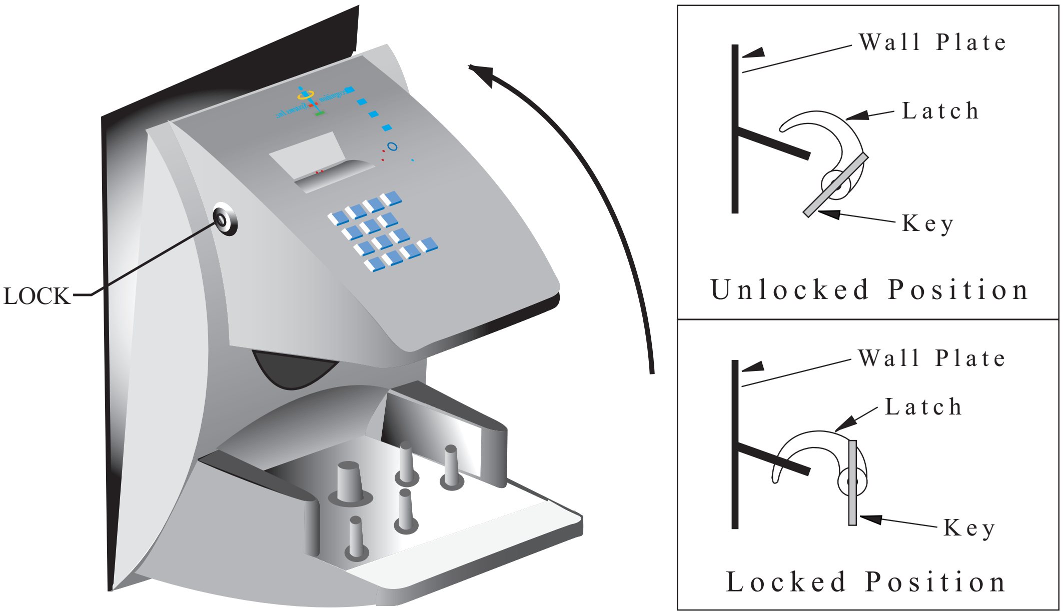


Figure 12-9: Closing the HandPunch

Appendix D

Troubleshooting Guide

Display Messages During Verification

Various messages can appear on the HandPunch's display during hand verification. These messages are defined in Table 18.

Table 11: Display Messages During Verification

Message	Definition
PLACE HAND	The platen is ready to receive your hand for verification.
ID VERIFIED	You are verified, proceed.
REMOVE HAND	Remove your hand and place it on the platen again. Follow proper hand placement rules.
TRY AGAIN	Your attempt was rejected. Repeat verification following proper hand placement rules.
ID REFUSED	Your rejections exceeded the maximum number of tries allowed. Wait until another employee has verified and try again or call your supervisor
ENTER ID	You entered your ID number incorrectly or your access time is restricted.

- If the display shows **TRY AGAIN**, you are not verified. You may have made an error in entering your ID number or in placing your hand on the platen. Re-enter your ID number and try again, taking care to follow proper hand placement rules (see page 35).
-
- If the display shows **TIME RESTRICTION**, you are not authorized to punch in at this time. If this seems to be in error, contact your supervisor about time restrictions.
-
- After a pre-programmed number of denied attempts, an ID number will no longer be accepted and the display will appear as follows.

ID INVALID
TEMPORARILY

This is called a “lockout.” Before the rejected ID number can be used again, another employee or a supervisor must successfully verify at the HandPunch.

- If you enter your ID number, but do not place your hand on the platen, the HandPunch will time-out in about 25 seconds. You can immediately end this time-out by pressing the **CLEAR** key.

Beeper and LED Status During Verification

The HandPunch’s beeper and LED status display also display hand verification information. This information is defined in Table 19.

Beeper and LED Status During Verification

Operation	Beeps	LED	Meaning
During Keypad Entry	1 per Keystroke	–	Keystroke Accepted
After ID Entry	–	–	OK - Proceed
After ID Entry	2	–	ID Number Not in Database
After Hand Placement	1	Green	ID Verified
After Hand Placement	2	Red	ID Not Verified - Try Again
After Hand Placement	1 Long Continuous	Red	ID Refused

Glossary

Address, HandPunch A HandPunch Address is a unique identification number assigned to a HandPunch. Each HandPunch on a network must be assigned a unique address.

AWG American Wire Gauge is a U.S. standard set of wire conductor sizes. The “gauge” refers to the diameter of the wire. The higher the gauge number, the smaller the diameter, the thinner the wire, and the greater the electrical resistance. Thicker, smaller gauge wire carries more current because it has less electrical resistance over a given length. Thicker wire is better for long wire distances.

HandPunch Address See Address, HandPunch

Platen The Platen is the flat surface at the base of the HandPunch, on which a user places his/her hand for enrollment and verification. The platen has guide pins to ensure the user’s fingers are consistently positioned correctly.

Template A Template is a set of data generated for a user. It is made up of the user’s enrollment information and any system configuration parameters that are assigned to the user. The template is stored at each HandPunch and can be stored at the host computer with the Time and Attendance software.

Transaction A Transaction is any kind of event recorded at a HandPunch. Transactions may include In or Out punches, department transfers, and supervisor edits.

Limited Warranty

Schlage Biometrics, Inc. (the “Company”) warrants to the original user the products manufactured by the Company (the “Product”) to be free of defects in material and workmanship for a period of three months from the date of purchase by such user or six months from the date of shipment from the factory, whichever is sooner, provided:

1. The Company has been notified within such period by return of any alleged defective product, free and clear of all liens and encumbrances, to the Company or its authorized dealer, transportation prepaid; and
2. The Product has not been abused, misused, or improperly maintained and/or repaired during such period; and
3. Such defect has not been caused by ordinary wear and tear; and
4. Such defect is not the result of voltage surges/brownouts, lightning, water damage/ flooding, fire, explosion, earthquakes, tornadoes, acts of aggression/war, or similar phenomenon; and
5. Accessories used as integral to the Product have been approved by the Company.

The Company shall, at its option, either repair or replace, free of charge, the Product found, upon the Company’s inspection, to be so defective, or if agreed upon, refund the purchase price, less a reasonable allowance for depreciation, in exchange for the Product.

THE COMPANY MAKES NO OTHER WARRANTY AND ALL IMPLIED WARRANTIES INCLUDING ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE ARE LIMITED TO THE DURATION OF THE EXPRESSED WARRANTY PERIOD AS SET FORTH ABOVE.

THE COMPANY’S MAXIMUM LIABILITY THEREUNDER IS LIMITED TO THE PURCHASE PRICE OF THE PRODUCT. IN NO EVENT SHALL THE COMPANY BE LIABLE FOR ANY CONSEQUENTIAL, INDIRECT, INCIDENTAL, OR SPECIAL DAMAGES OF ANY NATURE ARISING FROM THE SAME OR THE USE OF THE PRODUCT.

Schlage Biometrics Inc. reserves the right to make changes in the design of any of its products without incurring any obligation to make the same change on units previously purchased.

Ingersoll Rand
Security Technologies

Ingersoll Rand's Security Technologies Sector is a leading global provider of products and services that make environments safe, secure, and productive. The Sector's market-leading products include electronic and biometric access control systems; time and attendance and personnel scheduling systems; mechanical locks and portable security, door closures and exit devices, steel doors and frames, architectural hardware and technologies and services for global security markets.

866.861.2480

www.schlage.com www.ingersollrand.com

Schlage
Biometric Solutions
Ingersoll Rand Security Technologies
538 Oakmead Parkway
Sunnyvale, CA 94085
Office: 866-861-2480/512-712-1413 (international)
Fax: 866-303-1794/408-341-4101
E-mail: sbssupport@irco.com

SCHLAGE®

HP-2000

Terminal User's Guide

Ingersoll Rand
Security Technologies

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and, if not installed and used in accordance with the Installation Manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at the user's own expense.

This Class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numerique de la classe A respecte toutes les exigences du Reglemente sure le materiel brouilleur du Canada.

Document Part Number: 70100-6007 – Revision 3.3 – July, 2011

HandPunch is a trademark of Schlage Biometrics, Inc.

The trademarks used in this Manual are the property of the trademark holders. The use of these trademarks in this Manual should not be regarded as infringing upon or affecting the validity of any of these trademarks.

Schlage Biometrics, Inc. reserves the right to change, without notice, product offerings or specifications.

Table of Contents

Introduction

The HandPunch 2000 is a member of the Schlage Biometrics' line of biometric hand geometry Time and Attendance Terminals[1]. The HandPunch records and stores the three-dimensional shape of the human hand for comparison and identity verification. Upon verification, the HandPunch records the time, date, user ID number, and collected time and attendance data for collection by a host computer. The HandPunch can communicate with a host computer.

The HandPunch provides proof-positive employee identification combined with the sophisticated operating features one expects in a modern Time and Attendance Terminal. Because of this unique combination of capabilities, the HandPunch provides the most accurate Time and Attendance data collection terminal available. The key features of the HandPunch include:

- Two programmable Function Keys
- Transaction Buffer
  - 5,120 event capacity
- Programmable Clock and Date Formats and Daylight Savings Switch-over

Biometrics

Biometrics is a term describing the automatic measurement and comparison of human characteristics. While its origins are ancient, the evolution of advanced scanning and microprocessor technology brought biometrics into everyday life. Electronic hand geometry technology first appeared in the 1970s. Schlage Biometrics Inc., founded in 1986, built the first mass-produced hand geometry readers and made biometric technology affordable for the commercial market. Today, Schlage Biometrics' products are in use in every imaginable application from protecting cash vaults to verifying employee attendance in hospitals.

[1] For the sake of using a consistent name throughout the manual, the HandPunch 2000 terminal is referred to as the HandPunch for the remainder of this manual.

Principle of Operation

The HandPunch uses low-level infrared light, optics, and a CMOS (IC chip) camera to capture a three-dimensional image of the hand. Using advanced microprocessor technology, the HandPunch converts the image to an electronic template. It stores the template in a database with the user's ID number.

To gain punch, the user enters his or her ID number at the HandPunch's keypad or uses an external card reader. The HandPunch prompts the user to place his or her hand on the HandPunch's platen[2]. The HandPunch compares the hand on the platen with the user's unique template. If the images match, the HandPunch records the transaction for processing.

The HandPunch Terminal

The HandPunch is a time and attendance terminal designed for use with time and attendance software. Refer to Figure 1-1 on page page 5 when reviewing the information in this section.

The HandPunch has an integrated keypad for ID entry (see "Figure 1-1"). The CLEAR and ENTER keys are used for data entry and programming.

Four different features assist the user with hand placement and read verification.

1. A light emitting diode (LED) hand placement display on the HandPunch's top panel assists users with hand placement on the platen.
2. A liquid crystal display (LCD) shows operational data and programming menus.
3. "Red light/Green light" verification LEDs quickly inform users if their verification attempts were rejected or accepted.
4. An internal beeper provides audible feedback during keypad data entry and user verification.

[2] The Platen is the flat surface at the base of the HandPunch (see "Figure 1-1"). This is where users place their hands for enrollment and verification. It has guide pins to assist positioning the fingers during use.

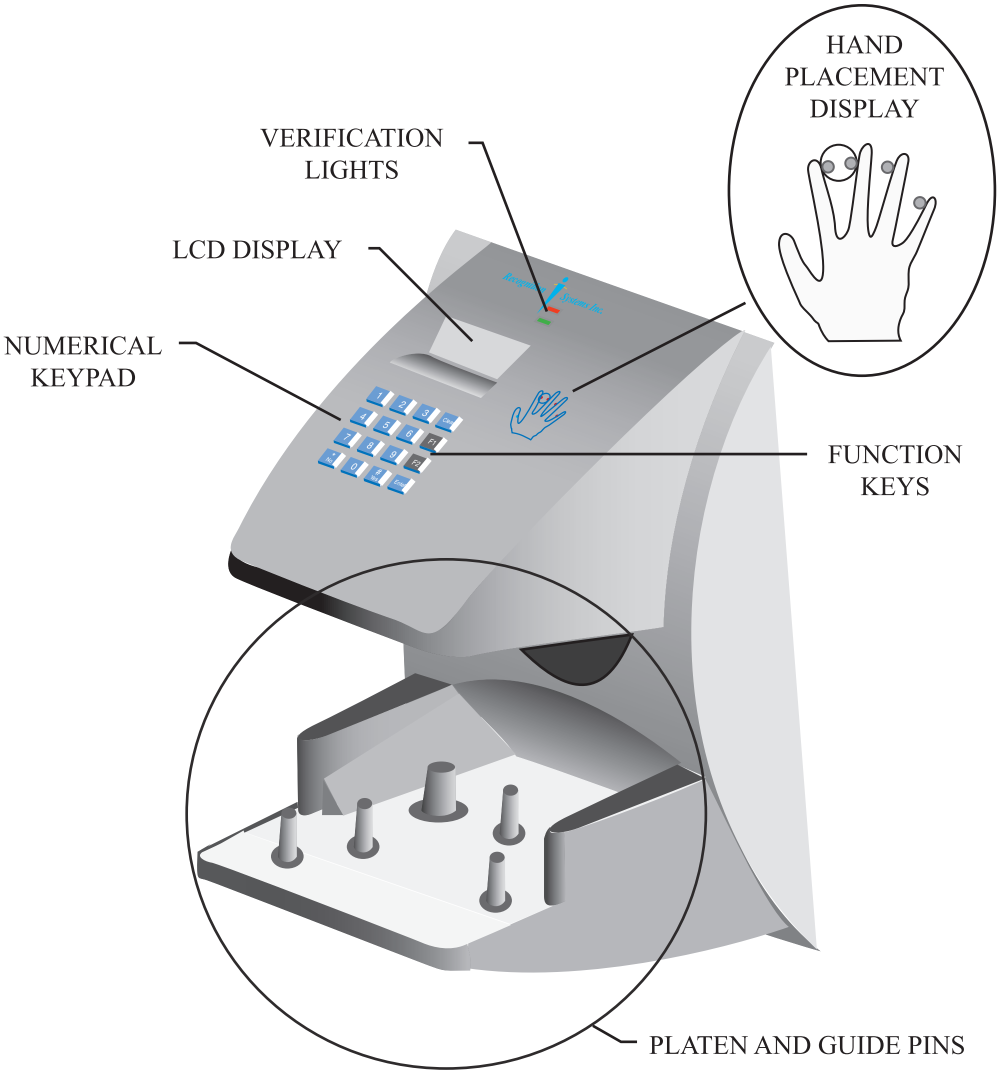


Figure 1-1: The HandPunch 2000

Specifications

Table 1: Specifications

Size:	8.85 inches wide by 11.65 inches high by 8.55 inches deep 22.3 cm wide by 29.6 cm high by 21.7 cm deep
Power:	12 to 24 VDC or 12 to 24 VAC 50-60 Hz, 7 watts
Weight:	6 lbs (2.7 kg) – 7 lbs (3.2 kg) with optional backup battery
Temperature:	-10°C to +60°C – non-operating/storage (14°F to 140°F) 5°C to 40°C – operating (40°F to 110°F)
Relative Humidity Non-Condensing:	5% to 95% – non-operating/storage (non-condensing) 20% to 80% – operating
Verification Time:	1 second or less
Memory Retention:	5 years using a standard internal lithium battery
Transaction Buffer:	5,120 transactions
ID Number Length:	1 to 10 digits
Baud Rate:	300 to 28.8 K bps
Communications:	RS-232, optional Modem
User Capacity:	512 users
Function Keys	2 User Definable

Options

The HandPunch has the following options available.

• Backup Battery Support	See Technical Note 70200-0012 rev C
• Modem Communication	See Technical Note 70200-0013 rev C

UL Compliance

Hand Readers are UL Listed as stand alone units only (i.e. the card reader function has not been evaluated by UL).

The HandKey II has not been tested for UL 294 in an Outdoor configuration.

CE approved

recyclable

This page is intentionally blank.

Planning an Installation

Site Preparation

Before you begin installation, check the site blueprints, riser diagrams, and specifications for important information about HandPunch location and for other systems that connect to the HandPunch. Look for any existing wall preparations and wiring that other contractors may have installed for the HandPunch. A wire routing layout diagram (see Figure 3-2 on page page 15) is provided to assist in planning wire routing.

HandPunch Placement

The recommended height for the HandPunch platen is 40 inches (102 cm) from the finished floor. The HandPunch should be out of the path of pedestrian and vehicular traffic, and convenient to the door it is controlling. Avoid placing the HandPunch where users must cross the swing path of the door. The HandPunch should be in an area where it is not exposed to excessive airborne dust, direct sunlight, water, or chemicals.

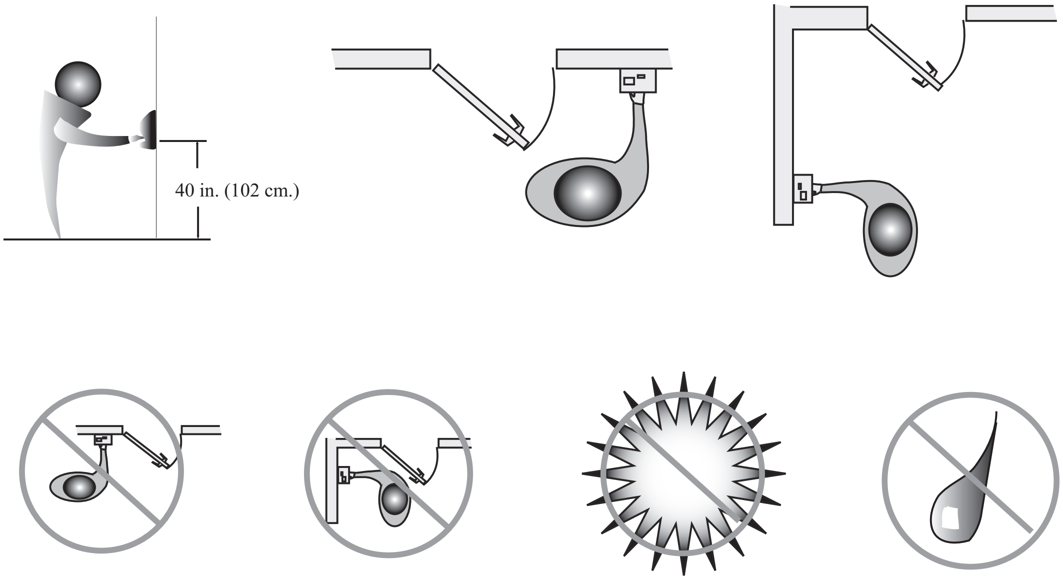


Figure 2-1: HandPunch Placement Rules

NOTE *For the following sections, Schlage Biometrics does not supply hardware items such as power or communications wiring.*

Wiring

Two basic circuits typically connect to the HandPunch:

- Power Input
- HandPunch to Host Computer
  - RS-232
  - modem

The minimum wire size for these circuits is AWG 22; the maximum is AWG 18.

Power Input

The HandPunch uses an internal switching regulator to obtain internal operational power. It accepts input voltages from 12 to 24 VDC or 12 to 24 VAC at 50 to 60 Hz. The HandPunch comes with a 120 VAC to 13.5 VDC power supply (Class 2, Model No. P48131000A010G – 120 VAC, 60 Hz, 21 W, 13.5 VDC output @ 1000mA). An optional 220 VAC to 13.5 VDC power supply is also available.

To power the HandPunch with this power supply, a 120 VAC (or 220 VAC as applicable) duplex outlet must be within 5 feet of the HandPunch. The power supply has a 6-foot cable to provide a comfortable reach between power outlet and HandPunch. The barrel jack at the end of the power supply's cable is connected to J12 on the HandPunch PCB.

!NOTE *Do not connect a HandPunch's power supply to a switched duplex outlet. The HandPunch must have a constant source of power for proper operation.*

Battery Backup Operation

An optional power-fail protection circuit board can be attached to the main circuit board to provide and control battery backup. The battery backup option uses a 12 volt 800 ma/hour sealed lead acid battery to provide backup battery power. This battery is located immediately inside the rear panel of the HandPunch and plugs into jack J4 on the keypad control circuit board located in the top of the chassis.

The design of the HandPunch's internal power supply is such that any range of the above input voltages may be used and still provide proper battery charge voltage and battery backup operation. Switch-over to battery power is automatic and occurs when the input voltage falls to approximately 10.5 volts. At that time the backup battery charger is disabled to save power, and uninterrupted operation continues on battery power.

When input power is restored, the HandPunch switches off of battery operation and the battery charger is re-enabled to recharge the battery. Battery charge voltage is set at approximately 13.65 volts, and battery charge current is limited to approximately 50 mA. A fully discharged battery requires approximately 12 hours of charge to fully recover.

Additional options installed and specific configurations within the HandPunch make it difficult to predict precisely how long battery support will last, but in general two hours of battery operation can be expected. While operating on battery backup due to loss of main input power, the battery output voltage is constantly monitored by internal circuitry. If the battery voltage reaches approximately 9.5 volts the HandPunch automatically shuts down. This is done to prevent full exhaustion of the battery. A yellow indicator on the top panel illuminates to indicate that the HandPunch is running on battery power. This indicator turns off when main input power is restored.

Shunt J7, which is located immediately in front of the DIP switches on the main logic board (see Figure 4-1 on page page 17), enables or disables battery operation on those HandPunches equipped with optional battery backup. If a HandPunch does not have the optional battery backup package installed, J7 is not used. On HandPunches equipped with the battery backup option, J7 allows service personnel a mechanism for disabling battery backup operation before removal of main input power.

To fully power down a HandPunch equipped with battery backup, remove or reposition shunt J7 so that the two pins protruding up from the main logic board are not connected to each other. This effectively opens the circuit, removing the battery from any internal circuitry. Main input power can then be removed and the HandPunch will fully shut down. Once the HandPunch has fully shut down, shunt J7 may be reinstalled.

The design of the power supply is such that main input power must be reapplied to re-enable the battery protection mechanism. If shunt J7 is not properly installed, the internal backup battery will not be charged, and in the event of a main input power loss, the HandPunch will shut down.

HandPunch to Host Computer Connection

HandPunch/host computer communications can be configured in one of two ways:

- via a direct RS-232 connection
- via an optional Modem connection

RS-232 Host Computer Connection

A direct HandPunch connection to a host computer can be made through an 4- conductor cable in an RS-232 serial configuration. A 6’ or 50’ cable may be purchased through RSI or a wiring diagram for the RS-232 to host computer connection is found on Table 2 on page page 18

Modem Host Computer Connection

The HandPunch is also available with an optional modem module for telephone line communications between the HandPunch network and the host computer. When connecting via modem, one HandPunch terminal must be configured with the modem option. This terminal will communicate with the host computer.

To make the modem connection, a telephone jack must be installed on or in the wall behind the modem HandPunch terminal. Position the RJ-11 jack location using the template provided in this manual (see Figure 3-2 on page page 15). The short black cable provided with the modem HandPunch connects the terminal to the telephone jack. Figure 4-4 on page page 19 a wiring diagram for a modem to host computer connection.

Mechanical Installation

Select an installation location based on the guidelines provided in the Planning an Installation section beginning on page page 9.

Wall Plate Installation

Wall Preparation

NOTE *For the following procedure protect the HandPunch from the dust and debris generated during the wall plate installation process.*

1. Remove the wall plate from the packing carton. Refer to Figure 3-1 for all wall plate references in the following section.

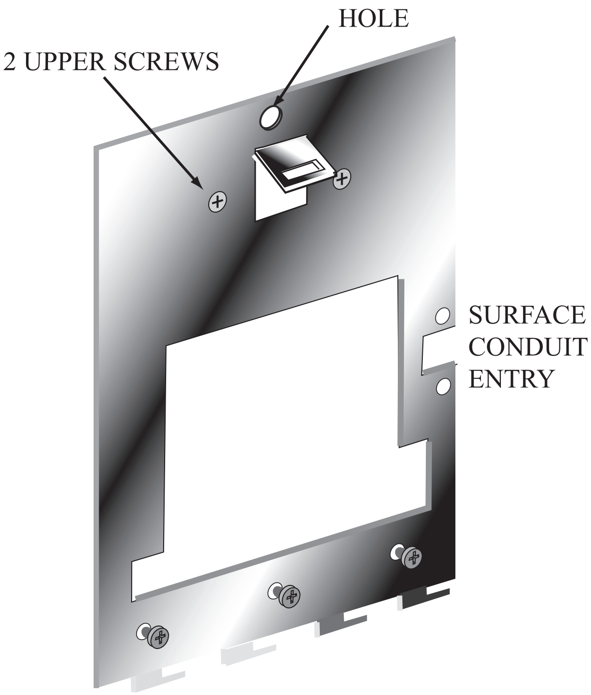


Figure 3-1: Wall Plate

2. Measure and mark a point 48 1/2 inches (123 cm) from the surface of the finished floor. This point will correspond to the Leveling Hole where the top-center point of the HandPunch should be mounted.
3. For a hollow wall, drive a small nail into the wall at the mark and hang the wall plate from the Leveling Hole located near the top of the wall plate.
4. For a solid wall, hold the wall plate against the wall, centering the Leveling Hole over the mark in the wall.

5. Align a bubble level with the top edge of the wall plate and gently rotate the wall plate until the bubble level shows that the top edge of the wall plate is level.
6. Secure the plate to the wall using heavy masking tape.
7. Using the wall plate as a template, mark the locations of the two upper screw holes and the three lower screw holes.
8. For a concealed wiring connection, trace the outline of the open area in the center of the wall plate. Identify and mark a 1/2 inch hole through which the HandPunch's wiring will be mounted.
9. For a surface conduit wiring connection, mark the two conduit clamp holes at the right side of the wall plate.
10. Remove the wall plate, masking tape, and the nail (if used).

Mounting the Wall Plate

1. For a hollow wall, use the provided hardware to mount the wall plate. Use the two auger style fasteners for the upper two mounting holes. Use the toggle bolts for the three lower mounting holes.
2. For a solid wall, use expansion bolts to mount the wall plate. For all five mounting holes, drill a 1/4 inch diameter hole, 1/4 of an inch deeper than the length of the expansion anchor.

Routing the Wire

1. Refer to Figure 3-2 on page page 15 for a template diagram to assist in routing wiring.
2. For a concealed wiring connection, drill a 1/2 inch hole in a convenient location within the open area of the wall plate. Pull the wiring to enter the HandPunch through this hole in the open area.
3. For a surface conduit wiring connection, drill a 1/4 inch diameter hole, 1/4 of an inch deeper than the length of the expansion anchor for each of the two conduit clamp holes. Route 1/2 inch, flexible conduit to the HandPunch, ending the conduit between the two conduit clamp holes. Pull the wiring to enter the HandPunch through the conduit. Pull 18 inches of wire past the end of the conduit to allow enough space for final connection to the HandPunch.
4. Clear all dust and debris away from the HandPunch mounting location.

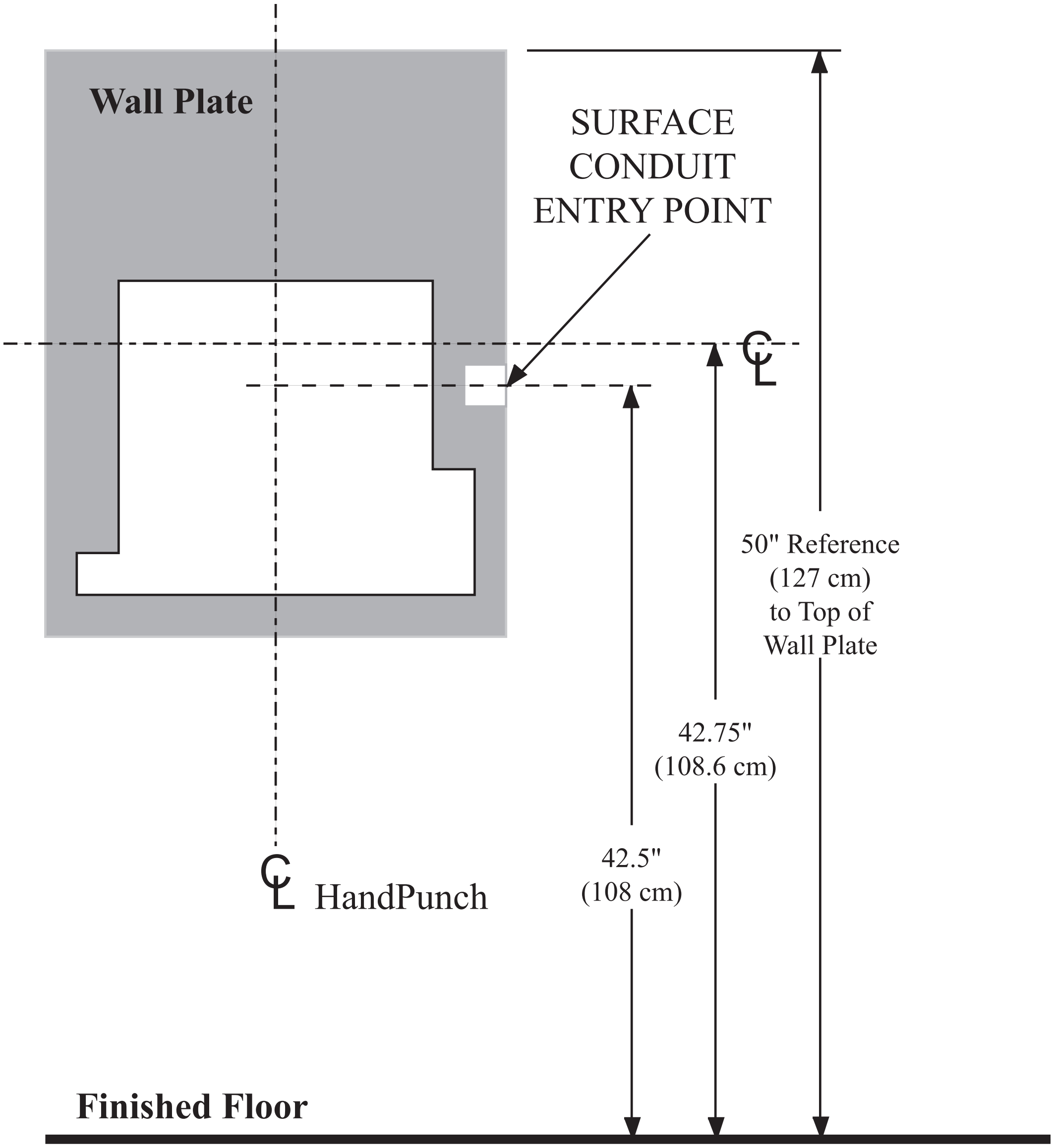

Wall Plate
SURFACE CONDUIT ENTRY POINT
CL
50" Reference (127 cm) to Top of Wall Plate
42.75" (108.6 cm)
42.5" (108 cm)
CL HandPunch
Finished Floor

Figure 3-2: HandPunch Wire Routing Layout

NOTE *Dust and debris surrounding the HandPunch can drastically affect the terminal's operation. It is important to ensure the HandPunch mounting location is free from dust and debris.*

Attaching the HandPunch

1. Remove the HandPunch from its carton.
2. Align the sleeves of the back plate with the pins of the wall plate and slide the HandPunch to the left as shown in "Figure 3-3".

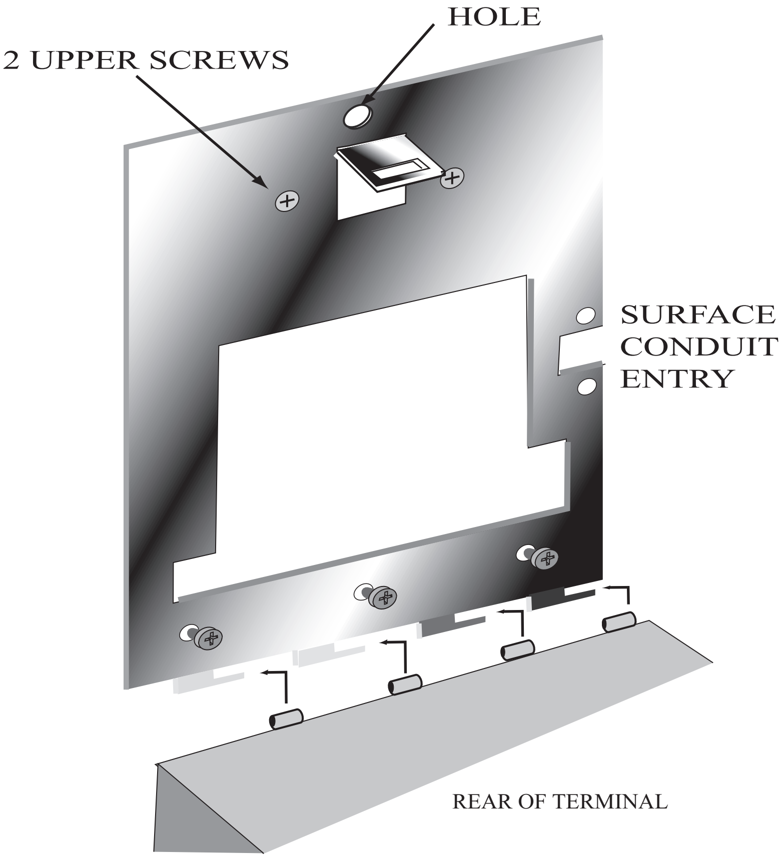


Figure 3-3: Attaching the HandPunch to the Wall Plate

Wiring Connections

Once the HandPunch is attached to the wall plate the wiring connections to the HandPunch can be made (see Figure 4-1).

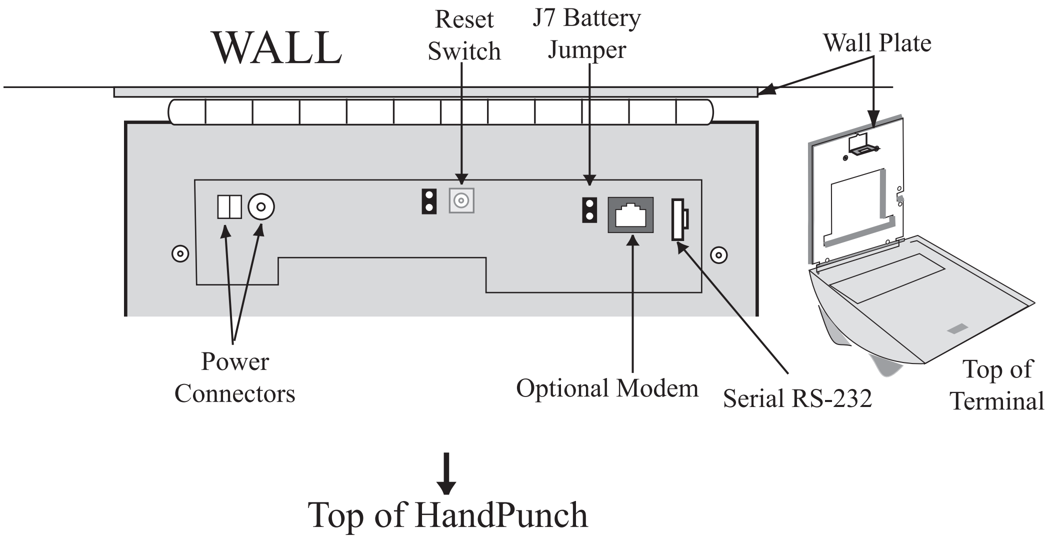


Figure 4-1: Board Layout

Wiring Examples

Table 2 on page page 18 provides the pinouts for the RS-232 Serial Host Computer Connection.

Figure 4-2 on page page 18 provides a diagram of the RS-232 Connector.

Figure 4-3 on page page 19 provides a Serial Connection diagram

Figure 4-4 on page page 19 provides a Host PC to HandPunch Modem Network wiring diagram (Modem wiring is a HandPunch option).

Table 2: RS-232 Serial Connection

J8 Pin	Signal	Connection
1	GND	Ground
2	RXD	Receive Data Input (from external device)
3	TXD	Transmit Data Output (to external device)
4	RTS	Ready to Send Output (to external device)

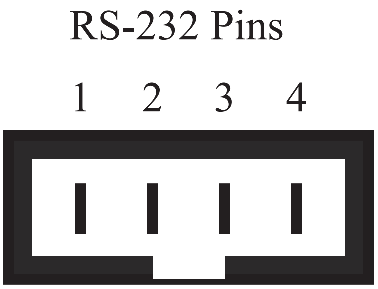


Figure 4-2: J4 - RS-232 Jack Pinout

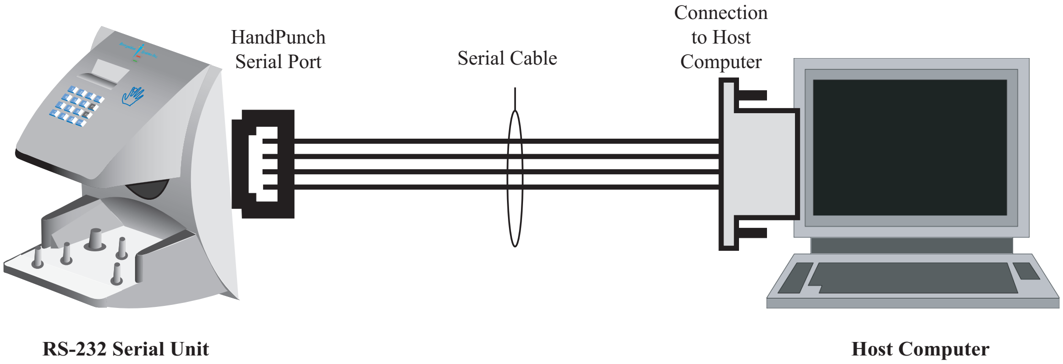


Figure 4-3: Host PC to RS-232 Connection

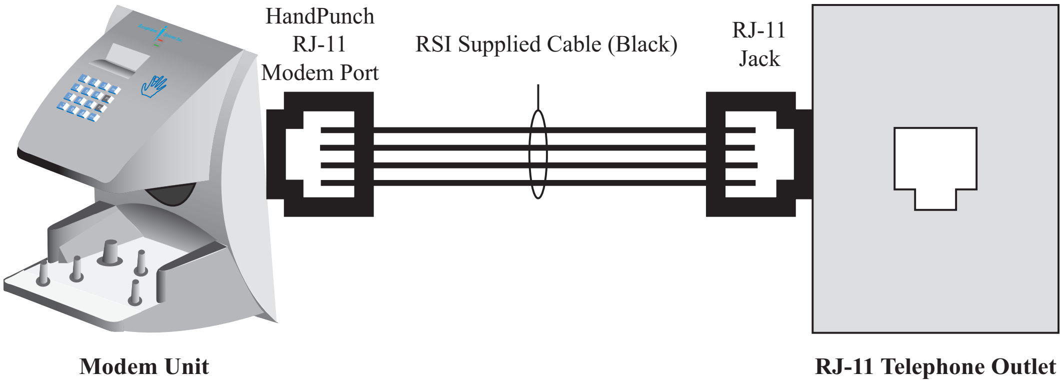


Figure 4-4: Host PC to HandPunch Modem Connection

Erasing the Memory

There are two options when erasing the memory of the HandPunch.

1. Setup
2. All

The erasing of the setup will set the HandPunch's address, passwords, etc. back to factory defaults.

Choosing the All option will take the HandPunch's setup back to factory defaults plus erase all user databases and datalogs. This action can not be undone. If there is a software that is managing the system then the users can be downloaded back to the HandPunch if needed.

Erasing HandPunch Memory

The erase memory function allows a HandPunch's setup and/or user database to be erased.

Perform the following steps to erase the setup programs but retain the user database.

1. With system power OFF, depress reset switch.
2. Turn system power ON and wait 5 seconds.
3. LCD screen will display

```
ERASE                  :1 SETUP
                       :9 ALL!!!
```

Closing the HandPunch

Before closing the HandPunch clear all dust and debris away from the HandPunch. With the wall mount latch in the unlocked position, swing the body of the HandPunch up and lock the latch into place with the key provided with the HandPunch (see Figure 6-1).

NOTE *Dust and debris surrounding the HandPunch can drastically affect the terminal's operation. It is important to ensure the HandPunch is free from dust and debris before closing the terminal.*

NOTE *Do not force the HandPunch onto the wall mount latch when the latch is in the locked position.*

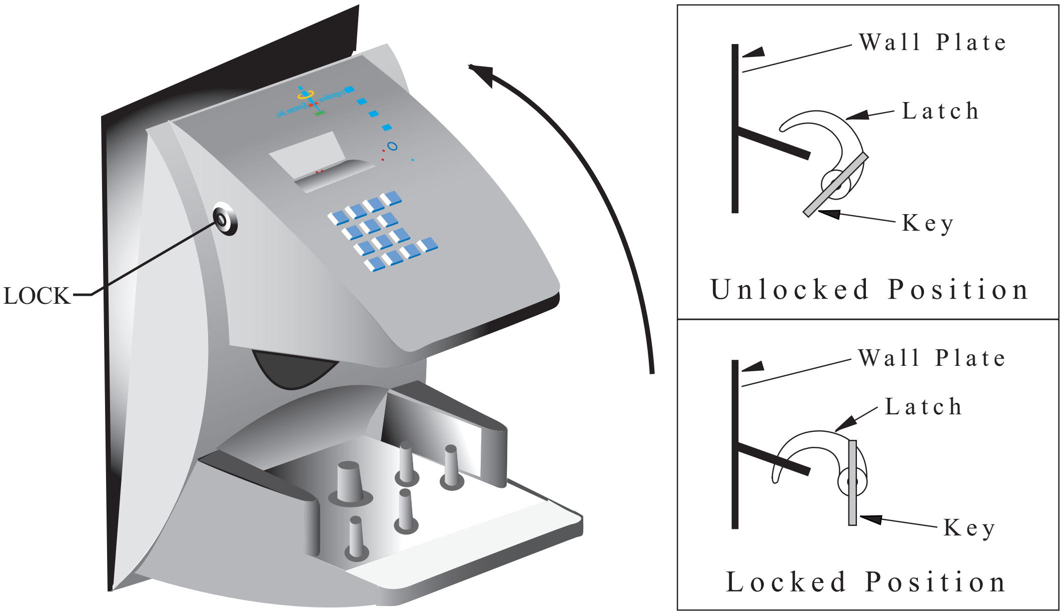


Figure 6-1: Closing the Handpunch

Enter Command Menu

Press the CLEAR and ENTER keys simultaneously to enter a command menu.

If No One is Enrolled in the HandPunch

1. The display appears as follows.

```
ENTER PASSWORD
```

2. Press the default password for the menu you wish to enter.

Press 1 for the Service Menu.

Press 2 for the Setup Menu.

Press 3 for the Management Menu.

Press 4 for the Enrollment Menu.

Press 5 for the Security Menu.

3. Press ENTER and the first command option in the selected menu appears.

If Users are Enrolled in the HandPunch

1. The display appears as follows.

```
ENTER ID
  *:
```

2. Enter your ID number on the keypad and place your hand on the platen for verification.
3. If verification is successful, the display appears as follows.

```
ENTER PASSWORD
```

4. Enter the password for the menu you wish to enter. The default passwords are as follows.

Press 1 for the Service Menu.

Press 2 for the Setup Menu.

Press 3 for the Management Menu.

Press 4 for the Enrollment Menu.

Press 5 for the Security Menu.

5. Press ENTER
6. If you are authorized to use this command the first command option in the selected menu appears.
7. If you are not authorized to enter this command the display appears as follows.

```
ENTER
*:
```

NOTE *To access these menus you must be the first person enrolled in a new system installation or you must have been enrolled as a supervisor. If you are blocked from the supervisory menus, verify your access rights with management personnel. If enrollment information has been incorrectly changed and you must have supervisory access to all menus, make these changes through software.*

NOTE *It is possible to physically reset the HandPunch's memory, however resetting memory sets all unit parameters back to the factory default values. Resetting memory allows access to all menus by the first person enrolled (as if it is a new system installation), but this means that all employee information programmed into the HandPunch is lost and must be re-entered manually. Be sure you need to reset memory before performing this function. To reset memory, refer to the Erasing HandPunch Memory section on page page 20.*

Navigating Command Menus

Once you have entered a command menu, there are three options available for navigating the command menu system.

1. Press # to enter the command shown on the display.
2. Press * to step to the next command in the menu.
3. Press CLEAR to exit the command menu (pressing any numeric key also exits the command menu). If you are in a command's sub-menu, you may have to press CLEAR multiple times to completely exit the command menu.

This page is intentionally blank

Programming the HandPunch

The HandPunch is programmed via a series of command menus. A summary of the menus and commands is given in Table 3.

Table 3: Basic Command Mode Structure

Service Menu	Setup Menu	Management Menu	Enrollment Menu	Security Menu
Password 1	Password 2	Password 3	Password 4	Password 5
Calibrate	Set Language	List Users	Add Employee	Special Enroll
Status Display	Set Date Format	Set User Data	Add Supervisor	
	Set Time and Date		Remove User	
	Set Address			
	Set ID Length			
	Set Serial			
	Upgrade			

To control access to the command menus, each menu has a unique password. This password is requested as a part of the process for accessing each menu. A supervisor must enter the correct password for that menu to access that menu. The default menu passwords are given in Table 3.

To increase the security of the HandPunch, Schlage Biometrics recommends changing the passwords for the command menus to new numbers. These password numbers can be up to 10 digits long. This is done with the Set Passwords command described on ?.

Autority Level

A second method for controlling access to the command menus is through the use of Authority Levels. Authority Levels control whether or not a user has access to the command menus.

- Level 0 is for a user who does not need access to any of the command menus.
- Level 5 is assigned to Supervisors who need access to all of the command menus.

The HandPunch automatically assigns Authority Level 0 to users enrolled by the Add Employee command. Authority Level 5 is automatically assigned to users enrolled by the Add Supervisor command.

NOTE *Until a user has been assigned to Supervisor, every user can access every menu. Once a user has been enrolled using the Add Supervisor (designated as a supervisor), all further user authority levels are assigned. The first person enrolled should be enrolled using the Add Supervisor command. This protects the integrity of the system. Schlage Biometrics strongly recommends enrolling at least two users as supervisors to ensure that more than one person has the authority to access all menus and all commands.*

Programming Order

When setting up HandPunch operations there is a general programming/operations order that should be followed.

Set HandPunch Site Parameters – Set the HandPunch site parameters to meet site-specific needs and usage: change the language used by the display, set the HandPunch’s address, and set the serial communication baud rate (used if you have installed a serial printer – see page page 30).

Enroll Supervisory Staff – Enroll yourself and the supervisors who will have responsibility for HandPunch management. This is done through the Enrollment Menu (see Supervisor Enrollment on page page 39).

NOTE *The time, date, and ID number length are normally set by the host computer. However, a supervisor can change these parameters at a HandPunch after setup information has been downloaded from the host computer.*

These tasks are done through the Setup Menu. The instructions for reader setup parameters begin on page page 30.

Train and Enroll Users – Train each user regarding HandPunch usage and then Enroll each user. This is done through the Enrollment Menu. The instructions for employee enrollment begin on page page 39. Special enrollment allows you to enroll people with disabilities that prevent them from using the HandPunch properly. Employees with special enrollment ID numbers can punch in without biometric verification.

NOTE *This means that anyone who knows a special enrollment ID number can punch in. This function should only be used if absolutely necessary. The instructions for special enrollment begin on page page 40.*

System Management

Once a HandPunch system is in operation the following commands are used for system management.

List Users – List the Users authorized to use a HandPunch. This is done through the Management Menu. The instructions for listing employees begin on page page 35.

Set User Data – Set a user's reject threshold (adjusting the sensitivity applied when a HandPunch reads a hand) this task is done through the Management Menu. The instructions for setting user data begin on page page 35.

Remove User – Remove employees (and supervisors) from a HandPunch. This is done through the Enrollment Menu. The instructions for removing employees begin on page page 39

Service Menu

The Service menu commands provide information that help you determine if the HandPunch is performing within normal operating parameters and identify the status of the unit's inputs and outputs. The following section provides a brief summary of the Service Menu commands.

NOTE *There are no user serviceable parts inside the HandPunch.*

Navigating the Service Command Menu

Enter the appropriate password to enter the Service command menu. Once you have entered the command menu, there are three options available for navigating the command menu system.

- Press # to enter the command shown on the display.
- Press * to step to the next command in the menu.
- Press CLEAR to exit the command menu (pressing any numeric key also exits the command menu). If you are in a command's sub-menu, press CLEAR multiple times to completely exit the command menu.

Service Commands

There are two commands available from the Service command menu.

- Calibrate
- Status Display

Refer to Table 4 and identify the command you need to perform. Step through all previous commands until you reach the desired command.

Table 4: Service Command Menu

Service Menu
Password = 1
Calibrate
Recal (Y/N)
Status Display
On/Off (Y/N)

Calibrate

The Calibrate command displays the HandPunch’s exposure values, allowing you to verify these values are within normal operating parameters. The standard operating parameters are shown in Table 5

.

Table 5: Normal Operating Parameters

Parameter	Normal Range
Row “r”	0 +/- 2
Column “c”	0 +/- 2
Exposure “e”	100 +/- 20

Status Display

The status display command allow you to enable or disable the displaying of the following information.

- the status values of HandPunch inputs and outputs
- the hand read score of the last user to verify on the system

When the status display is enabled, Figure 8-1 identifies each status display field value

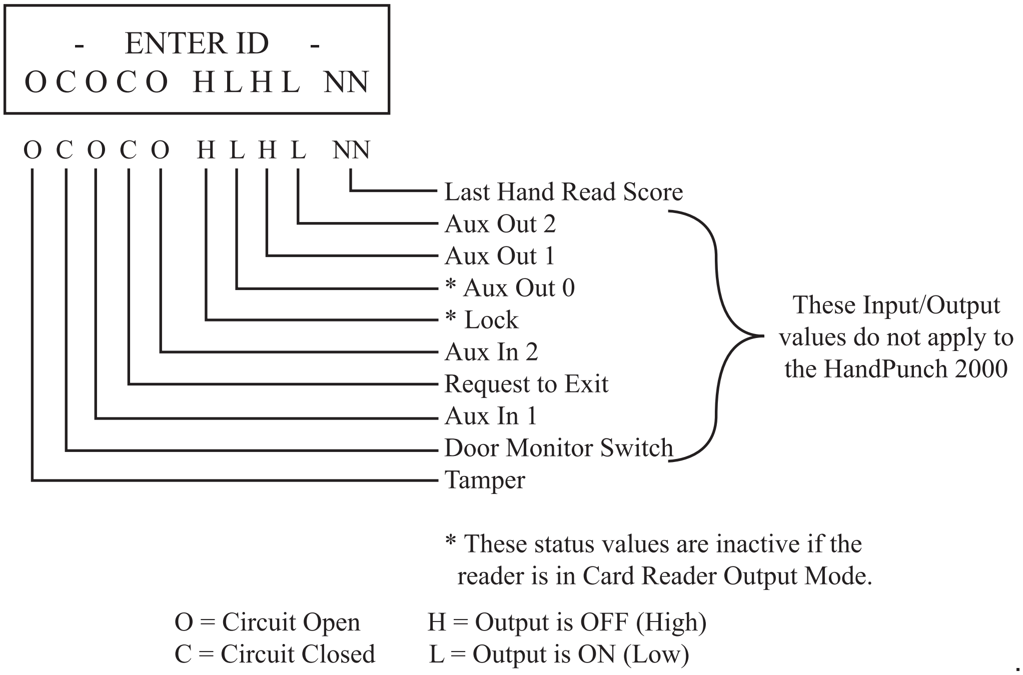


Figure 8-1: Status Display Chart

Setup Menu

The Setup menu commands allow you to set the basic operating parameters for the HandPunch unit. The following section provides a brief summary of all the parameters that may be set on a HandPunch unit.

!NOTE *Once in the Command Menu, you can step through and set the parameters for each command sequentially. You do not have to exit command mode after setting any individual command.*

Navigating the Setup Command Menu

Enter the appropriate password to enter the Setup command menu. Once you have entered the command menu, there are three options available for navigating the command menu system.

- Press # to enter the command shown on the display.
- Press * to step to the next command in the menu.
- Press CLEAR to exit the command menu (pressing any numeric key also exits the command menu). If you are in a command's sub-menu, press CLEAR multiple times to completely exit the command menu.

Setup Commands

There are six commands available from the Setup command menu.

- Set Language
- Set Date Format
- Set Date and Time
- Set Address
- Set ID Length
- Set Serial

Refer to Table 6 on page page 32 and identify the command you need to perform. Step through all previous commands until you reach the desired command.

Table 6: Setup Command Menu

Setup Menu
Password = 2
Set Language
Select Language
Set Date Format
Select Date Format
Set Time and Date
Month (MM)
Day (DD)
Year (YY)
Hour (HH)
Minute (MM)
Set Address
New Address
Set ID Length
New ID Length
Set T & A Mode
Set Serial
RS-232
Select Baud Rate
Upgrade
Code

Set Language

The Set Language command allows the language shown on the HandPunch's display to be "localized" for a variety of countries.

- English
- Japanese
- French
- Italian
- Spanish
- German
- Russian
- Indonesian
- Portuguese
- Polish

Set Date Format

The Set Date Format command allows the date format shown on the HandPunch's display to be "localized" for a variety of countries.

mm/dd/yy

dd-MMM-yy

dd-mm-yy

dd/mm/yy

-mm-dd-yy

-MMM dd,yy

-ddMMMyyyy

Set Time and Date

The Set Time and Date command allows the HandPunch's time and date to be set. This is normally not necessary as the HandPunch's time and date are set by the host computer.

Set Address

The Set Address command allows a unique address to be set for each HandPunch in a network. For proper operation, each HandPunch in the network must have a unique address. All units may use any address from 0 to 254. All units are sent with the address set to 1.

Set ID Length

The Set ID Length command allows you to reduce the number of keystrokes required to enter the ID number by eliminating the use of the ENTER key to complete an ID number entry. Once the ID Length is set, the HandPunch will automatically accept an ID number entry once the correct number of characters have been entered.

Set ID Length does not apply when ID entry is made from a card reader. Once the ID Length is set, the T & A Mode Set command appears, allowing you to configure the HandPunch to prepare punch data for time and attendance software.

Set Serial

The Set Serial command allows you to set the baud rate communication parameters.

Upgrade

This Upgrade Menu is where the HandPunch code gets input to allow for a Memory Upgrade

Management Menu

The Management menu commands allow you to manage employee data stored in a HandPunch unit. The following section provides a brief summary of the employee data that may be manipulated on a HandPunch unit.

Navigating the Setup Command Menu

Enter the appropriate password to enter the Setup command menu. Once you have entered the command menu, there are three options available for navigating the command menu system.

- Press # to enter the command shown on the display.
- Press * to step to the next command in the menu.
- Press CLEAR to exit the command menu (pressing any numeric key also exits the command menu). If you are in a command's sub-menu, press CLEAR multiple times to completely exit the command menu.

Management Commands

There are four commands available from the Management command menu.

- List Users
- Set User Data

Refer to Table 7 and identify the command you need to perform. Step through all previous commands until you reach the desired command.

Table 7: Setup Command Menu

Setup Menu
Password = 3
List Users
Display
Print
Set User Data
User Reject

List Users

The List Users command allows you to display or print a list of all the employees enrolled in a HandPunch.

Set User Data

The Set User Data command allows you to set an employee's Reject Threshold, adjusting the hand read threshold for one employee without affecting the threshold of other employees. This task should be done through your user software, however it can be done through the Management Menu.

Enrollment Menu

Enrollment is the process of recording a hand image and associating it with an ID number. The first person to enroll in the HandPunch has access to all command menus. This person should enroll using the Add Supervisor command (see page page 39). Once a supervisor has been enrolled, all further enrollments use the following rules:

- A user enrolled through the Add Employee command (page page 39) is assigned Authority Level 0. This allows the user to punch in and/or gain access through a door secured by the HandPunch.
- A user enrolled through the Add Supervisor command (see page page 39) is assigned Authority Level 5. This allows the supervisor to punch in and gain access through a door secured by the HandPunch, and it allows the supervisor to access all command menus.

!NOTE *Until a user has been assigned to Authority Level 5 using the Add Supervisor command, every user with Authority Level 0 can access every menu. This is done to ensure that the first person enrolled is able to access all the menus to perform all the programming required to support the HandPunch. Once a user has been enrolled using the Add Supervisor command, all further user authority levels are assigned as per the list above. This protects the integrity of the system by enacting the Authority Level rules described above. Schlage Biometrics strongly recommends enrolling at least two users as supervisors to ensure that more than one person has the authority to access all menus and all commands.*

Advance planning and training make enrollment fast and easy. Users should be informed on what to expect and how to place their hands on the HandPunch before you enroll them.

Navigating the Setup Command Menu

Enter the appropriate password to enter the Setup command menu. Once you have entered the command menu, there are three options available for navigating the command menu system.

- Press # to enter the command shown on the display.
- Press * to step to the next command in the menu.
- Press CLEAR to exit the command menu (pressing any numeric key also exits the command menu). If you are in a command’s sub-menu, press CLEAR multiple times to completely exit the command menu.

Preparation

Here are a few guidelines to help you prepare for an enrollment session.

- You can enroll one person or a group of people during an enrollment session.
- Each user must have a unique personal identification (ID) number. It will save you considerable time if you assign the ID numbers in advance.
- The HandPunch will not accept two people with the same ID number.
- If you enroll people using the last four digits of their phone numbers or social security numbers, you may get duplicate numbers.
- If you are enrolling large groups of people you may consider using an enrollment trainer. It is a replica of a platen that is available through your Schlage Biometrics reseller.

User Education

The HandPunch is easy to use and non-threatening. However, most people have never used a biometric HandPunch. Training users on how the HandPunch works and how to use it will eliminate most fears and concerns before they occur. Inform the users of these facts.

- The HandPunch reads the shape of the hand, not the fingerprints or palmprints.
- It does not identify people. It confirms people's identity.
- It scans with an invisible light of the type used in TV remote controls.
- It does not transfer germs any more than a doorknob or money.
- It does not invade privacy; it guarantees it.
- The enrollment process requires three or more reads to collect enough information to create a template.

Proper Hand Placement

For correct, consistent hand reads it is very important that your hand is placed on the platen in the same manner every time. The following rules apply for proper hand placement on the platen also refer to Figure 8-2 below.

- If you are wearing a ring, rotate the ring so the stone faces up in its normal position.
- Slide your right hand onto the platen rather like an airplane landing at the airport.
- Slide your hand forward until the web between your index and middle finger stops against the Web Pin.
- Keep your hand flat. You should feel the surface of the platen on your palm and the underside of your fingers.
- Close your fingers together until they touch the Finger Pins and watch the hand diagram light display on the top panel.
- The lights go out when you have properly placed your fingers. If a light remains on, a finger is not in proper contact with its Finger Pin.

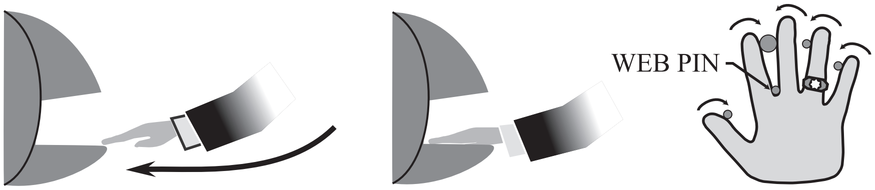


Figure 8-2: Placing Your Hand on the Platen

Left Hand Enrollment

Some right hands cannot be used in the HandPunch due to disabilities such as missing fingers. You can enroll a user with the left hand facing palm side up. The techniques for left hand enrollment are the same as for standard enrollment. The user should keep the back of the hand flat against the platen and move the fingers against the web pin and the finger pins in the same manner as in standard enrollment. Users enrolled with the left hand must always verify with the left hand. Extra practice on placing the hand on the platen may be required to ensure correct, consistent hand reads.

Read Score

When a user uses the HandPunch the display appears as follows.

```
      OKAY (USER ID)
SCORE IS: (SCORE NUMBER)
```

The score number on the display reflects how accurately the user's hand is placed on the platen. Scores that vary greatly between low and high numbers are indicative of inconsistent hand placement. Scores above 50 are indicative of improper hand placement or of a drastic change in the physical appearance of the hand.

When this occurs, emphasize the importance of sliding the hand onto the platen and keeping the hand flat. Re-training and practice should lower a user's score. It might be necessary to change a user's reject threshold if the user has a mild disability. Re-enrollment might be necessary to create a new user template.

Enrollment Commands

There are three commands available from the Enrollment command menu.

- Add Employee
- Add Supervisor
- Remove User

Refer to “Table 12” to identify the command you need to perform. Step through all previous commands until you reach the desired command.

Table 8: Enrollment Command Menu

Service Menu
Password = 4
Add Employee
ID #
Add Supervisor
ID
Remove User
ID

Add Employee

The Add Employee command allows you to enroll a new employee into the HandPunch.

Add Supervisor

The Add Supervisor command allows you to enroll a new supervisor into the HandPunch.

Remove User

The Remove User command allows you to remove an employee or supervisor from the HandPunch.

Special Menu

The Special menu has one command – Special Enroll. This command accommodates users with disabilities that make it difficult or impossible to use a HandPunch in its standard way. The following section provides a brief description of the Special Menu command.

Navigating the Special Command Menu

Enter the appropriate password to enter the Special command menu. Once you have entered the command menu, there are three options available for navigating the command menu system.

- Press # to enter the command shown on the display.
- Press * to step to the next command in the menu.
- Press CLEAR to exit the command menu (pressing any numeric key also exits the command menu). If you are in a command's sub-menu, press CLEAR multiple times to completely exit the command menu.

Special Command

There is one command available from the Special command menu.

- Special Enroll

Refer to Table 9 and identify the command you need to perform. Step through all previous commands until you reach the desired command.

Table 9: Special Command Menu

Special Menu
Password = 5
Special Enroll
ID
On/Off (Y/N)

Special Enroll

The Special Enroll command allows a user to be enrolled such that the ID number is the primary criteria for determining access. A hand read is required, but is not verified against any stored identification data. A time zone value can be applied to the Special Enrollment ID number to limit access times. The HandPunch default is for no time zone to be applied.

NOTE *Special Enrollment affects the integrity of the HandPunch terminal and should only be used as a last resort. Anyone who knows a Special Enroll ID number is granted access when the ID number is used. Before specially enrolling a user, try to alleviate verification problems by adjusting the individual user's reject threshold (see page page 38) or by using left hand enrollment (see page page 38).*

This page intentionally left blank

HandPunch Maintenance

A minimum amount of system maintenance is required to keep HandPunchs fully functional. HandPunchs should be cleaned periodically to prevent an accumulation of dust from affecting the HandPunch's readability. User Scores should be reviewed periodically to ensure the HandPunch is performing properly.

NOTE *There are NO user serviceable parts inside the HandPunch.*

Once a HandPunch system is in operation there are two HandPunch commands that can assist with system maintenance. These commands are performed through the Service Menu. The instructions for these commands begin on page page 29.

- Calibrate – View HandPunch exposure values.
- Status Display – Display HandPunch input/output status, the hand read score of the last user to verify on the system.

Cleaning the HandPunch

Inspect and clean the HandPunch regularly to maintain optimum performance. Clean the platen, side mirror, reflector, and the window above the platen using a clean cloth dampened with ordinary, non-abrasive window cleaner (see Figure 9-1). Start at the rear corners of the platen and work your way forward.

NOTE *DO NOT SPRAY CLEANING FLUID DIRECTLY INTO OR ON THE HandPunch.*

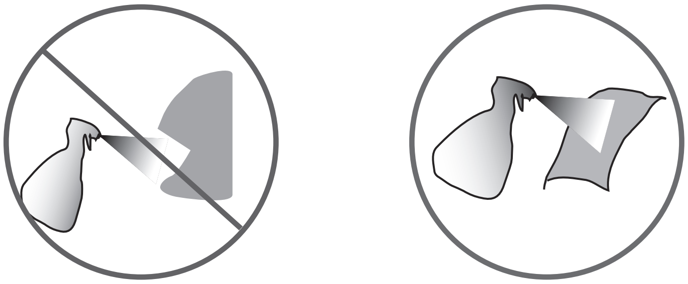


Figure 9-1: HandPunch Cleaning

User Score

Periodically check users' scores (refer to the Read Score section on page page 38). Scores should average under 30. Occasionally a user will score above 30. This is not necessarily an indication of poor performance. If a number of scores average over 30, clean the HandPunch and check scores again. If scores remain high, or if users are experiencing frequent rejections, run the Calibration command (see page page 30).

Appendix A

Tips for a successful Installation

HandPunch

- Think of the HandPunch as a camera
- Clean the HandPunch before it gets dirty
- Use non-abrasive cleaners such as glass cleaners and non-abrasive and clean cloths
- Make cleaning the HandPunch part of Janitorial program
- Do not remove the foam backing from the wall mounting plate
- Seal any holes made in the wall for wire routing, so that dust will not blow into the HandPunch

Location

- Mount all HandPunchs in a network so that the top of the platen is 40” off of the floor
- If an enrollment HandPunch is used make sure that it is placed with the top platen 40” off of the floor and not sitting directly on top of a desk, this will help to eliminate “bad enrollments”
- Mount the HandPunch so that it is not difficult or dangerous to verify then open the door
- It is not recommended to mount the HandPunch in an area where there is airborne dust, in the path of direct sunlight, or where the HandPunch can be exposed to water or corrosive gasses

Enrollment

- Educate the Enrollee on Hand Geometry
- Explain enrollment process
- Train Enrollee on hand placement
  - Practice placing hand on platen
  - Rotate rings to be stone-up
  - Make sure hand is flat on platen
  - Close finger towards the center of hand
- Fingers gently touch finger pins
- Let the enrollee enter in their own ID number during the enrollment process, this forces the Enroller to step aside allowing the Enrollee to stand in front of the HandPunch helping to eliminate “bad enrollments”
- If an enrollment transaction fails:
  - Retrain the user on correct placement and ensure that rings are rotated to be stone-up then
  - Try again to enroll the same hand
  - Try to enroll the other hand (with the hand placed upside-down so the thumb still contacts the thumb-pin on the platen)
- After enrollment, it is a good idea to let the enrollee enter their ID number and practice a verification transaction to ensure that the enrollment was high-quality
- If a user consistently fails during verifications days/months/years later, re-enroll the user to ensure a high quality and up-to-date enrollment record

Appendix B

Noted Board Configuration Differences

Because of Schlage Biometrics' camera retrofit of the HandPunch some changes have been made to the main PCB and they are listed as follows:

- Dipswitches have been removed
  - memory is reset with a push-button reset and user interface with keypad and LCD
- Power has moved to the right side of the PCB
- The RS-232 RJ-45 receptacle has been replaced with a 4 pin Molex connector on the left side of the PCB
- A 2 pin Molex connector (J5) has been added to the board, next to the reset button, to supply power for the LEDs. This connector should never be unplugged. unless a modem or Ethernet is added to the PCB
- The upgrading of the memory is now handled through software codes at the HandPunch. Contact Order Entry for memory upgrades

Memory Reset

To reset the memory of the HandPunch follow these steps-

1. Remove power and battery jumper, if a back up battery is installed
2. Press down on reset button and apply power
3. Release button
4. Reader will boot to

```
ERASE      :1 SETUP
           :9 ALL!!!
```

- Press 1 to erase setup i.e. address, outputs, passwords, but retain user database and datalogs
- Press 9 to erase everything i.e. HandPunch goes back to factory defaults

Appendix C

Mechanical Installation

Select an installation location based on the guidelines provided in the Planning an Installation section beginning on page page 9.

Wall Plate Installation

Wall Preparation

NOTE *For the following procedure protect the HandPunch from the dust and debris generated during the wall plate installation process.*

1. Remove the wall plate from the packing carton. Refer to Figure 12-1 for all wall plate references in the following section.

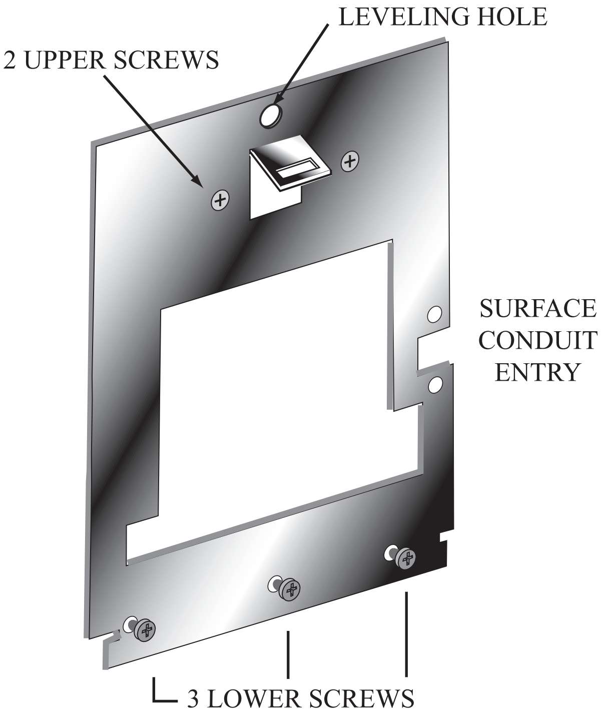


Figure 12-1: Wall Plate

2. Measure and mark a point 48 1/2 inches (123 cm) from the surface of the finished floor. This point will correspond to the Leveling Hole where the top-center point of the HandPunch should be mounted.
3. For a hollow wall, drive a small nail into the wall at the mark and hang the wall plate from the Leveling Hole located near the top of the wall plate.
4. For a solid wall, hold the wall plate against the wall, centering the Leveling Hole over the mark in the wall.

5. Align a bubble level with the top edge of the wall plate and gently rotate the wall plate until the bubble level shows that the top edge of the wall plate is level.
6. Secure the plate to the wall using heavy masking tape.
7. Using the wall plate as a template, mark the locations of the two upper screw holes and the three lower screw holes.
8. For a concealed wiring connection, trace the outline of the open area in the center of the wall plate. Identify and mark a 1/2 inch hole through which the HandPunch's wiring will be mounted.
9. For a surface conduit wiring connection, mark the two conduit clamp holes at the right side of the wall plate.
10. Remove the wall plate, masking tape, and the nail (if used).

Mounting the Wall Plate

1. For a hollow wall, use the provided hardware to mount the wall plate. Use the two auger style fasteners for the upper two mounting holes. Use the toggle bolts for the three lower mounting holes.
2. For a solid wall, use expansion bolts to mount the wall plate. For all five mounting holes, drill a 1/4 inch diameter hole, 1/4 of an inch deeper than the length of the expansion anchor

Routing the Wiring

1. Refer to Figure 12-2 on page page 48 for a template diagram to assist in routing wiring.
2. For a concealed wiring connection, drill a 1/2 inch hole in a convenient location within the open area of the wall plate. Pull the wiring to enter the HandPunch through this hole in the open area.
3. For a surface conduit wiring connection, drill a 1/4 inch diameter hole, 1/4 of an inch deeper than the length of the expansion anchor for each of the two conduit clamp holes. Route 1/2 inch, flexible conduit to the HandPunch, ending the conduit between the two conduit clamp holes. Pull the wiring to enter the HandPunch through the conduit. Pull 18 inches of wire past the end of the conduit to allow enough space for final connection to the HandPunch.
4. Clear all dust and debris away from the HandPunch mounting location.

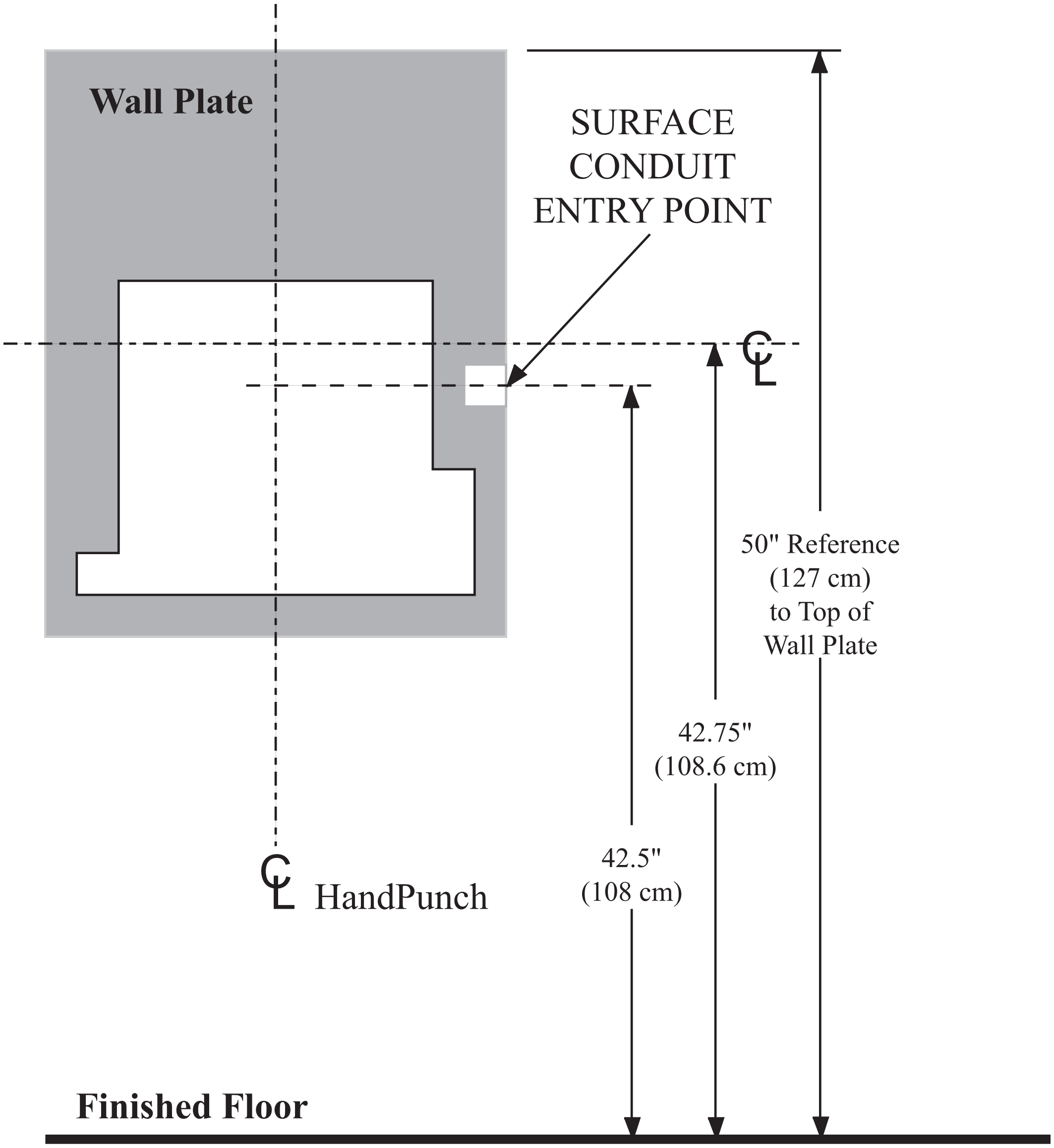

Wall Plate
SURFACE CONDUIT ENTRY POINT
CL
50" Reference (127 cm) to Top of Wall Plate
42.75" (108.6 cm)
42.5" (108 cm)
CL HandPunch
Finished Floor

Figure 12-2: HandPunch Wire Routing Layout

NOTE *Dust and debris surrounding the HandPunch can drastically affect the terminal's operation. It is important to ensure the HandPunch mounting location is free from dust and debris.*

Attaching the HandPunch

1. Loosen the three bottom mounting screws until there is approximately 1/8 inch (3 mm) clearance between the screw head and the wall plate.
2. Remove the HandPunch from its carton.
3. At the base of the HandPunch is a piano hinge with three keyhole shaped slots that correspond with the three lower mounting screws. Align and hang the HandPunch from the three lower mounting screws (see Figure 12-3 on page page 49).
4. Tighten all three lower mounting screws.
5. The HandPunch is now ready for its wiring connections.

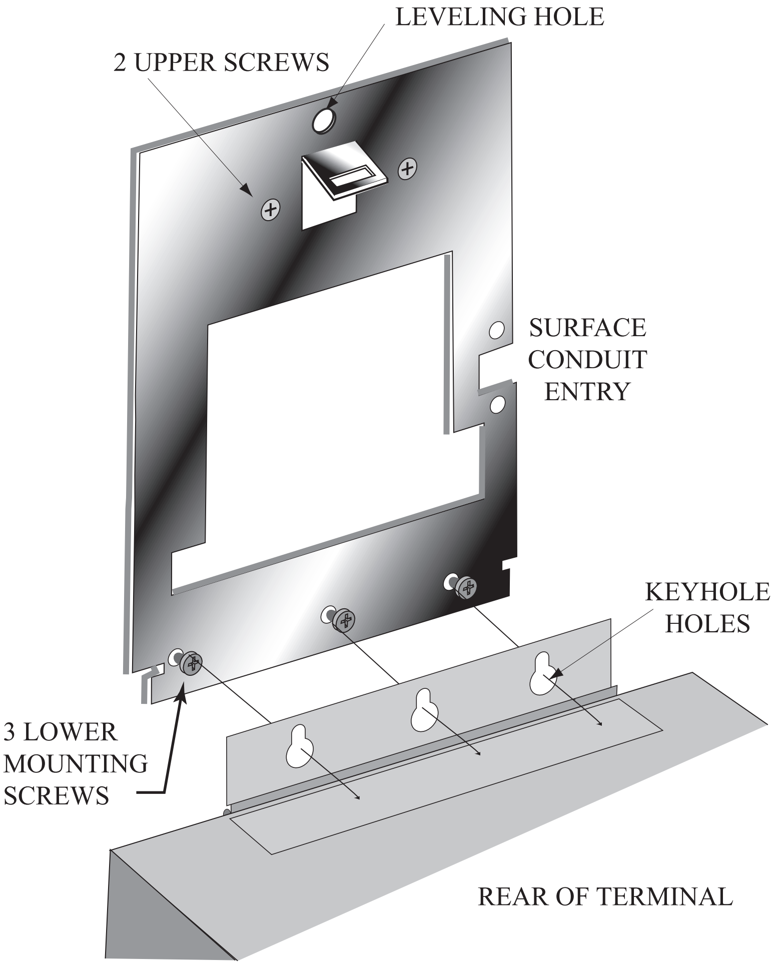


Figure 12-3: Attaching the HandPunch to the Wall Plate

Wiring Connections

Once the HandPunch is attached to the wall plate the wiring connections to the HandPunch can be made (see Figure 12-4).

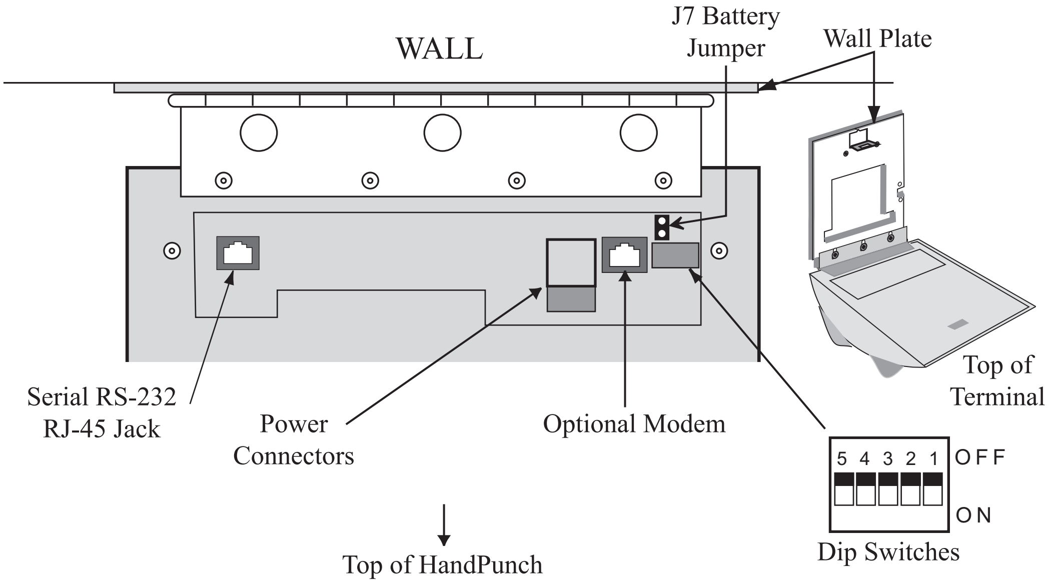


Figure 12-4: Wiring Connections and Dip Switches

Wiring Examples

Table 10 on page page 51 provides the pinouts for the RJ-45/RS-232 Serial Host Computer Connection.

Figure 12-5 on page page 51 provides a diagram of the RJ-45/RS-232 Connector.

Figure 12-6 on page page 52 provides a Host PC to HandPunch Modem Network wiring diagram (Modem wiring is a HandPunch option).

Table 10: RJ-45/RS232 Serial Connection

J8 Pin	Signal	Connection
1	RJ	- not used -
2	CD	- not used -
3	DTR	- not used -
4	GND	Ground
5	Rx Data	Receive Data Input (from external device)
6	Tx Data	Transmit Data Output (to external device)
7	CTS	- not used -
8	RTS	- not used -

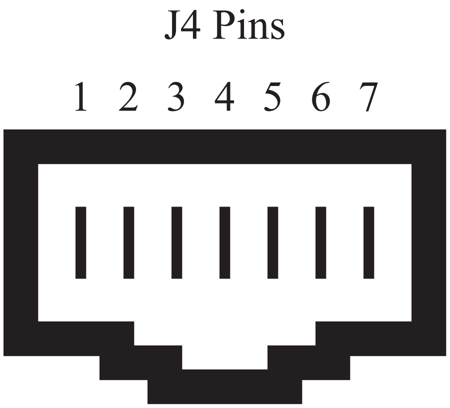


Figure 12-5: J4 - RJ-45/RS-232 Jack Pinout

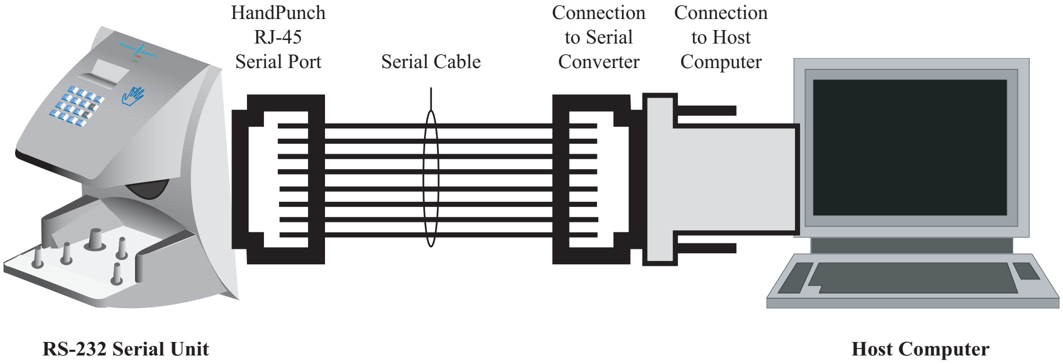


Figure 12-6: Host PC to HandPunch Modem Connection

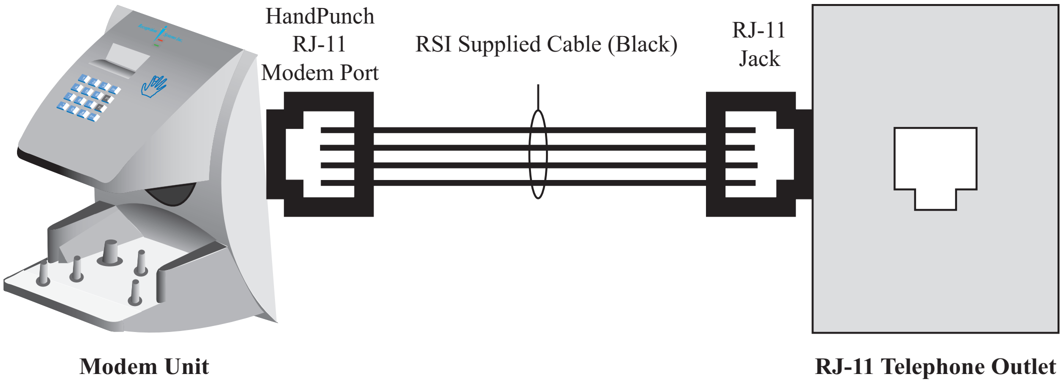


Figure 12-7: Host PC to HandPunch Modem Connection

Setting the DIP Switches

The DIP Switch settings perform three tasks for the HandPunch (see Figure 12-8).

- Set End of Line (EOL) Termination to match the type of termination needed by the network.
- Set the Communication Method to match the type of network used.
- Erase Memory to clear HandPunch memory to all factory default values and also clear all user memory.

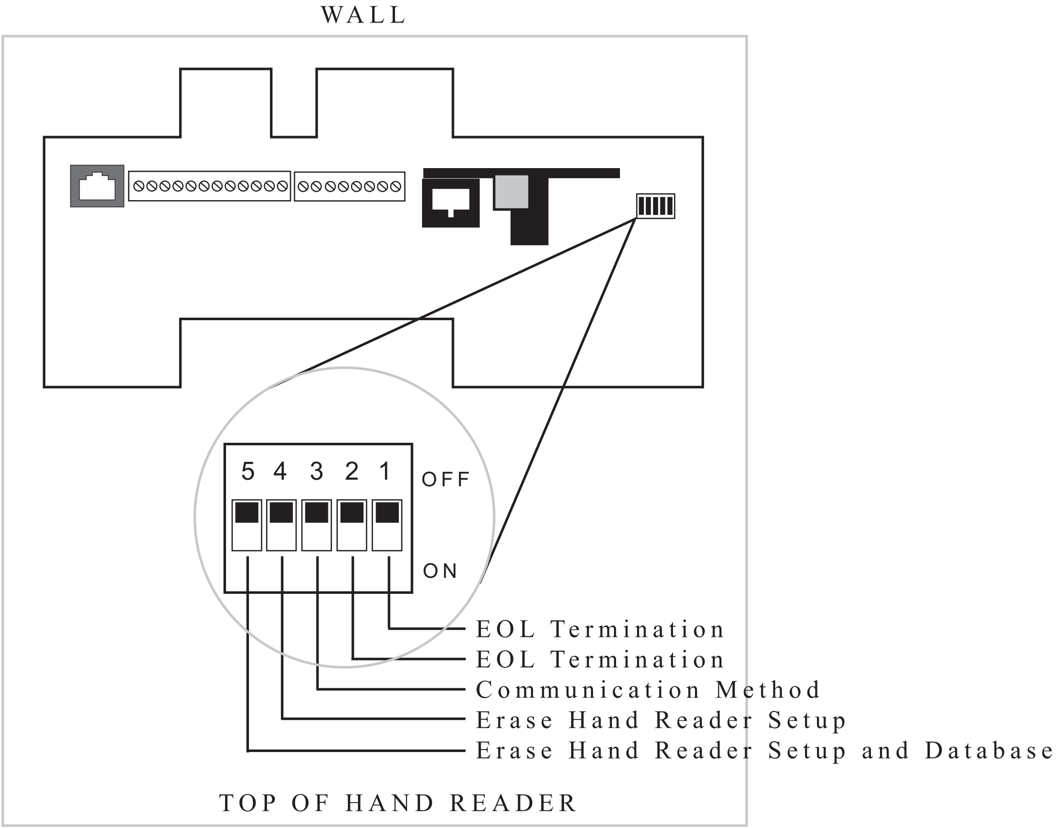


Figure 12-8: HandPunch Dip Switches

End of Line Termination

Termination helps to ensure clean data signals are transmitted through the network wiring. Termination is applied to the end-of-line (EOL) HandPunch in the network daisy-chain. The factory default setting is for EOL termination to be disabled – switches 1 and 2 OFF. Refer to Figure 12-8 on page page 53 for switch ON/OFF positioning.

- To enable EOL termination at a HandPunch, both switches 1 and 2 must be ON.
- To disable EOL termination at a HandPunch, both switches 1 and 2 must be OFF.

EOL Termination must be enabled for:

- A single HandPunch terminal installation.
- In a Modem to PC network the HandPunch terminal with the Modem option (for communication with the host computer).

Communication Method

The factory default setting and for standard operation, switch 3 must be OFF.

- Switch 3 must always be OFF.

Erasing HandPunch Memory

The erase memory function can perform either or both of the following:

- Erase a HandPunch's configuration data.
- Erase a HandPunch's user database and transaction buffer.

The factory default setting (and normal operation setting) is for switches 4 and 5 to be OFF, retaining memory.

NOTE *If the HandPunch is equipped with the battery backup option, remove shunt J7 in front of the DIP switch array (see Figure 12-4 on page page 50) before proceeding. Replace shunt J7 after completion of the following steps.*

Erasing the HandPunch Setup

Perform the following steps to erase the configuration data but retain the user database.

1. With system power OFF, set switch 4 ON.
2. Turn system power ON and wait for HandPunch boot information to appear on the display.
3. Turn switch 4 OFF.

Erasing the HandPunch Setup and User Database

Perform the following steps to erase both the configuration data and the user database.

1. With system power OFF, set both switches 4 and 5 ON.
2. Turn system power ON and wait 5 seconds.
3. Turn both switches 4 and 5 OFF.

! NOTE *Before putting the HandPunch into service ensure DIP switches 4 and 5 are both OFF. If switches 4 and 5 are not off, the next time the HandPunch's power is cycled the HandPunch's memory will be erased.*

Closing the HandPunch

Before closing the HandPunch, ensure dip switches 4 and 5 are OFF (refer to Figure 12-8 on page page 53). Clear all dust and debris away from the HandPunch. With the wall mount latch in the unlocked position, swing the body of the HandPunch up and lock the latch into place with the key provided with the HandPunch (see Figure 12-9).

NOTE *Dust and debris surrounding the HandPunch can drastically affect the terminal's operation. It is important to ensure the HandPunch is free from dust and debris before closing the terminal.*

NOTE *Do not force the HandPunch onto the wall mount latch when the latch is in the locked position.*

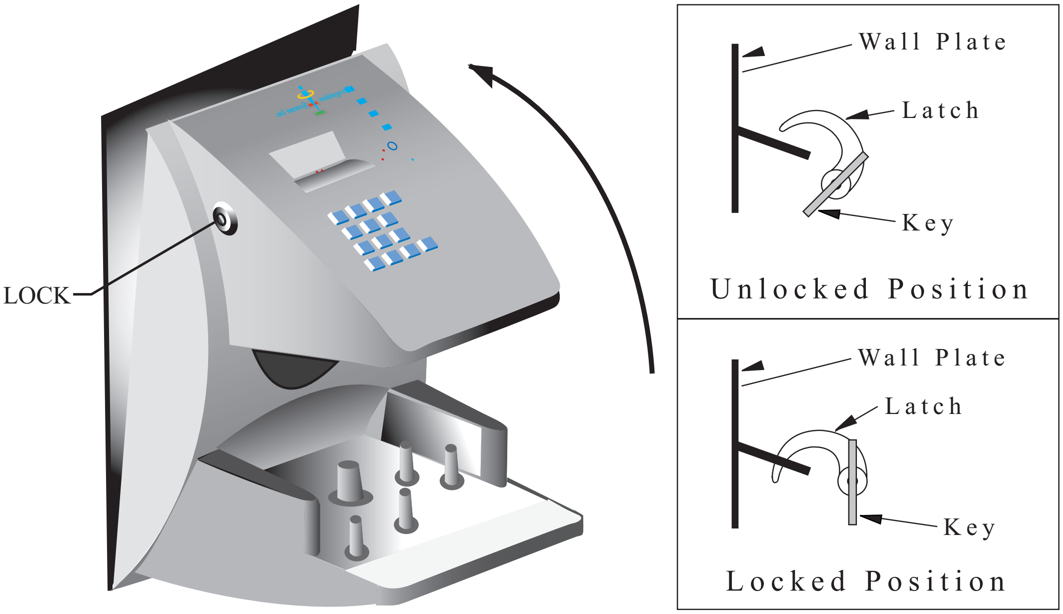


Figure 12-9: Closing the HandPunch

Appendix D

Troubleshooting Guide

Display Messages During Verification

Various messages can appear on the HandPunch's display during hand verification. These messages are defined in Table 11.

Table 11: Display Messages During Verification

Message	Definition
PLACE HAND	The platen is ready to receive your hand for verification.
ID VERIFIED	You are verified, proceed.
REMOVE HAND	Remove your hand and place it on the platen again. Follow proper hand placement rules.
TRY AGAIN	Your attempt was rejected. Repeat verification following proper hand placement rules.
ID REFUSED	Your rejections exceeded the maximum number of tries allowed. Wait until another employee has verified and try again or call your supervisor
ENTER ID	You entered your ID number incorrectly or your access time is restricted.

- If the display shows **TRY AGAIN**, you are not verified. You may have made an error in entering your ID number or in placing your hand on the platen. Re-enter your ID number and try again, taking care to follow proper hand placement rules (see page page 44).
-
- If the display shows **TIME RESTRICTION**, you are not authorized to punch in at this time. If this seems to be in error, contact your supervisor about time restrictions.
-
- After a pre-programmed number of denied attempts, an ID number will no longer be accepted and the display will appear as follows.

ID INVALID
TEMPORARILY

This is called a “lockout.” Before the rejected ID number can be used again, another employee or a supervisor must successfully verify at the HandPunch.

- If you enter your ID number, but do not place your hand on the platen, the HandPunch will time-out in about 25 seconds. You can immediately end this time-out by pressing the **CLEAR** key.

Beeper and LED Status During Verification

The HandPunch’s beeper and LED status display also display hand verification information. This information is defined in Table 12.

Table 12: Beeper and LED Status During Verification

Operation	Beeps	LED	Meaning
During Keypad Entry	1 per Keystroke	–	Keystroke Accepted
After ID Entry	–	–	OK - Proceed
After ID Entry	2	–	ID Number Not in Database
After Hand Placement	1	Green	ID Verified
After Hand Placement	2	Red	ID Not Verified - Try Again
After Hand Placement	1 Long Continuous	Red	ID Refused

Glossary

Address, HandPunch A HandPunch Address is a unique identification number assigned to a HandPunch. Each HandPunch on a network must be assigned a unique address.

AWG American Wire Gauge is a U.S. standard set of wire conductor sizes. The “gauge” refers to the diameter of the wire. The higher the gauge number, the smaller the diameter, the thinner the wire, and the greater the electrical resistance. Thicker, smaller gauge wire carries more current because it has less electrical resistance over a given length. Thicker wire is better for long wire distances.

HandPunch Address See Address, HandPunch

Platen The Platen is the flat surface at the base of the HandPunch, on which a user places his/her hand for enrollment and verification. The platen has guide pins to ensure the user’s fingers are consistently positioned correctly.

Template A Template is a set of data generated for a user. It is made up of the user’s enrollment information and any system configuration parameters that are assigned to the user. The template is stored at each HandPunch and can be stored at the host computer with the Time and Attendance software.

Transaction A Transaction is any kind of event recorded at a HandPunch. Transactions may include In or Out punches, department transfers, and supervisor edits.

Limited Warranty

Schlage Biometrics, Inc. (the “Company”) warrants to the original user the products manufactured by the Company (the “Product”) to be free of defects in material and workmanship for a period of three months from the date of purchase by such user or six months from the date of shipment from the factory, whichever is sooner, provided:

1. The Company has been notified within such period by return of any alleged defective product, free and clear of all liens and encumbrances, to the Company or its authorized dealer, transportation prepaid; and

2. The Product has not been abused, misused, or improperly maintained and/or repaired during such period; and

3. Such defect has not been caused by ordinary wear and tear; and

4. Such defect is not the result of voltage surges/brownouts, lightning, water damage/flooding, fire, explosion, earthquakes, tornadoes, acts of aggression/war, or similar phenomenon; and

5. Accessories used as integral to the Product have been approved by the Company.

The Company shall, at its option, either repair or replace, free of charge, the Product found, upon the Company’s inspection, to be so defective, or if agreed upon, refund the purchase price, less a reasonable allowance for depreciation, in exchange for the Product.

THE COMPANY MAKES NO OTHER WARRANTY AND ALL IMPLIED WARRANTIES INCLUDING ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE ARE LIMITED TO THE DURATION OF THE EXPRESSED WARRANTY PERIOD AS SET FORTH ABOVE.

THE COMPANY’S MAXIMUM LIABILITY THEREUNDER IS LIMITED TO THE PURCHASE PRICE OF THE PRODUCT. IN NO EVENT SHALL THE COMPANY BE LIABLE FOR ANY CONSEQUENTIAL, INDIRECT, INCIDENTAL, OR SPECIAL DAMAGES OF ANY NATURE ARISING FROM THE SAME OR THE USE OF THE PRODUCT.

Schlage Biometrics Inc. reserves the right to make changes in the design of any of its products without incurring any obligation to make the same change on units previously purchased.

Ingersoll Rand
Security Technologies

Ingersoll Rand's Security Technologies Sector is a leading global provider of products and services that make environments safe, secure, and productive. The Sector's market-leading products include electronic and biometric access control systems; time and attendance and personnel scheduling systems; mechanical locks and portable security, door closures and exit devices, steel doors and frames, architectural hardware and technologies and services for global security markets.

866.861.2480

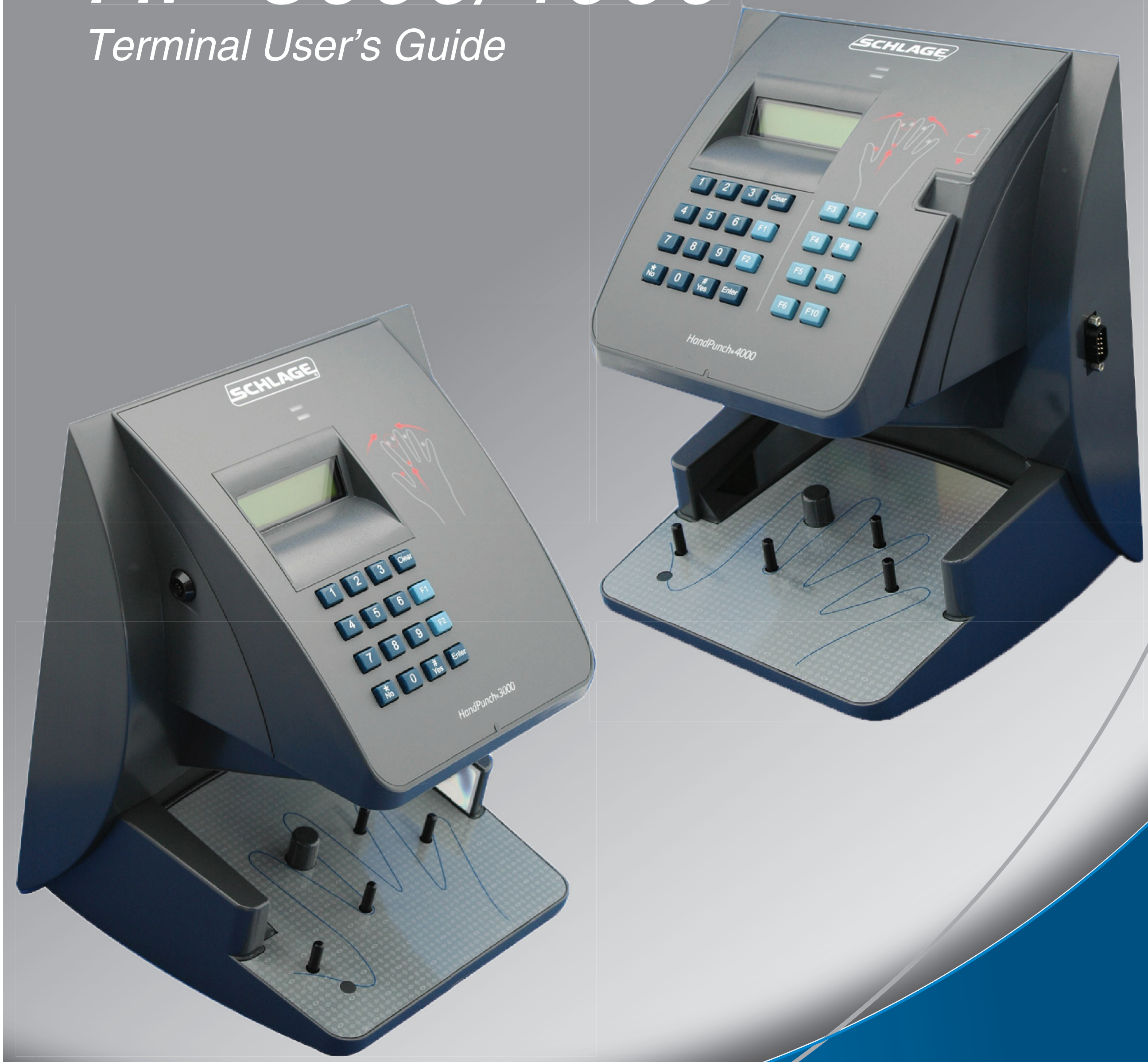
www.schlage.com www.ingersollrand.com

Schlage
Biometric Solutions
Ingersoll Rand Security Technologies
538 Oakmead Parkway
Sunnyvale, CA 94085
Office: 866-861-2480/512-712-1413 (international)
Fax: 866-303-1794/408-341-4101
E-mail: sbssupport@irco.com

SCHLAGE®

HP-3000/4000

Terminal User's Guide



Ingersoll Rand
Security Technologies

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and, if not installed and used in accordance with the Installation Manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at the user's own expense.

This Class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numerique de la classe A respecte toutes les exigences du Reglemente sure le materiel brouilleur du Canada.

Document Part Number: 70100-6003 – Revision 3.3 – July, 2011

HandPunch is a trademark of Schlage Biometrics, Inc.

The trademarks used in this Manual are the property of the trademark holders. The use of these trademarks in this Manual should not be regarded as infringing upon or affecting the validity of any of these trademarks.

Schlage Biometrics, Inc. reserves the right to change, without notice, product offerings or specifications.

Table of Contents

Introduction

The HandPunch 3000/4000 is part of Schlage Biometrics' 3rd generation line of biometric hand geometry Time and Attendance Terminals[1]. The HandPunch records and stores a three-dimensional shape of the human hand for comparison and identity verification. Upon verification, the HandPunch records the time, date, user ID number, and collected time and attendance data for collection by a host computer. The HandPunch can produce an output that can unlock a door and it can communicate with a host computer. The HandPunch also has auxiliary inputs and outputs that can be used to control other systems such as bells and alarms.

The HandPunch provides proof-positive employee verification combined with the sophisticated operating features one expects in a modern Time and Attendance Terminal. Because of this unique combination of capabilities, the HandPunch provides the most accurate Time and Attendance data collection terminal available. The key features of the HandPunch include:

- Programmable Function Keys
    - HP-3000 – 2
    - HP-4000 – 10
- User Time Restrictions
- Supervisor Override at the “Time Clock”
    - Add Punch
    - Add Bulk Hours or Dollars
    - Review Punches
- Department Transfers
- Explicit Punch Menu
- Transaction Buffer
    - HP-3000 – 5,120 event capacity
    - HP-4000 – 7,680 event capacity
- Bell Schedules
- Door Control and Monitoring
- Programmable Clock and Date Formats and Daylight Savings Switch-over

The HP-4000 also includes:

- Integrated Bar Code Reader
- Programmable User Messages
- Data Validation

[1] For the sake of using a consistent name throughout the manual, the HandPunch 3000/4000 terminal is referred to as the HandPunch for the remainder of this manual.

Biometrics

Biometrics is a term describing the automatic measurement and comparison of human characteristics. While its origins are ancient, the evolution of advanced scanning and microprocessor technology brought biometrics into everyday life. Electronic hand geometry technology first appeared in the 1970s. Schlage Biometrics Inc., founded in 1986, built the first mass-produced hand geometry readers and made biometric technology affordable for the commercial market. Today, Schlage Biometrics' products are in use in every imaginable application from protecting cash vaults to verifying employee attendance in hospitals.

Principle of Operation

The HandPunch uses low-level infrared light, optics, and a CMOS camera to capture a three-dimensional image of the hand. Using advanced microprocessor technology, the HandPunch converts the image to an electronic template. It stores the template in a database along with the user's ID number.

To gain punch, the user enters his or her ID number at the HandPunch's keypad or uses an external card reader. The HandPunch prompts the user to place his or her hand on the HandPunch's platen[1]. The HandPunch compares the hand on the platen with the stored user's unique template. If the images match, the HandPunch records the transaction for processing.

The HandPunch Terminal

The HandPunch is a time and attendance terminal designed for use with time and attendance software. Refer to "Figure 1-1" on page 5 and "Figure 1-2" on page 6 when reviewing the information in this section.

The HandPunch has an integrated keypad for ID entry and reader programming. The HandPunch 3000 has two function keys (F1 and F2 – see Figure 1-1). The HandPunch 4000 has ten function keys (F1 through F10 – see Figure 1-2). These function keys can be programmed to collect data or to activate auxiliary outputs. The **CLEAR** and **ENTER** keys assist in data entry and programming.

[1] The Platen is the flat surface at the base of the HandPunch (see Figure 1-1). This is where users place their hands for enrollment and verification. It has guide pins to assist positioning the fingers during use.

Four different features assist the user with hand placement and read verification.

1. A light emitting diode (LED) hand placement display on the HandPunch's top panel assists users with hand placement on the platen.
2. A liquid crystal display (LCD) shows operational data and programming menus.
3. "Red light/Green light" verification LEDs quickly inform users if their verification attempts were rejected or accepted.
4. An internal beeper provides audible feedback during keypad data entry and user verification.

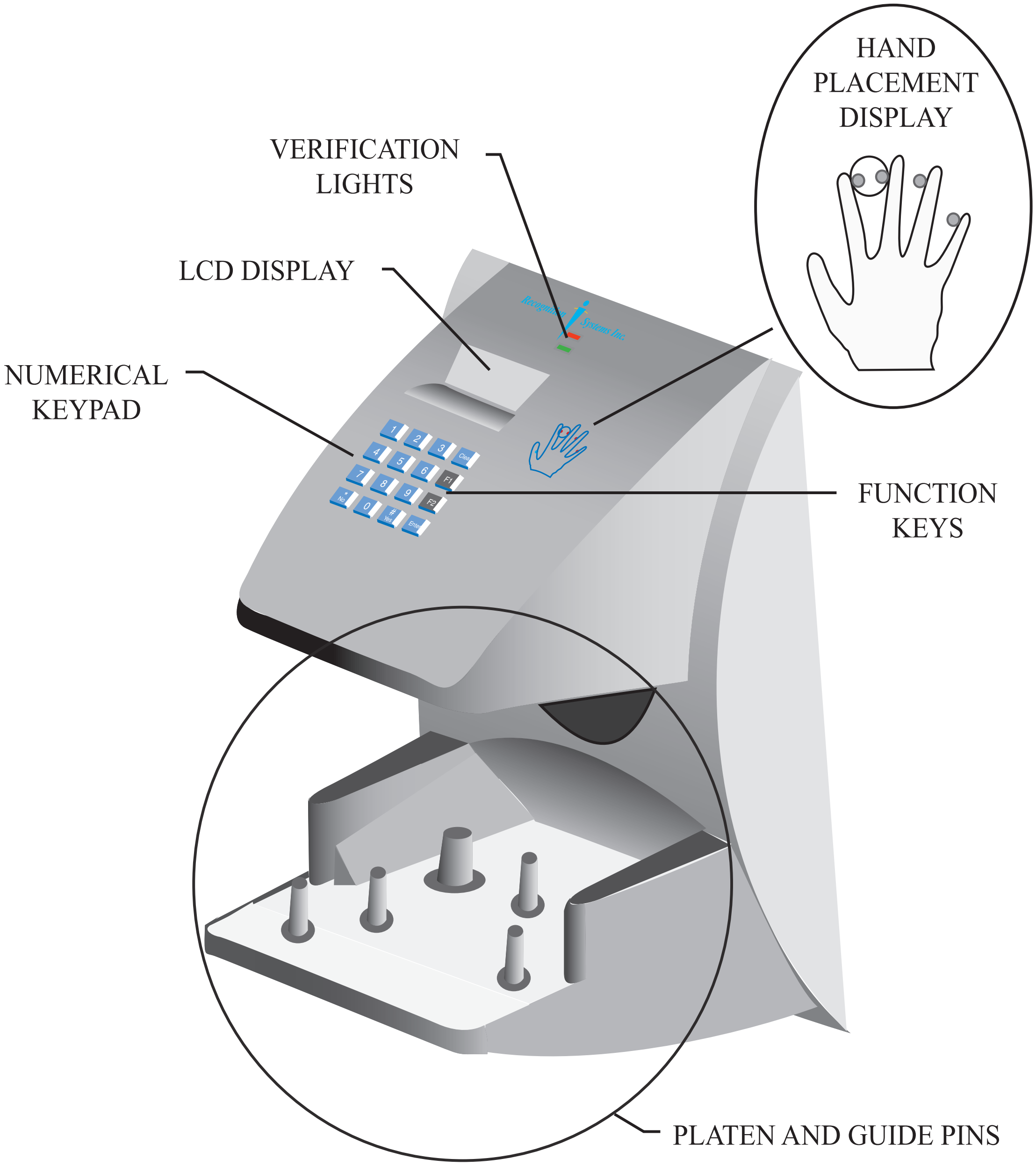
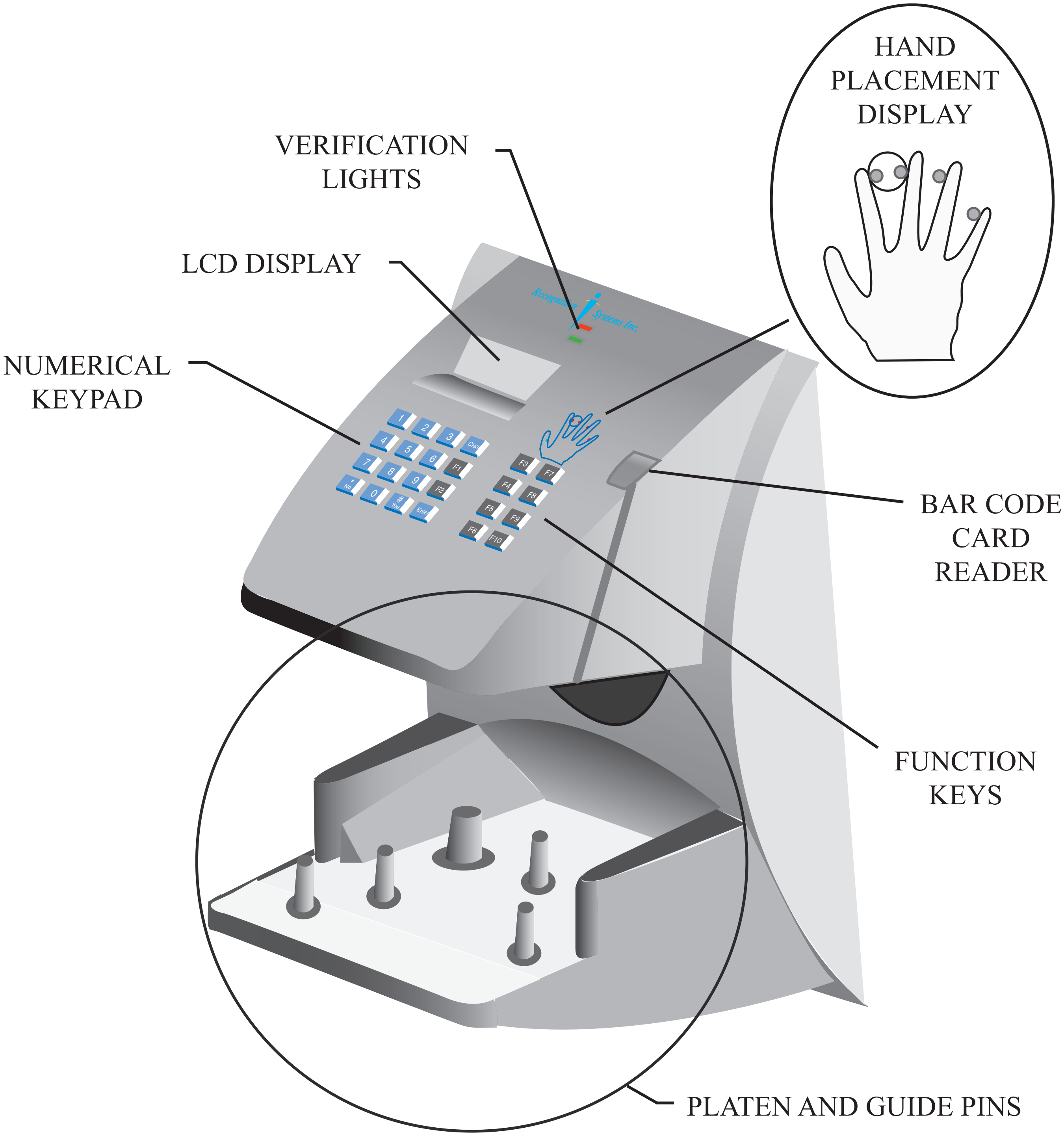


Figure 1-1: The HandPunch 3000



: The HandPunch 4000

Specifications

Table 1: Specifications

Size:	8.85 inches wide by 11.65 inches high by 8.55 inches deep.
	223 cm wide by 29.6 cm high by 21.7 cm deep.
Power:	12 to 24 VDC or 12 to 24 VAC 50-60 Hz, 7 watts
Weight:	6 lbs (2.7 kg) – 7 lbs (3.2 kg) with optional backup battery
Wiring:	2 twisted-pair, shielded, AWG 22 or larger (such as Belden 82732)
Temperature:	-10°C to +60°C – non-operating/storage (14°F to 140°F) 5°C to 40°C – operating (40°F to 110°F)
Relative Humidity Non-Condensing:	5% to 95% – non-operating/storage (non-condensing) 20% to 80% – operating
Verification Time:	1 second or less
Memory Retention:	5 years using a standard internal lithium battery
Transaction Buffer:	HP-3000 – 5,120 transactions HP-4000 – 7,680 transactions
ID Number Length:	1 to 10 digits
Baud Rate:	300 to 28.8 K bps
Communications:	RS-232, RS-422, optional Modem, optional Ethernet
User Capacity:	HP-3000 – 512 users expandable to 40,xxx HP-4000 – 530 users expandable to 5,xxx
Message Capacity:	HP-4000 – 550 exandable to 3520 (not available with the HP-3000)
Function Keys:	HP-3000 – 2 user definable, HP-4000 – 10 user definable
Card Reader Input:	Proximity, Wiegand, Magnetic Stripe, Bar Code (5 VDC provided by HandPunch unit)
Door Controls:	Lock output, Request to Exit input, Door Switch input (open collector, 5 VDC present, sinks to ground, 100 mA max)
Alarm Monitoring:	Tamper, Door Forced
Event Monitoring:	There are a variety of monitoring options including events such as: Invalid ID, Time Zone Violation, ID Refused, Try Again, Power Failure
Time Zones:	62 total: 2 fixed, 60 programmable

Table 1: Specifications

Time Schedules:	HP-4000 – 3 definable time schedules per user
Auxiliary Inputs:	2 (open collector, 5 VDC present, sinks to ground, 100 mA max)
Auxiliary Outputs:	up to 3 user definable (open collector, 5 VDC present, sinks to ground, 100 mA max)

Options

HandPunch units have the following options available.

• Backup Battery Support	See Technical Note 70200-0012 rev C
• Modem Communication	See Technical Note 70200-0013 rev C
• Ethernet Communication	See Technical Note 70200-0014 rev H

UL Compliance

Hand Readers are UL Listed as stand alone units only (i.e. the card reader function has not been evaluated by UL).

The HandKey II has not been tested for UL 294 in an Outdoor configuration.

CE approved

♻

recyclable

This page is intentionally blank.

This page is intentionally blank.

Planning an Installation

Site Preparation

Before you begin installation, check the site blueprints, riser diagrams, and specifications for important information about the HandPunch's location and other systems that will connect to the HandPunch. Look for any existing wall preparations and wiring that other contractors may have installed for the HandPunch. A wire routing layout diagram (see "Figure 3-2" on page 25) is provided to assist in planning.

HandPunch Placement

The recommended height for the HandPunch platen is 40 inches (102 cm) from the finished floor. The HandPunch should be out of the path of pedestrian and vehicular traffic, and convenient too, but not behind the door it is controlling. Avoid placing the HandPunch where users must cross the swing path of the door. **The HandPunch should be in an area where it is not exposed to excessive airborne dust, direct sunlight, water, or chemicals.**

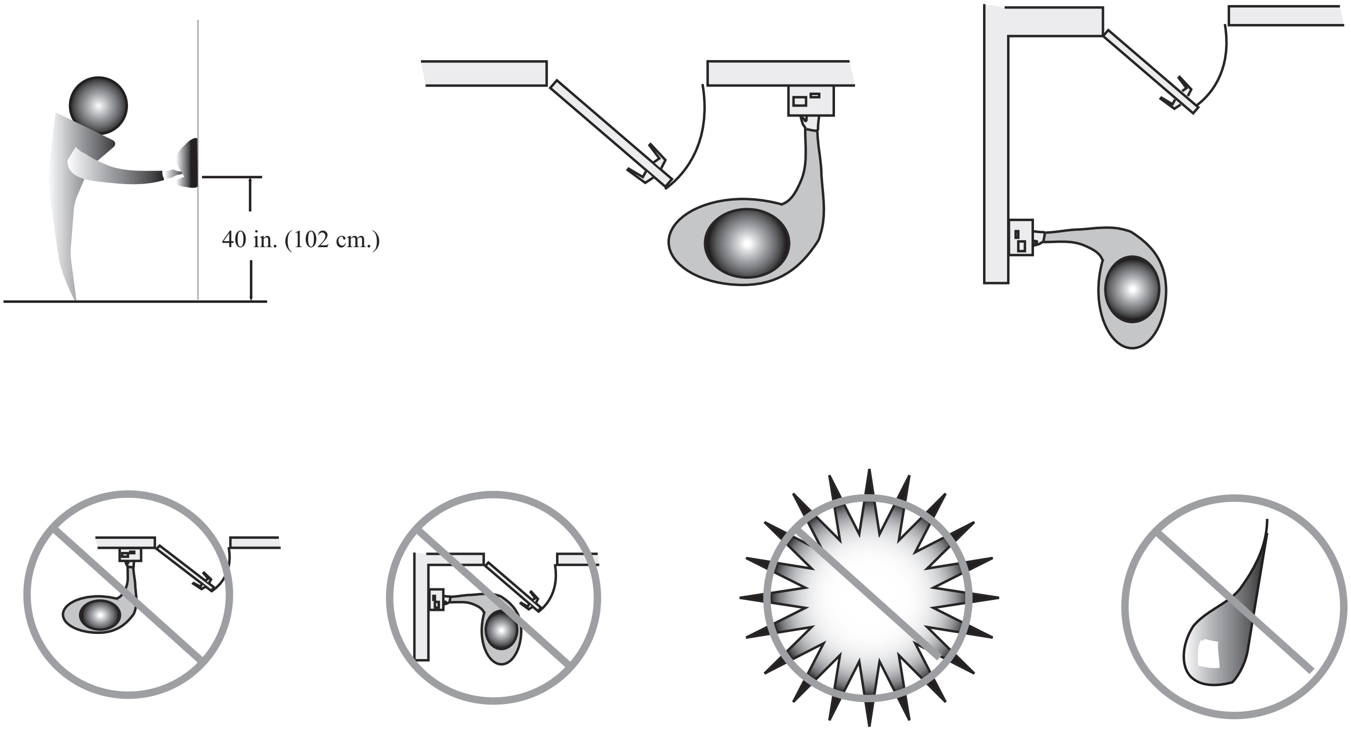


Figure 2-1: HandPunch Placement Rules

NOTE *For the following sections, Schlage Biometrics does not supply hardware items such as door control relays, door locks, switches, relays, communications or power wiring.*

Wiring

Four basic circuits typically connect to the HandPunch:

- Power Input
- Earth Ground and Shielding
- Networking and Communications
- External Devices

The minimum wire size for these circuits is AWG 22; the maximum wire size is AWG 18. Schlage Biometrics recommends using Belden 82732 or its equivalent when wiring for RS-422 communications.

Power Input

The HandPunch uses an internal switching regulator to obtain internal operational power. It accepts input voltages from 12 to 24 VDC or 12 to 24 VAC at 50 to 60 Hz. The HandPunch comes with a 120 VAC to 13.5 VDC power supply (Class 2, Model No. P48131000A010G-120 VAC, 60 Hz, 21 W, 13.5 VDC output @ 1000mA), if need an optional 220 VDC power supply is also available (this power supply was not evaluated for UL 294).

To power the HandPunch with this power supply, a 120 VAC (or 220 VAC as applicable) duplex outlet must be within 5 feet of the HandPunch. The power supply has a 6-foot cable to provide a comfortable reach between power outlet and HandPunch. The barrel jack at the of the power supply's cable is connected to J12 on the HandPunch PCB.

! NOTE J6 terminal 1 and the center pin of power jack J12 are connected together.
J6 terminal 2 and the sleeve of power jack J12 are connected together.

! NOTE Neither terminal 1 or terminal 2 is connected to the HandPunch ground.

! NOTE *Do not connect a HandPunch's power supply to a switched duplex outlet. The HandPunch must have a constant source of power for proper operation.*

Battery Backup

The HandPunch uses an internal switching regulator to obtain internal operational power. It accepts input voltages from 12 to 24 VDC or 12 to 24 VAC at 50 to 60 Hz. An optional power-fail protection circuit board can be attached to the main circuit board to provide and control battery backup. The design of the internal power supply is such that any range of the above input voltages may be used and still provide proper battery charge voltage and battery backup operation. Switch-over to battery power is automatic and occurs when the input voltage falls to approximately 10.5 volts. At that time the internal battery charger is disabled to save power and uninterrupted operation continues on battery power.

When input power is restored, the HandPunch switches off of battery operation and the battery charger is re-enabled to recharge the battery. Battery charge voltage is set at approximately 13.65 volts, and battery charge current is limited to approximately 50 mA. A fully discharged battery requires approximately 12 hours of charge to fully recover.

Additional options installed and specific configurations within the HandPunch make it difficult to predict precisely how long battery support will last, but in general two hours of battery operation can be expected. While operating on battery backup due to loss of main input power, the battery output voltage is constantly monitored by internal circuitry. If the battery voltage reaches approximately 9.5 volts the HandPunch automatically shuts down. This is done to prevent full exhaustion of the battery. A yellow indicator on the top panel illuminates to indicate that the HandPunch is running off of battery power. This indicator extinguishes when main input power is restored.

Shunt J7 which is located to the left of TS3 see “Figure 4-1” on page 31 enables or disables battery operation on those HandPunchs equipped with optional battery backup. If a HandPunch does not have the optional battery backup package installed, J7 is not used. On HandPunchs equipped with the battery backup option, J7 allows service personnel a mechanism for disabling battery backup operation before removal of main input power. To fully power down a HandPunch equipped with battery backup, remove or reposition shunt J7 so that the two pins protruding up from the main logic board are not connected to each other. This effectively opens the circuit, removing the battery from any internal circuitry. Main input power can then be removed and the HandPunch will fully shut down. Once the HandPunch has fully shut down, shunt J7 may be reinstalled. The design of the power supply is such that main input power must be reapplied to re-enable the battery protection mechanism. If shunt J7 is not properly installed, the internal backup battery will not be charged, and in the event of a main input power loss, the HandPunch will shut down.
The HandPunch with the battery backup option uses a 12 volt 800 ma/hour sealed lead acid battery to provide backup battery power. This battery is located immediately inside the rear panel of the HandPunch and plugs into jack J4 on the keypad control circuit board located in the top of the chassis.

Earth Ground and Shielding

Schlage Biometrics recommends that all HandPunchs be grounded with a solid, reliable earth ground connection. This connection establishes a common ground return point used to protect internal semiconductor devices from ElectroStatic Discharge (ESD) and from external signal line transients. It also provides a common signal level reference point between externally networked HandPunchs. Schlage Biometrics recommends that the earth ground source be identified by a qualified electrician familiar with electrical codes as well as wiring and grounding techniques.

This is an extremely important and often overlooked aspect of hard-wired serial communication systems. If the sending and receiving stations do not agree on the ground reference for the signal voltages, communication errors or a total inability to communicate may be observed. If the voltages are very different, it is even possible to damage the units.

The subject of grounding can be complicated, and the full circuit of a system, including power supplies and often even the building line power wiring, must be understood. It is strongly recommended that a qualified electrician or electrical engineer familiar with this subject be consulted when designing the wiring of an HGU network installation. Always adhere to any applicable electrical codes for your area. Schlage Biometrics is not responsible for damage done to units due to improper wiring.

! NOTE *Use any one of the following ground terminals to make the earth ground connection: 4, 10, or 13. Do* **NOT** *use terminal 2 to establish the earth ground connection; terminal 2 is not directly connected to ground.*

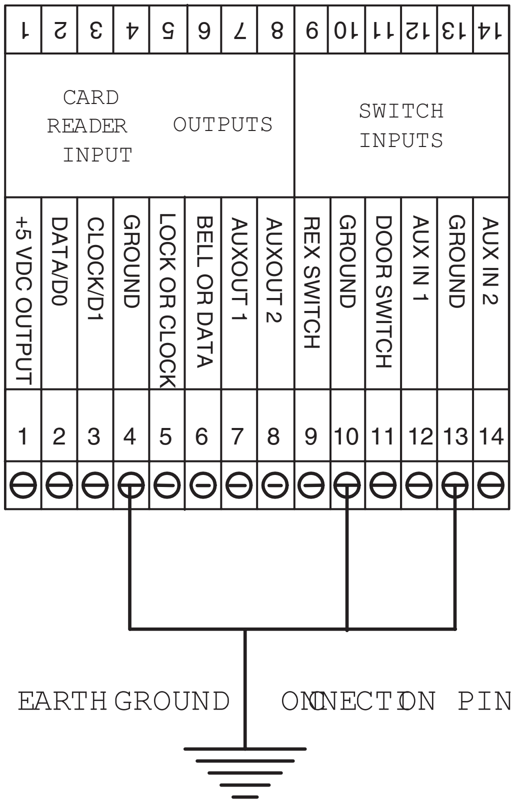


Figure 2-2: Earth Ground Connection Terminals

There are two standard methods for providing earth grounding to HandPunch units:

- earth grounding all units (see Figure 2-3)
- carrying an earth ground to each unit (see Figure 2-4)

Earth ground all units when there is a good earth ground source near each unit and/or when there are very long cable runs between units.

Carry an earth ground to each unit when there are no earth grounds convenient to the unit and the unit's power supply is floating.

Earth Ground All Units

One method of establishing a ground reference is to connect each unit's main board ground to earth ground. Earth ground is found on the third pin on standard AC line sockets (in the United States, this is the round one in the middle). If the building wiring is functioning correctly, this should be a low-impedance path to a true ground, which then serves as a common reference point for the units.

If this method of grounding the units is used, it is not necessary to connect the units in the network together with a ground line in the communication cable. Indeed, doing so could create ground loops—large-area loops which provide a good coupling to external magnetic fields—which may actually compound communication problems. If a magnetic field, such as that from a lightning strike, induces a voltage in the ground loop, it is possible for large currents to flow around the loop, which can raise the ground potential of some units relative to others. When the shield or the cable is connected to any ground in this configuration, it should be connected only at one end to prevent the formation of ground loops.

For systems with multiple units on a network, there will be a series of cables daisy-chained between the units, and the shield of each leg of the network should be connected to ground at only one end. It does not matter which end. An example of this method of grounding is shown in Figure 2-3.

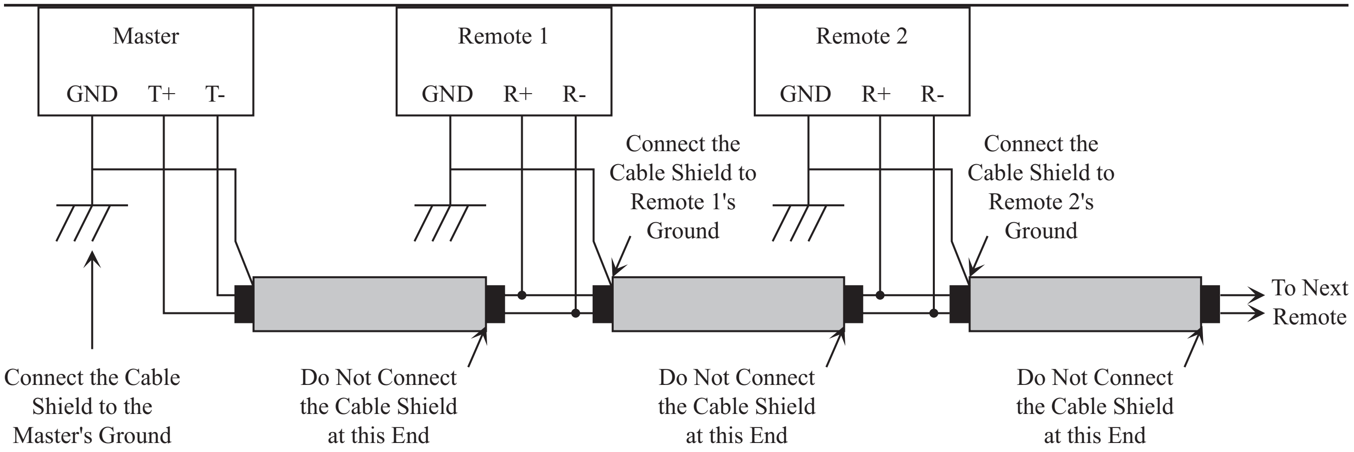
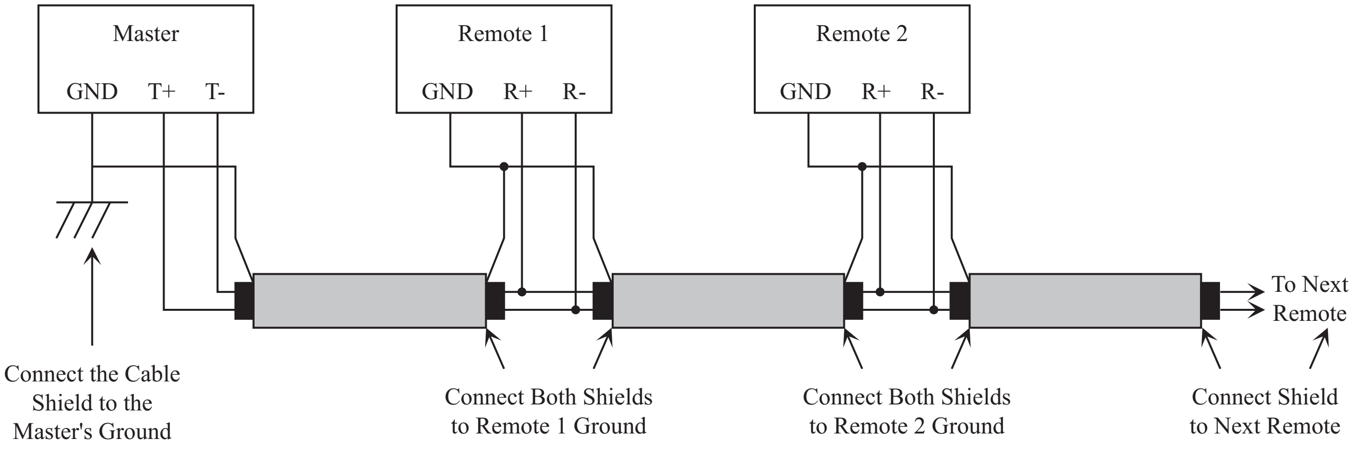

Master
GND
T+
T-
Remote 1
GND
R+
R-
Remote 2
GND
R+
R-
Connect the Cable Shield to Remote 1's Ground
Connect the Cable Shield to Remote 2's Ground
To Next Remote
Connect the Cable Shield to the Master's Ground
Do Not Connect the Cable Shield at this End
Do Not Connect the Cable Shield at this End
Do Not Connect the Cable Shield at this End

Figure 2-3: Communication Shielding with All Units Earth Grounded

All units are connected to the same earth ground. Each shield ground is connected to only one unit, then interrupted to prevent the formation of ground loops. Two sets of lines are wired as shown in Figure 2-3. It does not matter significantly which unit's GND is used for a particular shield, as long as the path is broken from unit to unit.

Carry a Ground Line to Each Unit

The second method of establishing a ground reference in a system with floating power supplies is to use the ground line in the RS-422 cable to establish a common reference voltage for the communication signals. This line should be connected to the negative power terminal on the data converter or the ground line in the RS-232 port from the host PC system. It should then be carried to one of the ground terminals on the back of each unit in the network. An example of this method of grounding is shown in Figure 2-4.


Master
GND
T+
T-
Remote 1
GND
R+
R-
Remote 2
GND
R+
R-
To Next Remote
Connect the Cable Shield to the Master's Ground
Connect Both Shields to Remote 1 Ground
Connect Both Shields to Remote 2 Ground
Connect Shield to Next Remote

: Communication Shielding Carrying a Single Ground to Each Unit

If no earth ground is available at the units, this is the only possible method of connecting the grounds. Even if an earth ground is available, depending on the building's power wiring and other environmental issues, this method may be superior to the previous one, since it establishes the ground of each unit independently of the building power lines. Local variations in grounds between buildings, or from one point to another in a very large building, (perhaps due to elevator motors or other large-current drawing machines) will have no effect on the communication network if this configuration is used.

However, the power supplies must be truly floating, with no hidden paths back to the high-voltage side of the transformers, or to earth ground. Since this is difficult to achieve (there is always some parasitic capacitance between the primary and secondary in any transformer), this method may be more susceptible to high-frequency transients in the high-voltage side of the power lines than the earth-grounded method.

The master unit's ground establishes the ground for the entire system. The main board ground points are connected to the shield ground at each unit, but are not connected to earth ground. The ground point on the master can be the data converter power supply negative terminal, or the GND pin on the RS-232 cable. If the master is an HGU, its main board ground can be used. This configuration should only be used if the power supplies to the units are truly floating, otherwise ground loops will be created, and differences in local grounds may cause large currents to flow through the cable shield.

Communications

HandPunch to Host Computer Connection

HandPunch/host computer communications can be configured in one of three ways:

- via a direct RS-232 connection
- via a direct RS-422 connection using a data converter
- via an optional Ethernet network connection (one HandPunch terminal must have the Ethernet communication option installed)
- via an optional Modem connection (one HandPunch terminal must have the Modem communication option installed)

RS-232 Host Computer Connection

A direct HandPunch connection to a host computer can be made through an 4-conductor cable in an RS-232 serial configuration. A 6’ or 50’ cable may be purchased through Schlage Biometrics or a wiring diagram for the RS-232 to host computer connection is found on “Table 4” on page 33.

!NOTE *If you make the RS-232 to host computer connection you cannot use the serial printer option (see page 21).*

RS-422 Host Computer Connection

A direct HandPunch network connection to a host computer can be made through a shielded, 4-conductor cable in a full-duplex RS-422 configuration. An RJ-11 jack must be installed within 6 feet of the host computer. Position the RJ-11 jack using the template provided in this manual (see “Figure 3-2” on page 25). The HandPunch RS-422 network is connected to this jack.

A data converter (Schlage Biometrics P/N: DC-102) is required to connect the host computer to the RS-422 HandPunch network. The DC-102 is connected to an available RS-232 serial port on the computer. Then connect the DC-102 to the RJ-11 jack using the 8 foot cable provided with the DC-102. A wiring diagram for the RS-422 to host computer connection is found on page 31.

A HandPunch communication network is then connected, unit-to-unit, via an RS-422 “daisy-chain” network. A network RJ-11 jack is installed on or in the wall behind each terminal. Each RJ-11 jack is then interconnected in daisy-chain fashion using two, twisted-pair, AWG22 wires (Schlage Biometrics recommends using Belden No. 82723 cable). The daisy-chain network can extend up to 4,000 feet in length, and can have up to 31 HandPunch terminals connected to it.

Connect the HandPunch terminal to the RJ-11 jack using the short silver cable provided with the terminal.

NOTE *When wiring the RS-422 daisy-chain network, do not wire HandPunch terminals in a “star” network (a network where a number of units are all connected to the network at one, central location – see Figure 2-5).*

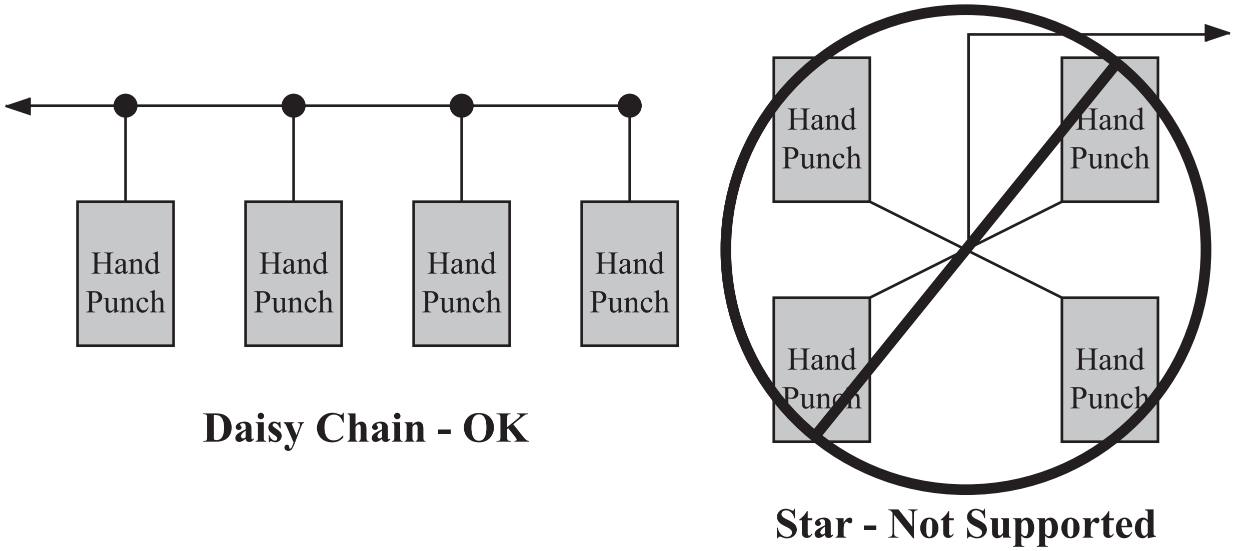


Figure 2-5: Daisy-Chain Versus Star Network Communication Connections

Ethernet Host Computer Connection

The HandPunch is available with an optional, internal Ethernet communications module for TCP/IP communications between the HandPunch network and the host computer. When connecting via an Ethernet connection, one HandPunch terminal must be configured with this Ethernet option. This terminal will communicate with the host computer.

To make the Ethernet connection, the Ethernet wiring must conform to 10BaseT standards. An Ethernet RJ-45 jack must be installed on or in the wall behind the Ethernet HandPunch terminal. Position the jack location using the template provided in this manual (see “Figure 3-2” on page 25). The cable from the jack to the HandPunch is not provided with the Ethernet option. A wiring diagram for the Ethernet to host computer connection is found on page 39.

IP Address and Gateway and Subnet Mask information is entered at the HandPunch using the Set Serial command (see page 59).

Modem Host Computer Connection

The HandPunch is also available with an optional modem module for telephone line communications between the HandPunch network and the host computer. When connecting via modem, one HandPunch terminal must be configured with the modem option. This terminal will communicate with the host computer.

To make the modem connection, a telephone jack must be installed on or in the wall behind the modem HandPunch terminal. Position the RJ-11 jack location using the template provided in this manual (see “Figure 3-2” on page 25). The short black cable provided with the modem HandPunch connects the terminal to the telephone jack. A wiring diagram for a modem to host computer connection is found on page 40.

External Devices

The HandPunch can control external devices such as:

- Bell
- Door Lock
- Request to Exit, Door Switch, and Auxiliary Inputs
- Auxiliary Outputs
- External Card Reader
- Serial Printer

The HandPunch requires the use of an external DC power supply to operate other controls or relays. The power supply can be of a different voltage than that used to power the HandPunch. The bell, door lock, and auxiliary outputs switch to ground when activated. For these devices, one pole of a control relay is connected to the PLUS side of the power supply, and the other pole connects to the output connection (switched minus) on the HandPunch. The negative pole on the external power supply must connect to a negative (ground) connection on the HandPunch to complete the circuit. The current draw of the relay or external device must not exceed 0.1A.

Wiring for these devices should enter the HandPunch through the opening in the center of the wall plate or through the conduit opening at the right side of the HandPunch.

!NOTE *The external DC power supplies and relays needed to operate external devices such as bells or door locks are* **NOT** *provided by Schlage Biometrics. You must provide these power supplies.*

Bell

The bell control circuit switches direct current to ground when actuated. The bell must receive its power from an external power supply through the contacts of a bell control relay. Refer to the Bell Output Wiring Diagram on page 34.

Door Lock

The door lock control output of the HandPunch switches to ground upon verification (unless programmed to send card data to a third-party control panel). As the output is limited to 0.1A, a lock control relay must be used. Refer to the Lock Output Wiring Diagram on page 35 for lock output wiring connections. The relay and lock must receive power from an external power supply.

Request to Exit, Door Switch, and Auxiliary Inputs

The HandPunch terminal has four inputs. Refer to the Inputs Wiring Diagram on page 36.

- Request to Exit
- Door Switch
- Two Auxiliary Inputs

A Request to Exit switch (REX) on the secure side of a controlled door will activate the lock output. When the REX switch is pressed, the door unlocks for a specified time. The REX switch must be a momentary contact, normally open switch rated greater than 0.5 mA, 5 VDC circuit.

A Door Switch monitors door status – open or closed. The door switch must be a normally closed switch rated greater than 0.5 mA, 5 VDC circuit.

Auxiliary Input requirements vary, depending upon the type of input device, but the input device should be rated greater than 0.5 mA, 5 VDC circuit.

Auxiliary Outputs

The HandPunch allows for the connection of up to three auxiliary output devices. Refer to the Outputs Wiring Diagram on page 35.

External Card Reader

You can connect an external card reader (such as a magnetic stripe, bar code, or proximity reader) to a HandPunch. This external card reader provides a secondary level of user identification.

!NOTE *The HandPunch may require special format programming to be able to read these external card reader formats. Contact your dealer for information.*

The connection to an external card reader is made through TS-3 on the HandPunch. Refer to the External Card Reader Wiring Diagram on page 37.

Serial Printer

You can connect a serial printer to a HandPunch. A serial printer connected to the HandPunch prints punches as they occur. Schlage Biometrics does not supply serial printers. The connection to a serial printer is made through J4, the 4 pin connector on the HandPunch. Refer to the Serial Printer Connection Diagram on page 41. Refer to the Printer String Information Application Note (available from Schlage Biometrics) for detailed information on connecting a serial printer to a HandPunch.

!NOTE *If you use the serial printer option you cannot use the RS-232 HandPunch network to host computer option (see page 18).*

This page is intentionally blank.

Mechanical Installation

Select an installation location based on the guidelines provided in the Planning an Installation section beginning on page 11.

Wall Plate Installation

NOTE *For the following instructions protect the HandPunch from the dust and debris generated during the wall plate installation process.*

1. Remove the wall plate from the packing carton. Refer to Figure 3-1 for all wall plate references in the following section.

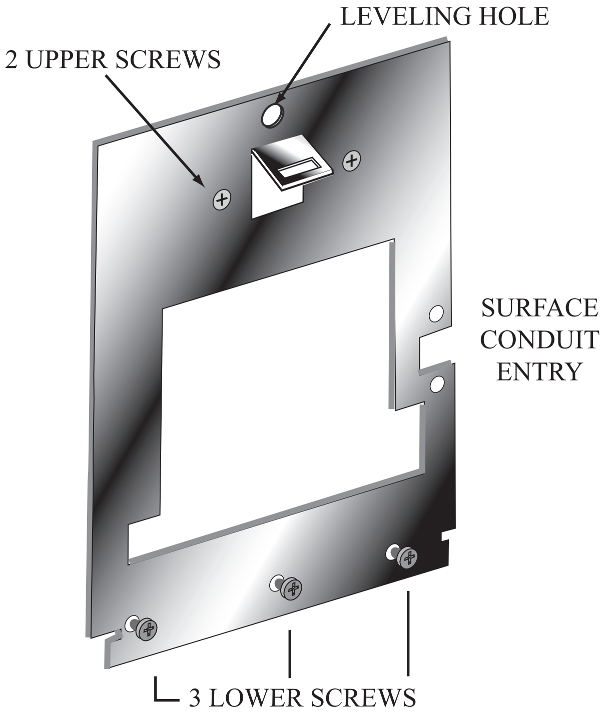


Figure 3-1: Wall Plate

2. Measure and mark a point 42 1/2 inches (123 cm) from the surface of the finished floor. This point will correspond to where the top-center point of the HandPunch should be mounted.
3. For a hollow wall, drive a small nail into the wll at the mark and hang the wall plate from the leveling hole located near the top of the wall plate.
4. For a solid wall, hold teh wall plate against the wall, centering the leveling hole over the mark in the wall.

5. Align a bubble level with the top edge of the wall plate and gently rotate the wall plate until the bubble level shows that the totp edge of the wall plate is level.
6. Secure the plate to the wall using heavy masking tape.
7. Using the wall plate as a template, mark the locations of teh two upper screw holes and the three lower screw holes.
8. For a concealed wiring connection, trace the outline of the open area in the center of the wall plate. Identify and mark a 1/2 inch hole through which the HandPunch's wiring will be mounted.
9. For a surface conduit wiring connection, mark the two conduit clamp holes at the right side of the wall plate.
10. Remove the wall plate, masking tape, and the nail (if used).

Mounting the Wall Plate

1. For a hollow wall, use the provided hardware to mount the wall plate. Use the two auger style fasteners for teh upper two mounting holes. Use the toggle bolts for the three lower mounting holes.
2. For a solid wall, use expansion bolts to mount the wall plate. For all five mounting holes, drill a 1/4 inch diameter hole, 1/4 of an inch deeper than the length of the expansion anchor.

Routing the Wiring

1. For a concealed wiring connection, drill a 1/2 inch hole in a convenient location within the open area of the wall plate. Pull the wiring to enter the HandPunch through this hole in the open area.
2. For a surface conduit wiring connection, drill a 1/4 inch diameter hole, 1/4 of an inch deeper than the length of the expansion anchor for each of the two conduit clamp holes. Route 1/2 inch conduit to the HandPunch, ending the conduit between the two conduit clamp holes. Pull the wiring to enter the HandPunch through the conduit.

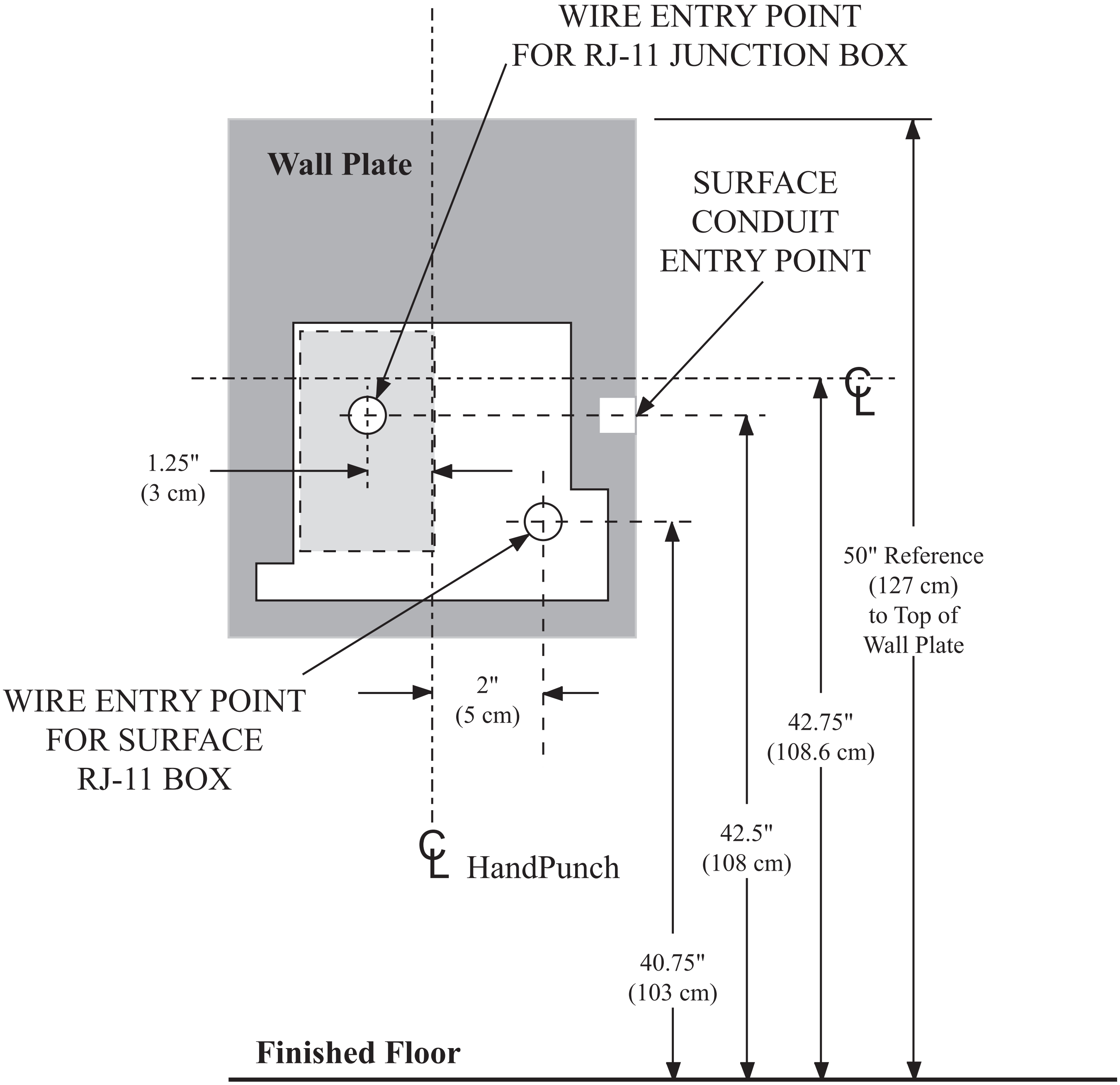
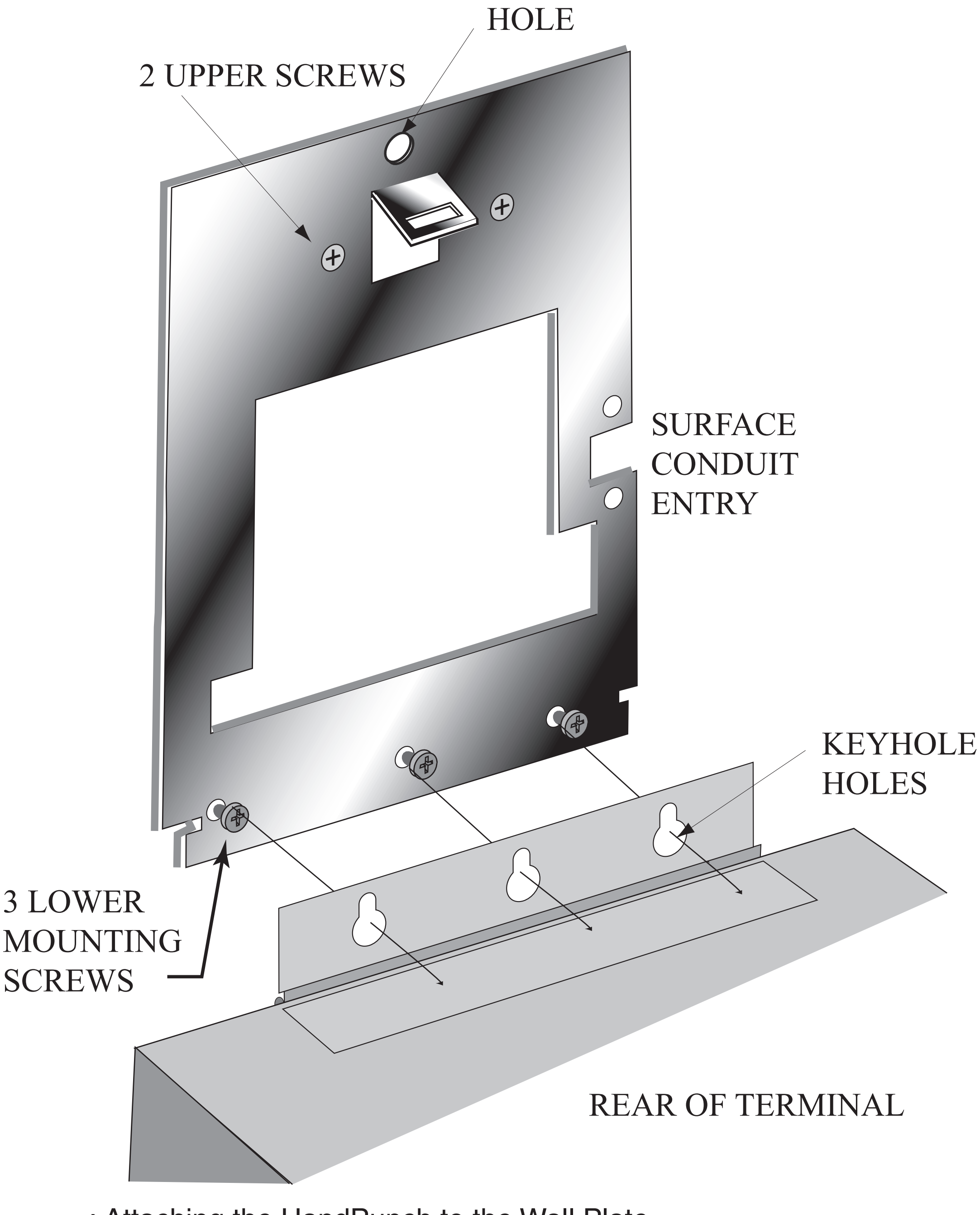


Figure 3-2: HandPunch Wire Routing Layout

Attaching the HandPunch

1. Remove the HandPunch from its carton.
2. Align the sleeves of the back plate with the pins of the wall plate and slide the HandPunch to the left as shown in “Figure 3-3” on page 26.



: Attaching the HandPunch to the Wall Plate

3. The Hand Punch is now ready for its wiring connections.

Networking and Communications

HandReader networking and communications can be configured in one of five ways:

- as a stand-alone HandReader
- as a master or remote HandReader in a HandReader network
- as a remote HandReader in a HandReader network connected to a host PC
- as a remote network connected via optional Modem to host PC
- as a remote network connected via optional Ethernet to host PC

Stand-alone HandReader

When installed as a stand-alone access control system there is no communication wiring to other HandReaders or to a host computer. Power input and control output wiring are all that are required. An RS-232 serial printer output is available for event logging (refer to the Printer section on 29). Schlage Biometrics highly recommends using Backhand™ software to backup template information stored in the HandReader.

Master or Remote HandReader in a HandReader Network

Multiple HandReaders can be linked together in a HandReader network.

- Up to 32 HandReaders can be linked together on a 2-wire RS-485 or 4-wire RS-422 network (see Figure 3-1).
- Two twisted-pair, shielded, AWG 22 (or larger) wire should be used (Schlage Biometrics recommends Belden 82732 or its equivalent).
- The wiring must be a “daisy-chain” network from HandReader to HandReader and must not exceed 4,000 feet (1220 meters) in total length.

The master/remote network requires user enrollment at the “master” HandReader. The master HandReader distributes hand template data with ID numbrs and time restrictions (if any) to the other HandReaders in the network. Users removed at the master HandReader are automatically removed from the remote readers. A printer connected to the master HandReader will report transactions from all Handreaders on the network.

Remote HandReader in a HandReader Network Connected to a Host PC

Multiple HandReaders can be linked to a presonal computer (PC) for an integrated access control network. Real time monitoring of door status and a variety of alarm types can be done with Schlage Biometrics’ HandNet for Windows™ (Schlage Biometrics model number HN-300) software. To run HandNet for Windows™, the computer must be PC compatible, using a Pentium™-166 or faster microprocessor and it must have a CD-ROM.

- The HandNet software can monitor over 1,000 HandReaders simultaneously.

- An unlimited number of sites can be created with up to 32 HandReaders per site.
- The HandReaders report all transactions to the PC. The HandNet software records all transactions and displays a variety of reports generated from this information.
- Template management is handled automatically.
- Users may enroll at any HandReader in the system. The PC collects the data and distributes it to other HandReaders in the network.
- Access may be restricted by time and by HandReader via HandNet's access profiles and by the use of time zones.

Typically, HandReader networks link to a PC using an RS-422 connection. These networks have the following requirements:

- Two twisted pair, shielded, AWG 22 wire or larger should be used (Schlage Biometrics recommends Belden No. 82723 or equivalent cable).
- HandReaders must be wired together in a "daisy-chain" network from HandReader to HandReader and then to the host PC. The total length of teh wiring must not exceed 4,000 feet per network.
- The network requires an RS-422 to RS-232 converter (Schlage Biometrics P/N DC-102) at the PC.

Schlage Biometrics' optional HandNet for Windows™ software allows programming of most of the remote HandReader setups from the computer. However, each HandReader on the network requires the setting of an address. HandReader addresses may be repeated, but **only** on different sites. Display language, date format changes, and the communication mode must also be set at the HandReader.

Remote HandReader Connected to a Host PC via Optional Modem

An optional internal "answer only" 14.4 bps modem is available for HandReaders. This modem is designed for operation with United States phone systems. Site wiring should conform to standard telephone wiring standards and terminate at teh HandReader with a standard RJ-11 modular phone jack. Each HandReader with a modem includes a XXXX cable for the final connection between the phone jack and the HandReader modem. Modem HandReaders may be networked with up to 31 non-modem HandReaders using RS-422 wiring. Refer to the Modem application note (available from Schlage Biometrics) for detailed information.

Remote HandReader Connected to a Host PC via Optional Ethernet

The HandReader is available with an optional internal Ethernet communications module for TCP/IP communications. The wiring must conform to 10BaseT standards. Typically, network wiring terminates at the HandReader with a standard RJ-45 modular jack. The cable from the jack to the HandReader is not provided with the Ethernet option. The IP address, Gateway, and Host Bits are entered at the HandReader in the SET SERIAL menu. Ethernet HandReaders may be networked with up to 31 non-Ethernet HandReaders using RS-422 twisted pair cable. Refer to the Ethernet application note (available from Schlage Biometrics) for detailed information.

Printer

A serial printer can be connected to a HandReader. A printer connected to a remote HandReader will print only the events that occur at that HandReader. Schlage Biometrics Inc. does not supply serial printers. Refer to the Printer String application note (available from Schlage Biometrics) for detailed information.

This page is intentionally blank.

Wiring Connections

Once the HandPunch is attached to the wall plate the wiring connections to the HandPunch can be made (see Figure 4-1).

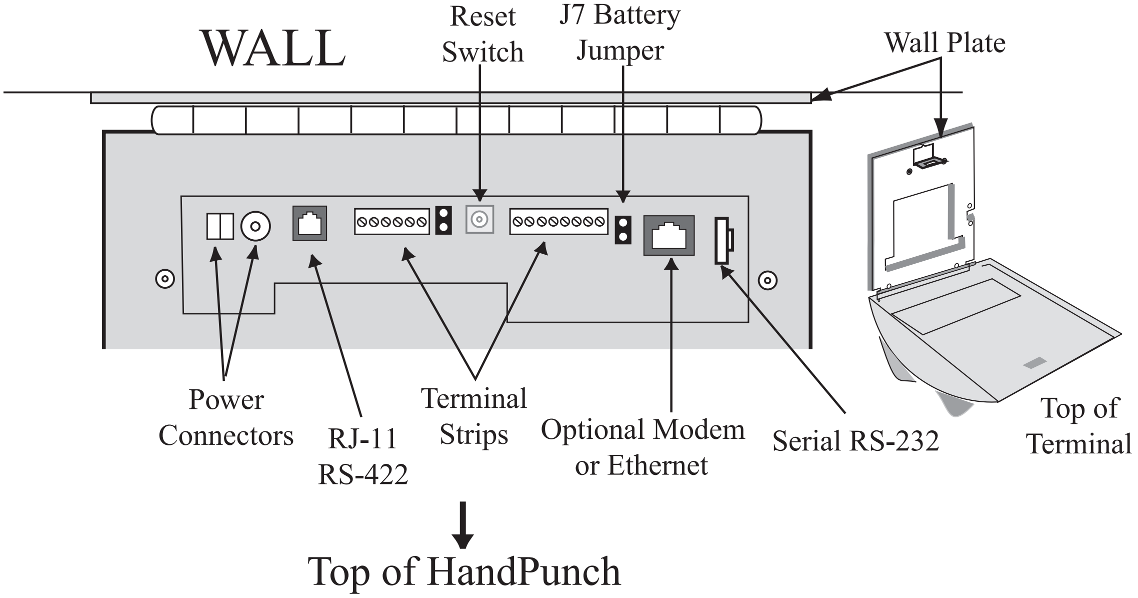


Figure 4-1: Wiring Connections

Wiring Examples

The following tables provide the pinouts for the terminal strips on the HandPunch.

- “Table 2” on page 32 provides the pinouts for TS-2: Input Connections.
- “Table 3” on page 32 provides the pinouts for TS-3: Card Reader and Output Connections.
- “Table 4” on page 33 provides the pinouts for the Serial RS-232 Connection.
- “Table 5” on page 33 provides the pinouts for the RS-422 HandPunch to HandPunch Network Connection.

The following figures provide the pinout diagrams for the RJ-11 and RS-232 connectors:

- “Figure 4-2” on page 33 provides the pinouts for J3, the RJ-11/RS-422 Network Configuration.
- “Figure 4-3” on page 34 provides the pinouts for J8, the RS-232 Serial Printer Connection.

The following figures provide typical HandPunch wiring diagrams.

- "Figure 4-4" on page 34 provides a typical Bell Output wiring diagram.
- "Figure 4-5" on page 35 provides a typical Lock Output wiring diagram.
- "Figure 4-6" on page 36 provides a typical Input wiring diagram.
- "Figure 4-7" on page 37 provides a typical Card Reader Emulation Mode wiring diagram.
- "Figure 4-8" on page 38 provides a typical Host PC Network System wiring diagram.
- "Figure 4-9" on page 39 provides a typical Ethernet Network wiring diagram.
- "Figure 4-10" on page 40 provides a typical Modem Network wiring diagram.
- "Figure 4-11" on page 41 provides a typical Printer to HandPunch wiring diagram.

Table 2: TS-2 - Input Connections

Terminal	Connection
9	Request to Exit Input
10	Ground
11	Door Monitor Switch Input (NC Standby)
12	Auxiliary Input 1
13	Ground
14	Auxiliary Input 2

Table 3: TS-2 - Output Connections

Terminal	Connection
1	+5 VDC @ 400mA Max. Output for External Card Reader
2	Card Reader: Wiegand D0 or Magnetic Stripe Data Input
3	Card Reader: Wiegand D1 or Magnetic Stripe Clock Input
4	Ground
5	Lock Output or Wiegand D1 or Magnetic Stripe Clock Output
6	Auxiliary Output 0 or Wiegand Data 0 or Magnetic Stripe Data Output
7	Auxiliary Output 1zt

Table 3: TS-2 - Output Connections

Terminal	Connection
8	Auxiliary Output 2

Table 4: RS-232 Connection

Pin	Signal	Connection
1	GND	Ground
2	RXD	Receive Data Input (from external device)
3	TXD	Transmit Data Output (to external device)
4	RTS	Ready to Send Output (to external device)

Table 5: RJ-11/RS-422 Network Connection

J3 Pin	Signal
1	Rx+
2	Rx-
3	Tx-
4	Tx+

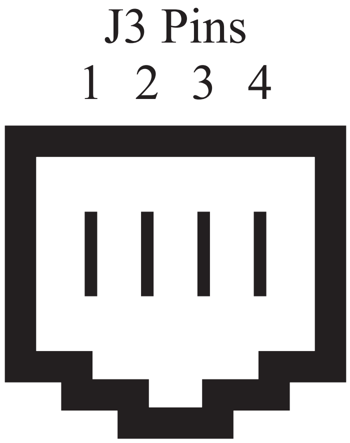


Figure 4-2: J3 - RJ-11/RS-422 Jack Pinout

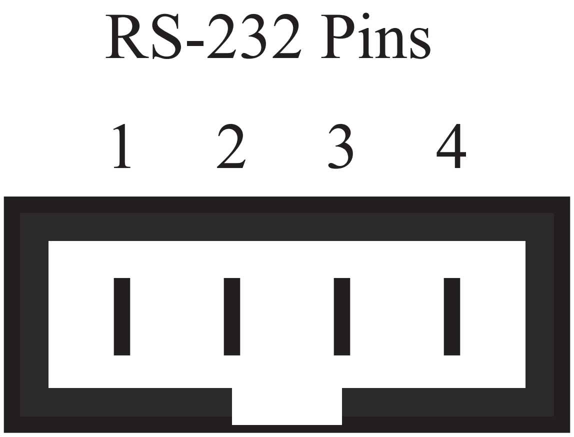
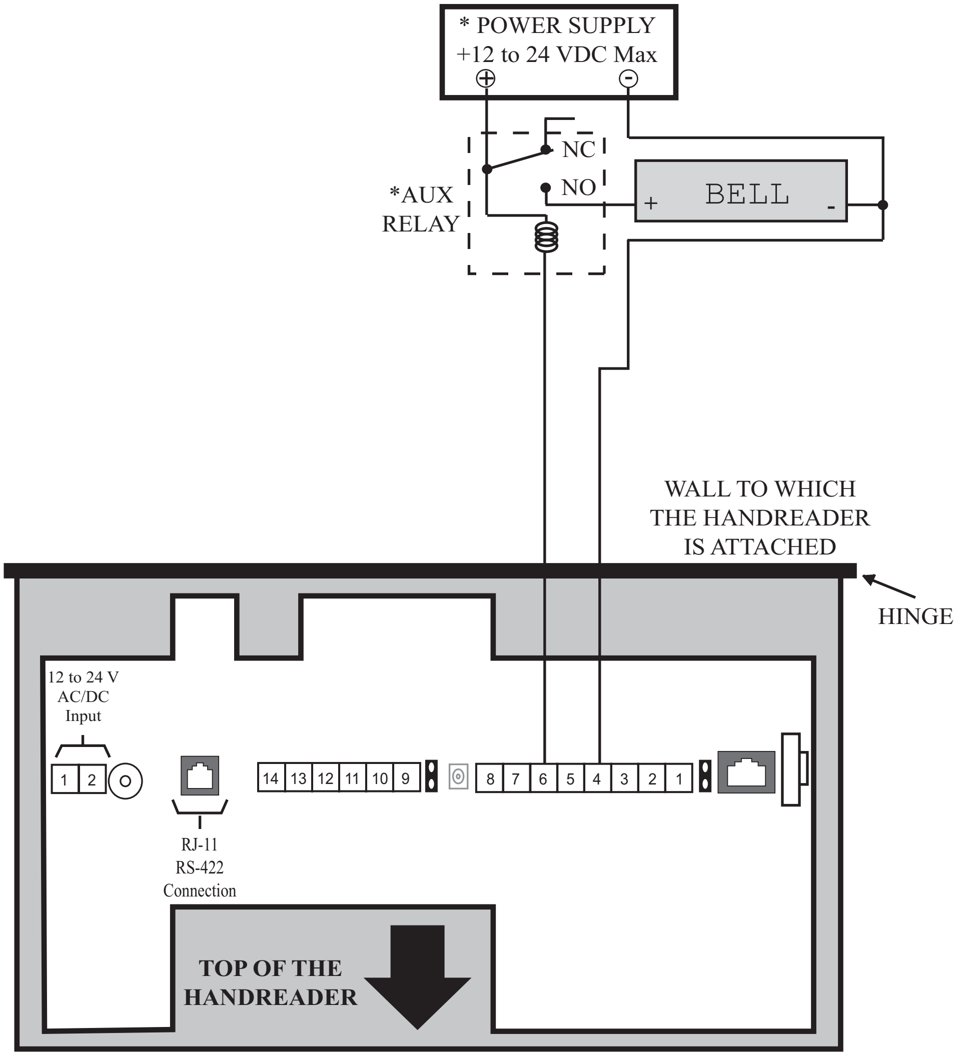


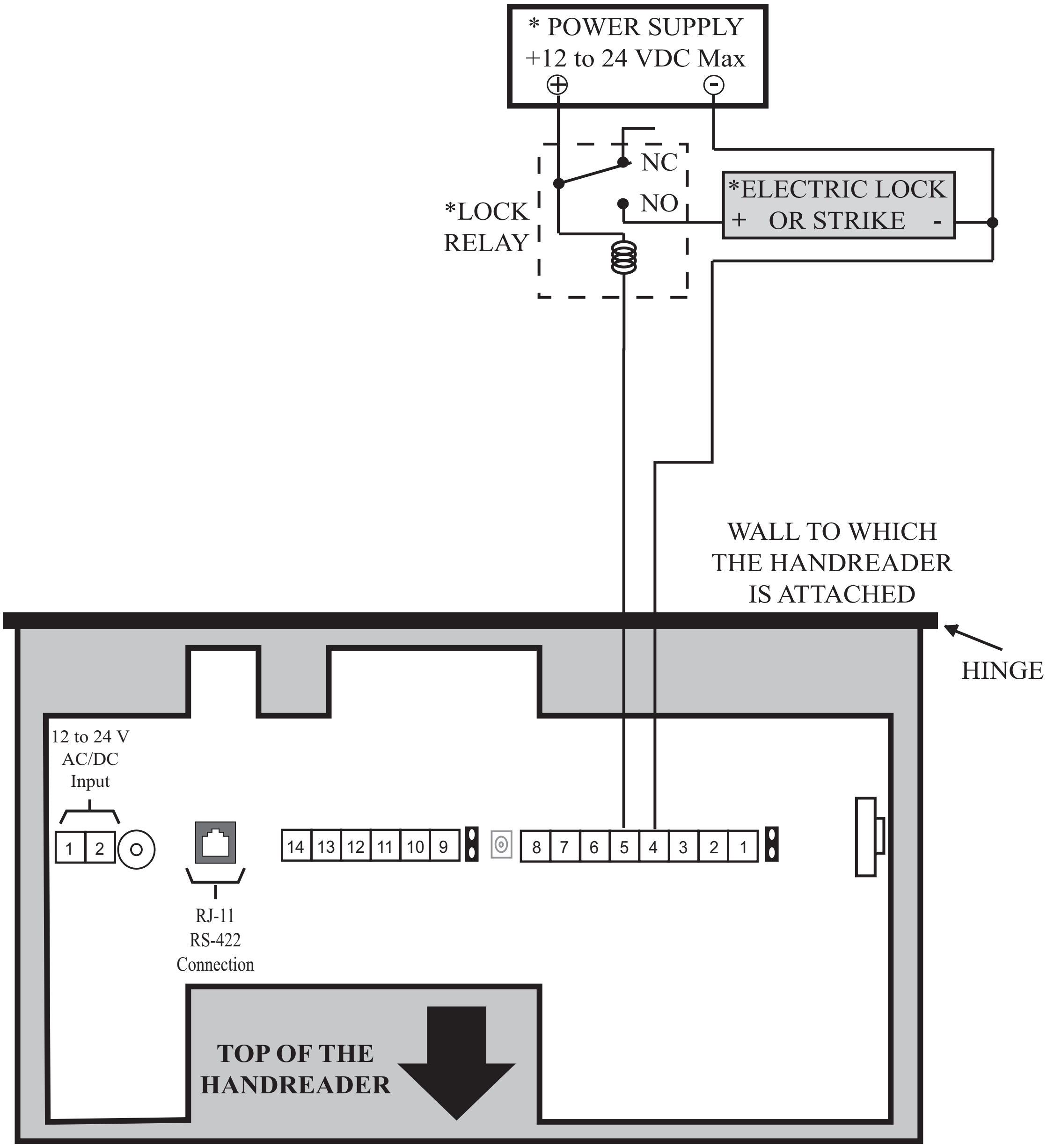
Figure 4-3: J4 - RS-232 Jack Pinout



* These components are not supplied by Recognition Systems, Inc.

** The operation of the Auxiliary Outputs depend upon how the inputs have been configured.

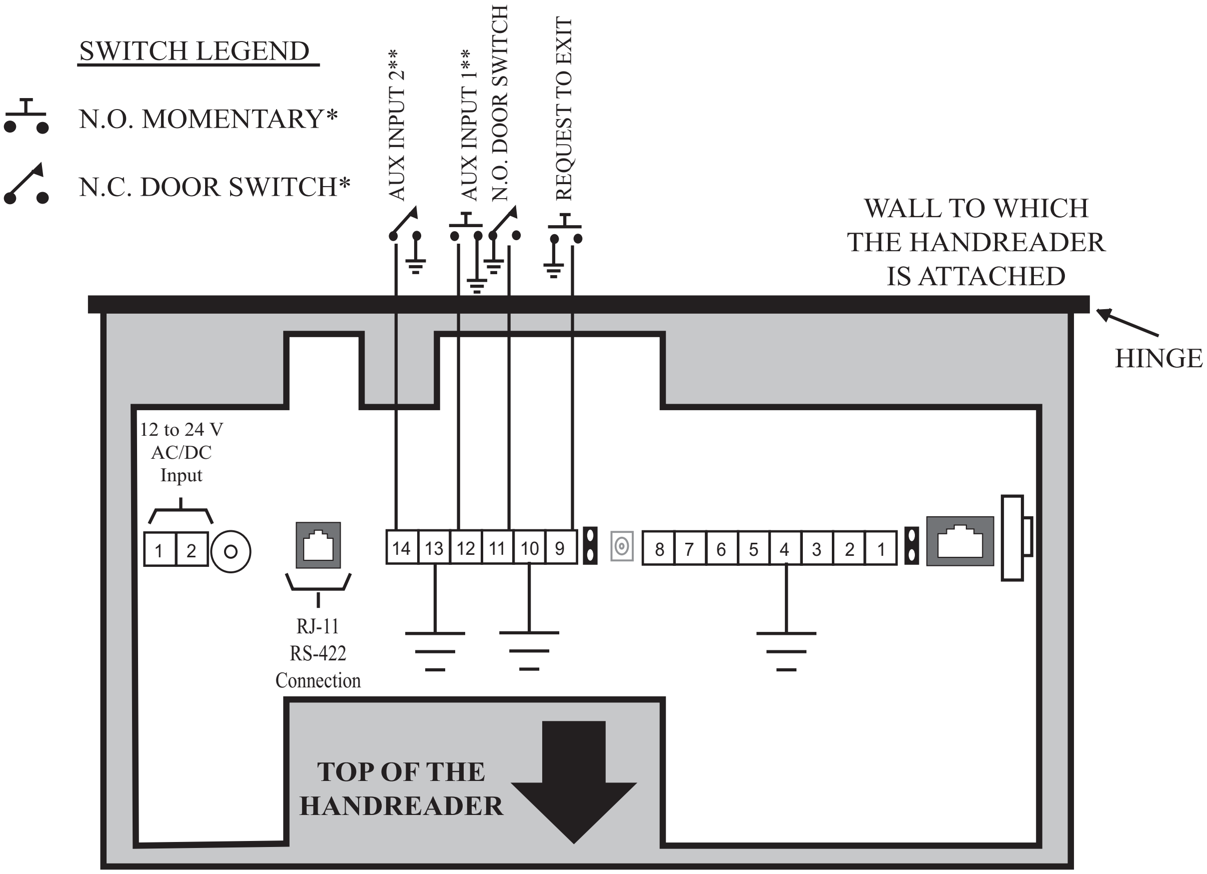
Figure 4-4: Bell Output Wiring Diagram



* These components are not supplied by Recognition Systems, Inc.

** The operation of the Auxiliary Outputs depend upon how the inputs have been configured.

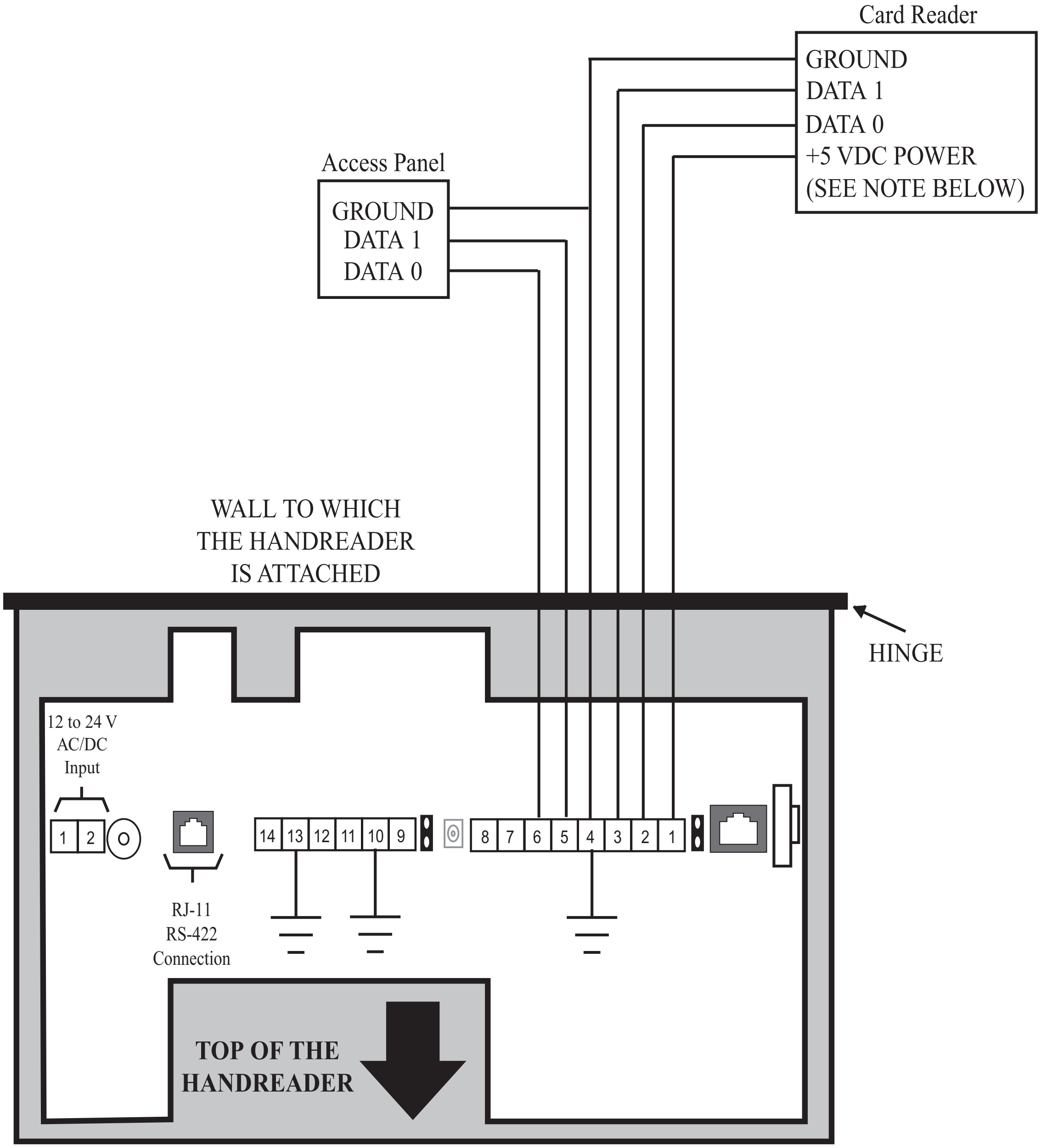
Figure 4-5: Lock Output Wiring Diagram



* These components are not supplied by Recognition Systems, Inc.

** The operation of the Auxiliary Inputs depend upon how the inputs have been configured.

Figure 4-6: Request to Exit, Door Switch, and Auxiliary Inputs Wiring Diagram



NOTE: For +12 VDC readers, connect power supply +12 VDC to card reader.

Figure 4-7: Card Reader Emulation Mode Wiring Diagram

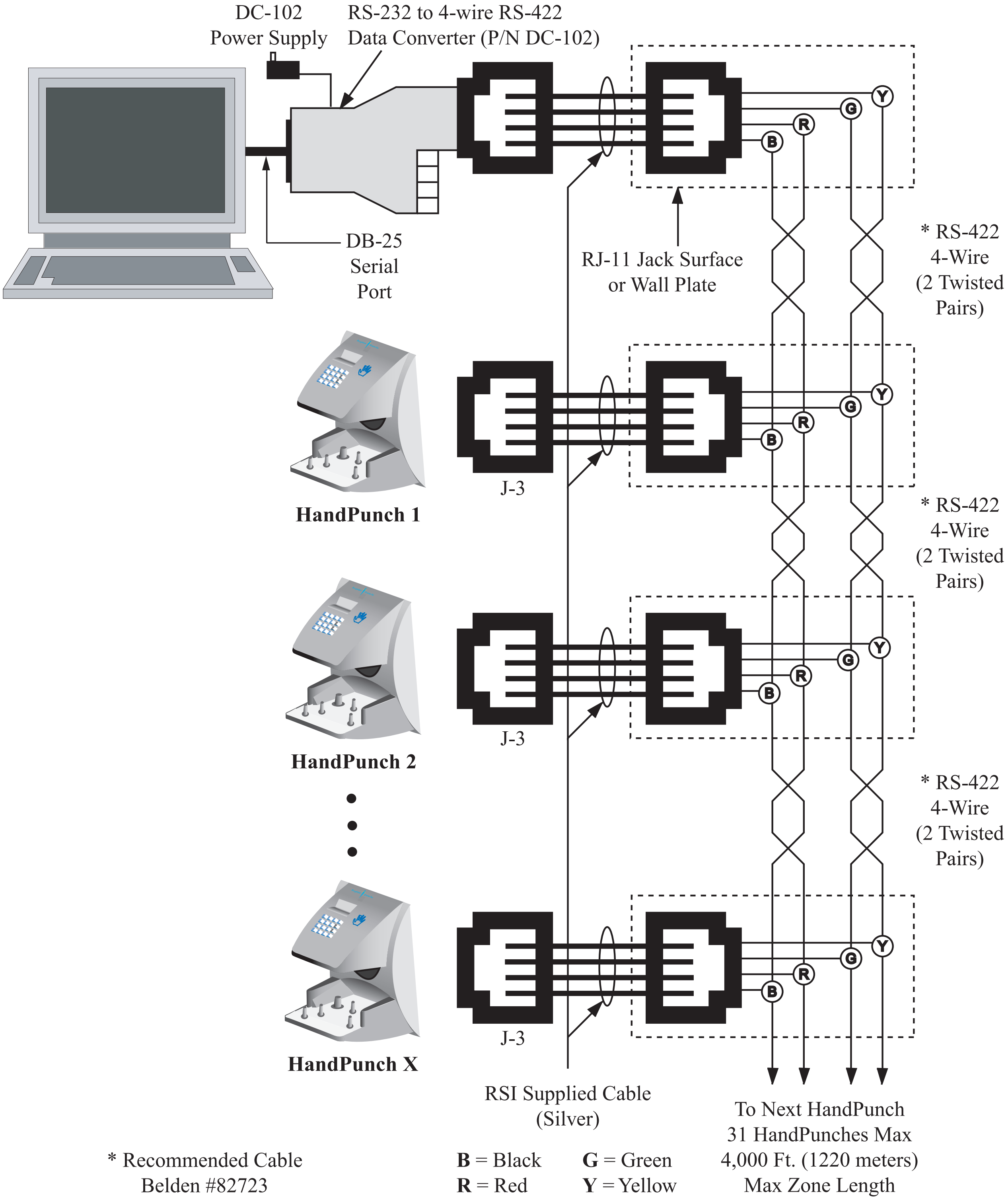


Figure 4-8: Host PC to RS-422 Direct-Connect Network System Wiring Diagram

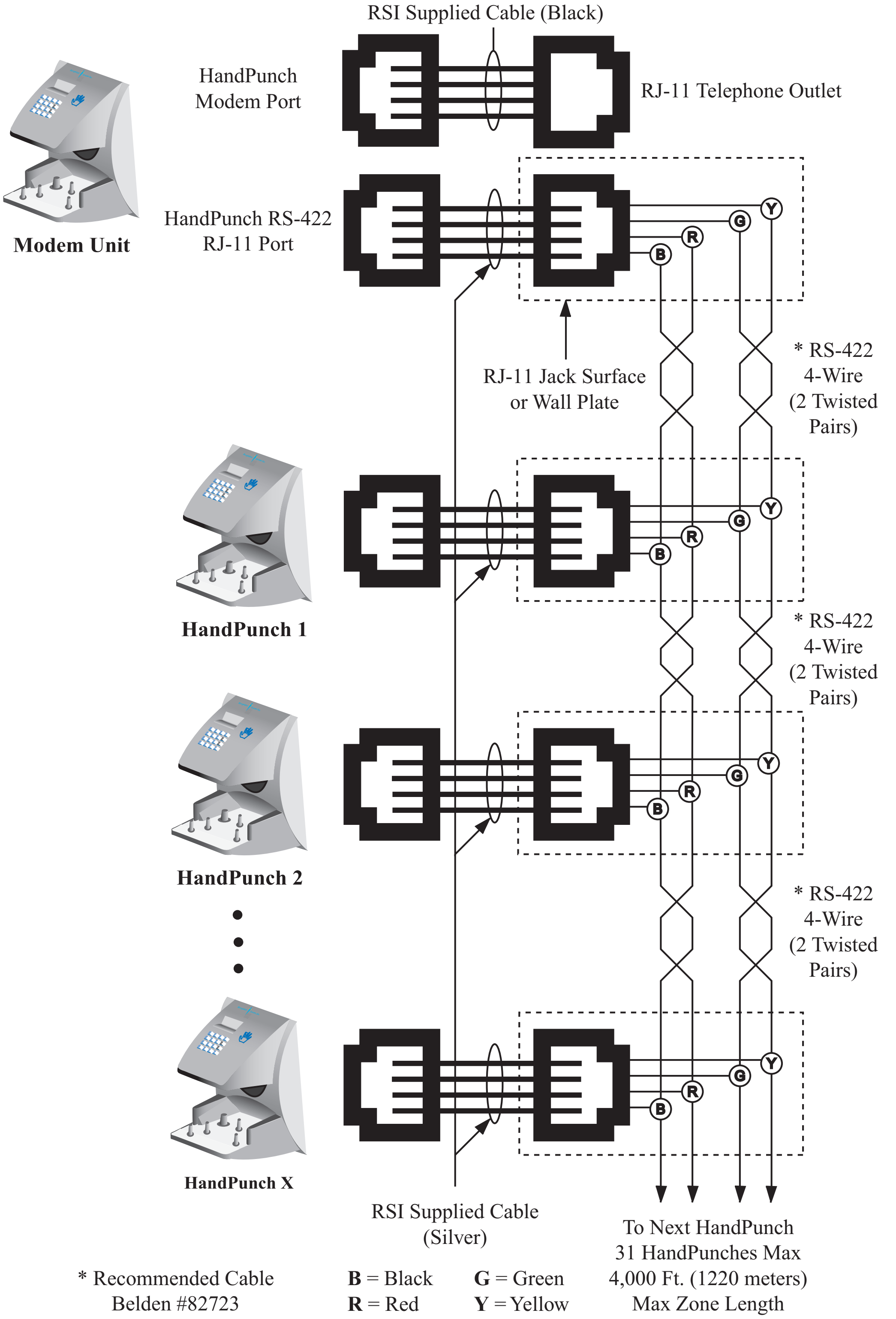


Figure 4-9: Host PC to HandPunch Ethernet Connection Diagram

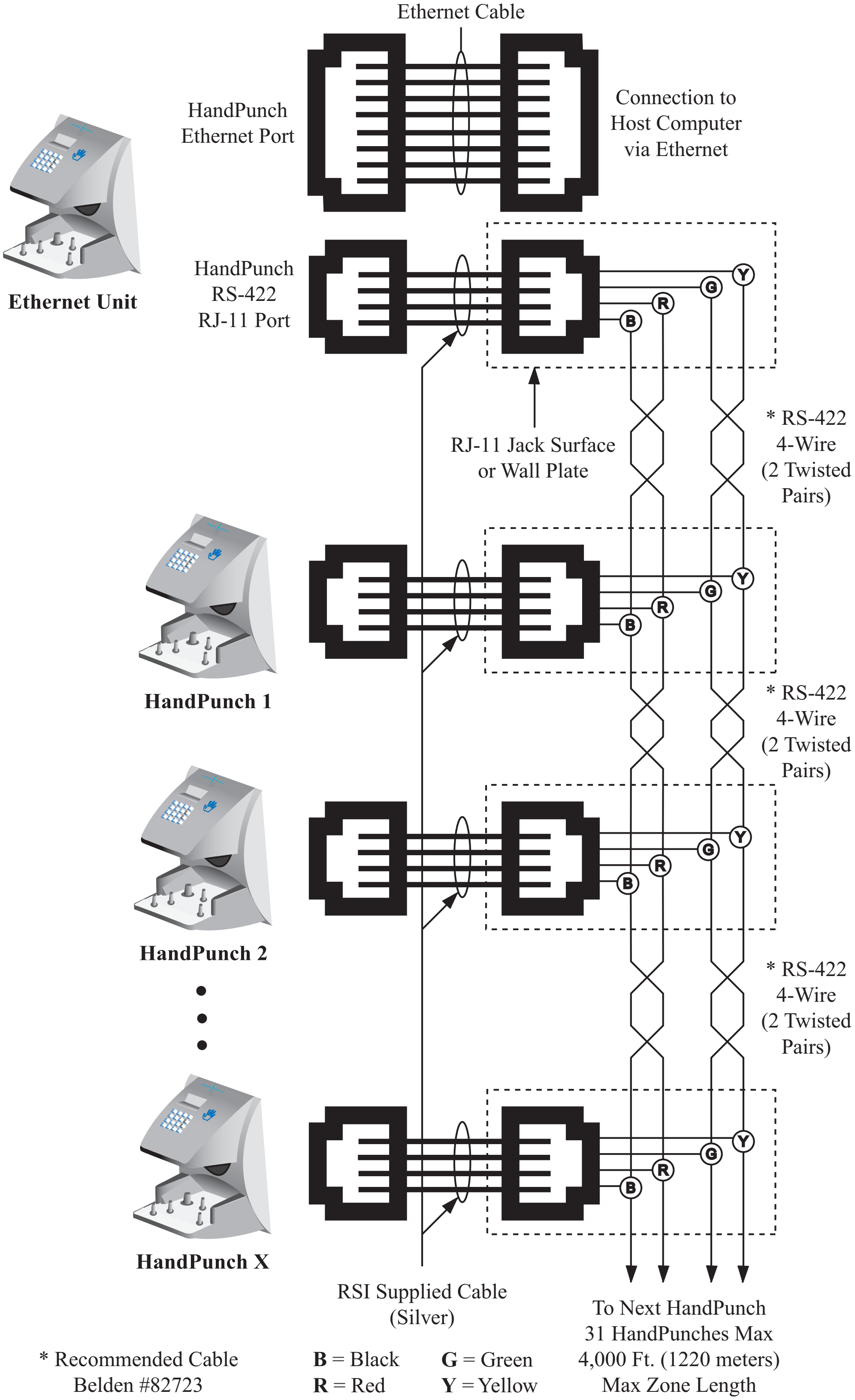
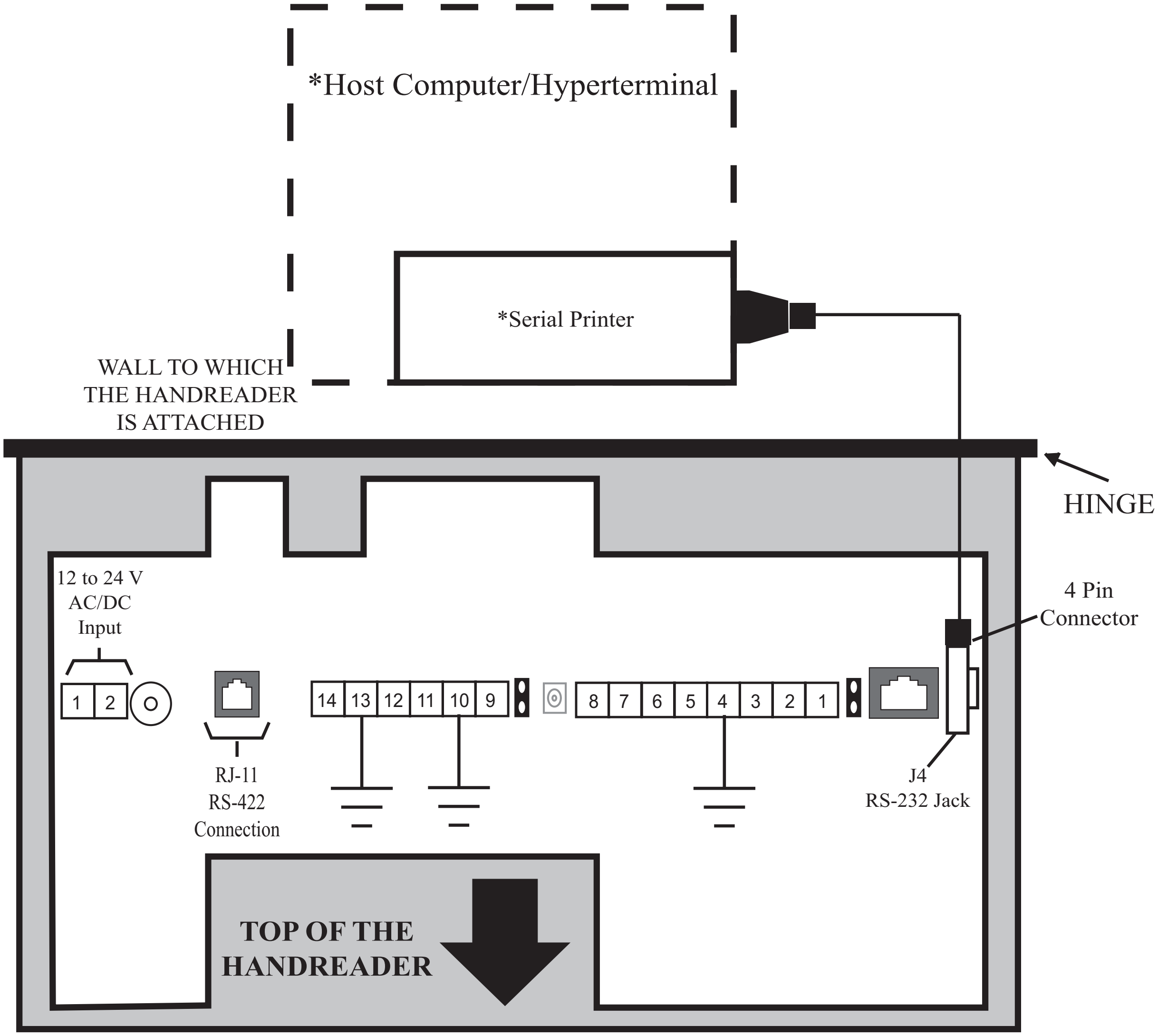

Ethernet Cable
HandPunch Ethernet Port
Connection to Host Computer via Ethernet
Ethernet Unit
HandPunch RS-422 RJ-11 Port
Y
G
R
B
RJ-11 Jack Surface or Wall Plate
* RS-422 4-Wire (2 Twisted Pairs)
HandPunch 1
* RS-422 4-Wire (2 Twisted Pairs)
HandPunch 2
* RS-422 4-Wire (2 Twisted Pairs)
HandPunch X
RSI Supplied Cable (Silver)
To Next HandPunch
31 HandPunches Max
4,000 Ft. (1220 meters) Max Zone Length
* Recommended Cable Belden #82723
B = Black
R = Red
G = Green
Y = Yellow

Figure 4-10: Host PC to HandPunch Modem Connection



* These components are not supplied by Recognition Systems, Inc.

Figure 4-11: HandPunch to Serial Printer or Host Computer Wiring Diagram

This page is intentionally blank.

Erasing the Memory

There are two options when erasing the memory of the HandReader:

1. Setup
2. All

The erasing of the setup will set the HandReader's address, passwords, etc., back to factory defaults.

Erasing HandReader Memory

Choosing the All option will take the HandReader's setup back to factory defaults plus erase all user databases and datalogs. This action cannot be undone. If there is a software that is managing the system then the users can be downloaded back to the HandReader if needed.

The erase memory function allows a HandReader's setup and/or user database to be erased.
Perform the following steps to erase the setup programs but retain the user database.

1. With system power OFF, depress reset switch.
2. Turn system power ON and wait 5 seconds.
3. LCD screen will display.

```
ERASE              :1 SETUP
                    :9 ALL!!!
```

This page intentionally blank.

Closing the HandPunch

Before closing the HandPunch clear all dust and debris away from the HandPunch. With the wal mount latch in the unlocked position, swing the body of the HandPunch up and lock the latch into place with the key provided with the HandPunch (see Figure 6-1 below).

Dust and debris surrounding the HandPunch can drastically affect the terminal's operation. It is important to ensure the HandPunch is free from dust and debris before closing the terminal.

Do not force the HandPunch onto the wall mount latch when the latch is in the locked position.

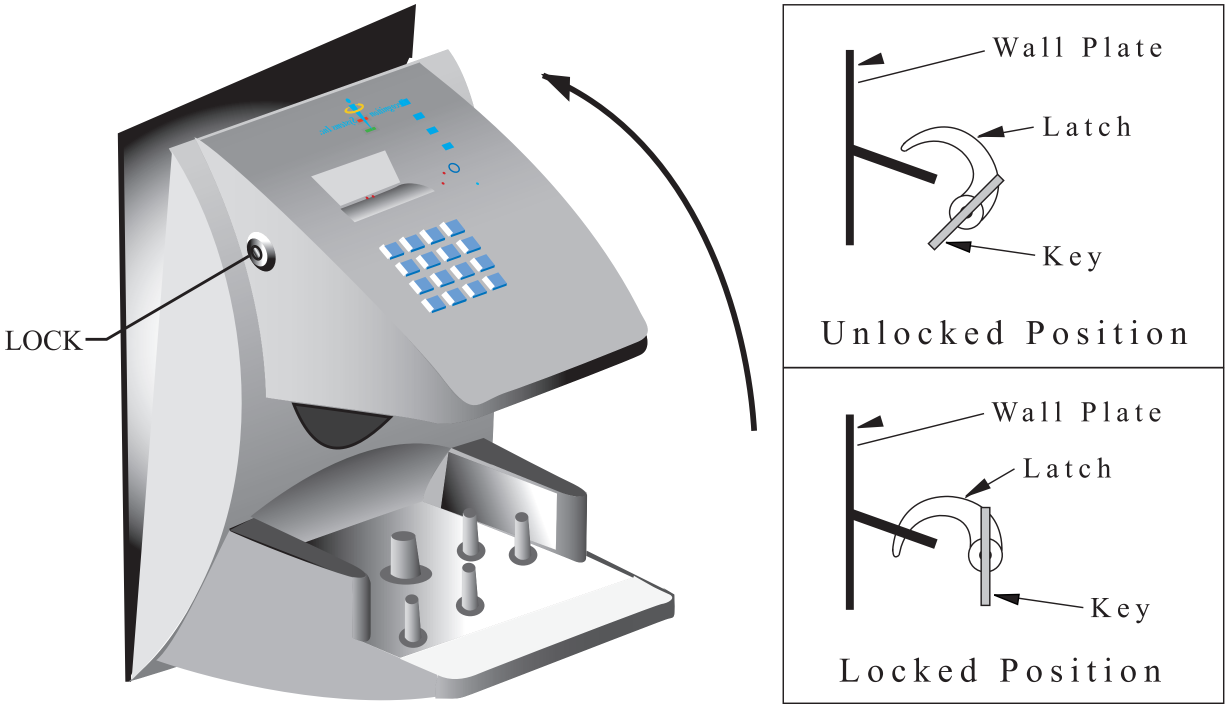


Figure 6-1: Closing the HandPunch

This page intentionally blank.

Enter Command Menu

Press the CLEAR and ENTER keys simultaneously to enter a command menu.

If No One is Enrolled in the HandPunch

1. The display appears as follows:

```
ENTER PASSWORD
```

2. Press the default password for the menu you wish to enter.

Press 1 for the Service Menu.
Press 2 for the Setup Menu.
Press 3 for the Management Menu.
Press 4 for the Enrollment Menu.
Press 5 for the Security Menu.

3. Press ENTER and the first command option in the selected menu appears.

If Users are Enrolled in the HandPunch

1. The display appears as follows.

```
ENTER ID
*:
```

2. Enter your ID number on the keypad and place your hand on the platen for verification.
3. If verification is successful, the display appears as follows.

Enter Password

4. Enter the password for the menu you wish to enter. The default passwords are as follows:

Press 1 for the Service Menu.
Press 2 for the Setup Menu.
Press 3 for the Management Menu.
Press 4 for the Enrollment Menu.
Press 5 for the Security Menu.

5. Press **ENTER**
6. If you are authorized to use this command, the first command option in the selected menu appears.
7. If you are not authorized to enter this command, the display appears as follows:

ENTER ID
***:**

NOTE *To access these menus you must be the first person enrolled in a new system installation or you must have been enrolled as a supervisor. If you are blocked from the supervisory menus, verify your access rights with management personnel. If enrollment information has been incorrectly changed and you must have supervisory access to all menus, make these changes through software.*

NOTE *It is possible to physically reset the HandPunch's memory, however resetting memory sets all unit parameters back to the factory default values. Resetting memory allows access to all menus by the first person enrolled (as if it is a new system installation), but this means that* ***all employee information programmed into the HandPunch is lost and must be re-entered manually.*** *Be sure you need to reset memory before performing this function. To reset memory, refer to the Erasing HandPunch Memory section on page 43.*

Navigating Command Menus

Once you have entered a command menu, there are three options available for navigating the command menu system

- Press # to enter the command shown on the display.
- Press * to step to the next command in the menu.
- Press **CLEAR** to exit the command menu (pressing any numeric key also exits the command menu). If you are in a command's sub-menu, you may have to press **CLEAR** multiple times to completely exit the command menu.

This page is intentionally blank.

Programming the HandPunch

The HandPunch is programmed via a series of command menus. A summary of the menus and commands is given in Table 6.

Table 6: Basic Command Mode Structure

Service Menu	Setup Menu	Management Menu	Enrollment Menu	Security Menu
Password 1	Password 2	Password 3	Password 4	Password 5
Calibrate	Set Language	Supervisor Override	Add Employee	Special Enroll
Status Display	Set Date Format	List Users	Add Supervisor	
	Set Time and Date	Set User Data	Remove User	
	Set Address	Restrictions		
	Set ID Length			
	Set Serial			
	Set Reader Mode			
	Upgrade			

To control access to the command menus, each menu has a unique password. This password is requested as a part of the process for accessing each menu. A supervisor must enter the correct password for that menu to access that menu. The default menu passwords are given in Table 6.
To increase the security of the HandPunch, Schlage Biometrics recommends changing the passwords for the command menus to new numbers. These password numbers can be up to 10 digits long. This is done with the Set Passwords command described on.

Authority Level

A second method for controlling access to the command menus is through the use of Authority Levels. Authority Levels control whether or not a user has access to the command menus.

- Level 0 is for a user who does not need access to any of the command menus.
- Level 5 is assigned to Supervisors who need access to all of the command menus.

The HandPunch automatically assigns Authority Level 0 to users enrolled by the Add Employee command. Authority Level 5 is automatically assigned to users enrolled by the Add Supervisor command.

NOTE *Until a user has been assigned to Supervisor, every user can access every menu. Once a user has been enrolled using the Add Supervisor (designated as a supervisor), all further user authority levels are assigned. The first person enrolled should be enrolled using the Add Supervisor command. This protects the integrity of the system. Schlage Biometrics strongly recommends enrolling at least two users as supervisors to ensure that more than one person has the authority to access all menus and all commands.*

Programming Order

When setting up HandPunch operations there is a general programming/ operations order that should be followed.

Set HandPunch Site Parameters – Set the HandPunch site parameters to meet site-specific needs and usage: change the language used by the display, set the HandPunch's address, and set the serial communication baud rate (used if you have installed a serial printer – see page 56).

Enroll Supervisory Staff – Enroll yourself and the supervisors who will have responsibility for HandPunch management. This is done through the Enrollment Menu (see Supervisor Enrollment on page 66).

NOTE *The time, date, and ID number length are normally set by the host computer. However, a supervisor can change these parameters at a HandPunch after setup information has been downloaded from the host computer.*

These tasks are done through the Setup Menu. The instructions for reader setup parameters begin on page 56.

Train and Enroll Users – Train each user regarding HandPunch usage and then Enroll each user. This is done through the Enrollment Menu. The instructions for employee enrollment begin on page 66. Special enrollment allows you to enroll people with disabilities that prevent them from using the HandPunch properly. Employees with special enrollment ID numbers can punch in without biometric verification.

WARNING *This means that anyone who knows a special enrollment ID number can punch in. This function should only be used if absolutely necessary. The instructions for special enrollment begin on page 68.*

System Management

Onca a HandPunch system is in operation the following commands are used for system management.

Supervisor Override – Review employee punch history, add bulk hours or dollars, or record a punch for an employee. This is done through the Management Menu. The instructions for supervisor override begin on page 61.

List Users – List the users authorized to use a HandPunch. This is done through the Management Menu. The instructions for listing employees begin on page 62.

Set User Data – Set a user's reject threshold (adjusting the sensitivity applied when a HandPunch reads a hand) and assign time zones to users (defining when users are allowed to punch in and out). These tasks are done through the Management Menu. The instructions for setting user data begin on page 62.

Restrictions – Set or remove time restrictions for when employees punch in. This is doen through the Management Menu. The instructions for setting in time restrictions begin on page 62.

Remove User – Remove employees (and supervisors) from a HandPunch. This is done through the Enrollment Menu. The instructions for removing employees begin on page 66.

Set Amnesty[1] – Temporarily remove time resrictions at a HandPunch to accommodate circumstances that may affect when employees punch in (such as inclement weather). This is done through the Management Menu. The instructions for setting amnesty begin on page 62.

[1] On HandPunch 4000 units only.

Service Menu

The Service menu commands provide information that help you determine if the HandPunch is performing within normal operating parameters and identify the status of the unit's inputs and outputs. The following section provides a brief summary of the Service Menu commands.

NOTE *There are no user serviceable parts inside the HandPunch.*

Navigating the Service Command Menu

Enter the appropriate password to enter the Service command menu. Once you have entered the command menu, there are three options available for navigating the command menu system.

- Press # to enter the command shown on the display.
- Press * to step to the next command in the menu.
- Press **CLEAR** to exit the command menu (pressing any numeric key also exits the command menu). If you are in a command's sub-menu, press **CLEAR** multiple times to completely exit the command menu.

Service Commands

There are two commands available from the Service command menu.

- Calibrate
- Status Display

Refer to Table 7 and identify the command you need to perform. Step through all previous commands until you reach the desired command.

Table 7: Service Command Menu

Service Menu
Password = 1
Calibrate
Recal (Y/N)
Status Display
On/Off (Y/N)

Calibrate The Calibrate command displays the HandPunch’s exposure values, allowing you to verify these values are within normal operating parameters. The standard operating parameters are shown in Table 8.

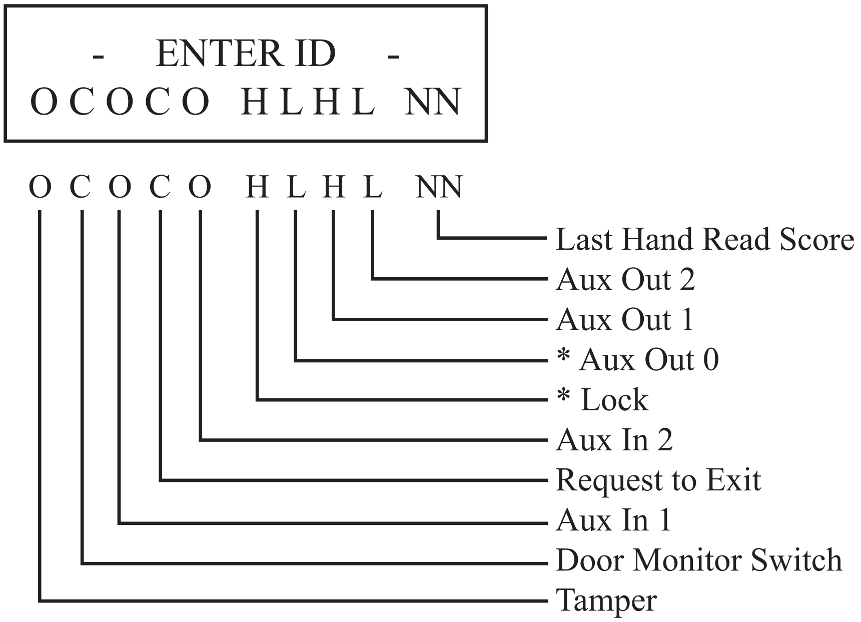
Table 8: Normal Operating Parameters

Parameter	Normal Range
Row “r”	0 +/- 2
Column “c”	0 +/- 2
Exposure “e”	100 +/- 20

Status Display The status display command allows you to enable or disable the displaying of the following information.

- the status values of HandPunch inputs and outputs
- the hand read score of the last user to verify on the system

When the status display is enabled, Figure 8-1 identifies each status display field value.



* These status values are inactive if the reader is in Card Reader Output Mode.

O = Circuit Open H = Output is OFF (High)
C = Circuit Closed L = Output is ON (Low)

Figure 8-1: Status Display Chart

Setup Menu

The Setup menu commands allow you to set the basic operating parameters for the HandPunch unit. The following section provides a brief summary of all the parameters that may be set on a HandPunch unit.

!NOTE *Once in the Command Menu, you can step through and set the parameters for each command sequentially. You do not have to exit command mode after setting any individual command.*

Navigating the Setup Command Menu

Enter the appropriate password to enter the Setup command menu. Once you have entered the command menu, there are three options available for navigating the command menu system.

- Press # to enter the command shown on the display.
- Press * to step to the next command in the menu.
- Press **CLEAR** to exit the command menu (pressing any numeric key also exits the command menu). If you are in a command's sub-menu, press **CLEAR** multiple times to completely exit the command menu.

Setup Commands

There are six commands available from the Setup command menu:

- Set Language
- Set Date Format
- Set Date and Time
- Set Address
- Set ID Length
- Set Serial
- Set Output Mode

Refer to "Table 9" on page 57 and identify the command you need to perform. Step through all previous commands until you reach the desired command.

Table 9: Setup Command Menu

Setup Menu
Password = 2
Set Language
Select Language
Set Date Format
Select Date Format
Set Time and Date
Month (MM)
Day (DD)
Year (YY)
Hour (HH)
Minute (MM)
Set Address
New Address
Set ID Length
New ID Length
Set T & A Mode
Set Serial[a]
RS-422 (Y/N)
Select Baud Rate
RS-232
Select Baud Rate
Use RS-232 for Printer or Host

Table 9: Setup Command Menu

Setup Menu
Password = 2
Set Serial[a]
Verify/Enter IP Address
Verify/Enter Gateway
Verify/Enter Host Bit
Set Output Mode
For Lock & Auxiliary (Y/N)
For Card Reader Output (Y/N)
Upgrade
Code

a. The Set Serial command has different values based on whether the HandPunch unit is configured for serial or modem communication versus Ethernet communication.

Set Language The Set Language command allows the language shown on the HandPunch's display to be "localized" for a variety of countries:

- English
- Japanese
- French
- Italian
- Spanish
- German
- Russian
- Indonesian
- Portuguese
- Polish

Set Date Format The Set Date Format Command allows the date format shown on the HandPunch's display to be "localized" for a variety of countries.

- mm/dd/yy
- dd-MMM-yy
- dd-mm-yy
- dd/mm/yy
- mm-dd-yy
- MMM dd,yy
- ddMMMyyyy

Set Time and Date The Set Time and Date command allows the HandPunch's time and date to be set. This is normally not necessary as the HandPunch's time and date are set by the host computer.

Set Address

The Set Address command allows a unique address to be set for each HandPunch in a network. For proper operation, each HandPunch in the network must have a unique address. All units may use any address from 0 to 254. All units are sent with the address set to 1.

Set ID Length

The Set ID Length command allows you to reduce the number of keystrokes required to enter the ID number by eliminating the use of the **ENTER** key to complete an ID number entry. Once the ID Length is set, the HandPunch will automatically accept an ID number entry once the correct number of characters have been entered.

Set ID Length does not apply when ID entry is made from a card reader. Once the ID Length is set, the T & A Mode Set command appears, allowing you to configure the HandPunch to prepare punch data for time and attendance software.

Set Serial

The Set Serial command allows you to set communication parameters depending upon the communication method for which the HandPunch has been configured. Different configuration parameters are entered based on if the unit is configured for a direct-connection or a modem connection, or if the unit is configured for Ethernet communication.

The unit defaults to the RS-422 communication mode unless a modem or Ethernet module has been installed. The unit defaults to 9600 bps which is suitable for most communication applications.

If an Ethernet module has been installed, the IP Address and Gateway and Subnet Mask must be set. The host bits should be left at 0, if communicating across a LAN.

Set Output Mode

The Set Output Mode command allows you to set how the output relays operate. The relays should be set based on the HandPunch application.

Set the HandPunch to Lock/Auxiliary Relay mode if the unit is acting as door controller (this is the factory default setting).
Set the HandPunch to Card Reader Emulation mode if the unit is outputting to an access control panel.

Upgrade

This Upgrade Menu is where the HandPunch code gets input to allow for a Memory Upgrade.

Management Menu

The Management menu commands allow you to manage employee data stored in a HandPunch unit. The following section provides a brief summary of the employee data that may be manipulated on a HandPunch unit.

Enter the appropriate password to enter the Setup command menu. Once you have entered the command menu, there are three options available for navigating the command menu system.

- Press # to enter the command shown on the display.
- Press * to step to the next command in the menu.
- Press **CLEAR** to exit the command menu (pressing any numeric key also exits the command menu). If you are in a command's sub-menu, press **CLEAR** multiple times to completely exit the command menu.

There are four commands available from the Management command menu.

- Supervisor Override
- List Users
- Set User Data
- Restrictions

Refer to Table 10 and identify the command you need to perform. Step through all previous commands until you reach the desired command.

Table 10: Setup Command Menu

Setup Menu
Password = 3
Supervisor Override
Review
ID #
Add
Bulk Hours
Bulk Dollars
Punch

Table 10: Setup Command Menu

Setup Menu
Password = 3
List Users
Display
Print
Set User Data
User Reject
User Time Zone
Amnesty
Set Restrictions
On/Off (Y/N)

Supervisor Override

The Supervisor Override command allows you to review an employee’s punch record, add or remove bulk hours or dollars to an employee’s punch record, or add a new punch to an employee’s punch record (see “Table 11” on page 62 for a description on Punch Type codes).

Table 11: Punch Type Information

T & A Code	Type
1	IN
2	Back From Lunch
3	Out
4	Department Code
5	Back From Break
6	-not used-
7	Called Back to Work
8	Supervisor Entered Hours
9	Supervisor Entered Dollars
15	Supervisor Entered Category

List Users

The List Users command allows you to display or print a list of all the employees enrolled in a HandPunch.

Set User Data

The Set User Data command allows you to set an employee's Reject Threshold (adjusting the hand read threshold for one employee without affecting the threshold of other employees), set an employee's Time Zone (the hours an employee is allowed access), and set employee Amnesty (removing time zone restrictions for a specified number of punches – available on the HP-4000 only).

Restrictions

The Restrictions command allows you to enable or disable employee punch time restrictions, allowing or disallowing punches outside an employee's assigned time zone.

Enrollment Menu

Enrollment is the process of recording a hand image and associating it with an ID number. The first person to enroll in the HandPunch has access to all command menus. This person should enroll using the Add Supervisor command (see page 66). Once a supervisor has been enrolled, all further enrollments use the following rules:

- A user enrolled through the Add Employee command (page 66) is assigned Authority Level 0. This allows the user to punch in and/or gain access through a door secured by the HandPunch.
- A user enrolled through the Add Supervisor command (see page 66) is assigned Authority Level 5. This allows the supervisor to punch in and gain access through a door secured by the HandPunch, and it allows the supervisor to access all command menus.

! NOTE *Until a user has been assigned to Authority Level 5 using the Add Supervisor command, every user with Authority Level 0 can access every menu. This is done to ensure that the first person enrolled is able to access all the menus to perform all the programming required to support the HandPunch. Once a user has been enrolled using the Add Supervisor command, all further user authority levels are assigned as per the list above. This protects the integrity of the system by enacting the Authority Level rules described above. Schlage Biometrics strongly recommends enrolling at least two users as supervisors to ensure that more than one person has the authority to access all menus and all commands.*

Navigating the Setup Command Menu

Advance planning and training make enrollment fast and easy. Users should be informed on what to expect and how to place their hands on the HandPunch before you enroll them.

Enter the appropriate password to enter the Setup command menu. Once you have entered the command menu, there are three options available for navigating the command menu system.

- Press **#** to enter the command shown on the display.
- Press **#** to step to the next command in the menu.
- Press **CLEAR** to exit the command menu (pressing any numeric key also exits the command menu). If you are in a command's sub-menu, press **CLEAR** multiple times to completely exit the command menu.

Preparation

Here are a few guidelines to help you prepare for an enrollment session:

- You can enroll one person or a group of people during an enrollment session.
- Each user must have a unique personal identification (ID) number. It will save you considerable time if you assign the ID numbers in advance (Refer to the Design an ID Numbering System section on page 47).
- The HandPunch will not accept two people with the same ID number.
- If you enroll people using the last four digits of their phone numbers or social security numbers, you may get duplicate numbers.
- If you are enrolling large groups of people you may consider using an enrollment trainer. It is a replica of a platen that is available through your Schlage Biometrics reseller.

User Education

The HandPunch is easy to use and non-threatening. However, most people have never used a biometric HandPunch. Training users on how the HandPunch works and how to use it will eliminate most fears and concerns before they occur. Inform the users of these facts.

- The HandPunch reads the shape of the hand, not the fingerprints or palmprints.
- It does not identify people. It confirms people's identity.
- It scans with an invisible light of the type used in TV remote controls.
- It does not transfer germs any more than a doorknob or money.
- It does not invade privacy; it guarantees it.
- The enrollment process requires three or more reads to collect enough information to create a template.

Proper Hand Placement

For correct, consistent hand reads it is very important that your hand is placed on the platen in the same manner every time. The following rules apply for proper hand placement on the platen also refer to "Figure 8-2" on page 65.

- If you are wearing a ring, rotate the ring so the stone faces up in its normal position.
- Slide your right hand onto the platen rather like an airplane landing at the airport.
- Slide your hand forward until the web between your index and middle finger stops against the Web Pin.
- Keep your hand flat. You should feel the surface of the platen on your palm and the underside of your fingers.
- Close your fingers together until they touch the Finger Pins and watch the hand diagram light display on the top panel.
- The lights go out when you have properly placed your fingers. If a light remains on, a finger is not in proper contact with its Finger Pin.

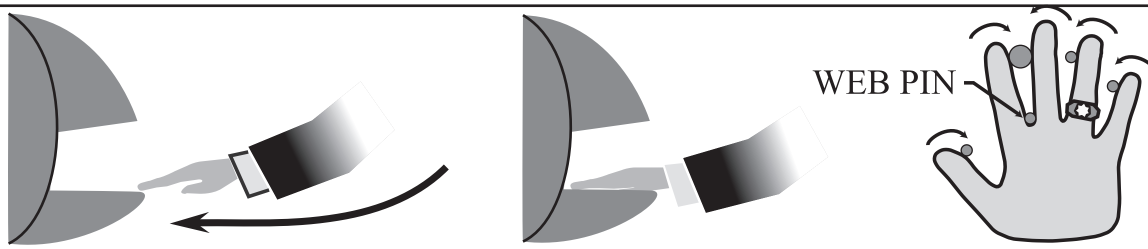


Figure 8-2: Placing Your Hand on the Platen

Left Hand Enrollment

Some right hands cannot be used in the HandPunch due to disabilities such as missing fingers. You can enroll a user with the left hand facing palm side up. The techniques for left hand enrollment are the same as for standard enrollment. The user should keep the back of the hand flat against the platen and move the fingers against the web pin and the finger pins in the same manner as in standard enrollment. Users enrolled with the left hand must always verify with the left hand. Extra practice on placing the hand on the platen may be required to ensure correct, consistent hand reads.

Read Score

When a user uses the HandPunch, the display appears as follows:

```
OKAY (USER ID)
SCORE IS: (SCORE NUMBER)
```

The score number on the display reflects how accurately the user's hand is placed on the platen (see page 64). Scores that vary greatly between low and high numbers are indicative of inconsistent hand placement. Scores above 50 are indicative of improper hand placement or of a drastic change in the physical appearance of the hand.

When this occurs, emphasize the importance of sliding the hand onto the platen and keeping the hand flat. Re-training and practice should lower a user's score. It might be necessary to change a user's reject threshold if the user has a mild disability. Re-enrollment might be necessary to create a new user template.

Enrollment Commands

There are three commands available from the Enrollment command menu:

- Add Employee
- Add Supervisor
- Remove User

Refer to Table 12 to identify the command you need to perform. Step through all previous commands until you reach the desired command.

Table 12: Enrollment Command Menu

Service Menu
Password = 4
Add Employee
ID #
Add Supervisor
ID #
Remove User
ID #

Add Employee

The Add Employee command allows you to enroll a new employee into the HandPunch.

Add Supervisor

The Add Supervisor command allows you to enroll a new supervisor into the HandPunch.

Remove User

The Remove User command allows you to remove an employee or supervisor from the HandPunch.

Special Menu

The Special menu has one command – Special Enroll. This command accommodates users with disabilities that make it difficult or impossible to use a HandPunch in its standard way. The following section provides a brief description of the Special Menu command.

Enter the appropriate password to enter the Special command menu. Once you have entered the command menu, there are three options available for navigating the command menu system.

Press # to enter the command shown on the display.
Press * to step to the next command in the menu.
Press **CLEAR** to exit the command menu (pressing any numeric key also exits the command menu). If you are in a command's sub-menu, press **CLEAR** multiple times to completely exit the command menu.

Special Command

There is one command available from the Special command menu:

- Special Enroll

Refer to Table 13 and identify the command you need to perform. Step through all previous commands until you reach the desired command.

Table 13: Special Command Menu

Special Menu
Password = 5
Special Enroll
ID #
On/Off (Y/N)

Special Enroll The Special Enroll command allows a user to be enrolled such that the ID number is the primary criteria for determining access. A hand read is required, but is not verified against any stored identification data. A time zone value can be applied to the Special Enrollment ID number to limit access times (see page 62). The HandPunch default is for no time zone to be applied.

❗**NOTE** *Special Enrollment affects the integrity of the HandPunch terminal and should only be used as a last resort. Anyone who knows a Special Enroll ID number is granted access when the ID number is used. Before specially enrolling a user, try to alleviate verification problems by adjusting the individual user's reject threshold (see page 62) or by using left hand enrollment (see page 65).*

HandPunch Maintenance

A minimum amount of system maintenance is required to keep HandPunchs fully functional. HandPunchs should be cleaned periodically to prevent an accumulation of dust from affecting the HandPunch's readability. User Scores should be reviewed periodically to ensure the HandPunch is performing properly.

NOTE *There are* **NO** *user serviceable parts inside the HandPunch.*

Cleaning the HandPunch

Once a HandPunch system is in operation there are three HandPunch commands that can assist with system maintenance. These commands are performed through the Service Menu. The instructions for these commands begin on page 54.

- Calibrate – View HandPunch exposure values.
- Status Display – Display HandPunch input/output status, the hand read score of the last user to verify on the system.

Inspect and clean the HandPunch regularly to maintain optimum performance. Clean the platen, side mirror, reflector, and the window above the platen using a clean cloth dampened with ordinary, non-abrasive window cleaner (see Figure 9-1 below). Start at the rear corners of the platen and work your way forward.

NOTE *DO NOT SPRAY CLEANING FLUID DIRECTLY INTO OR ON THE HandPunch.*

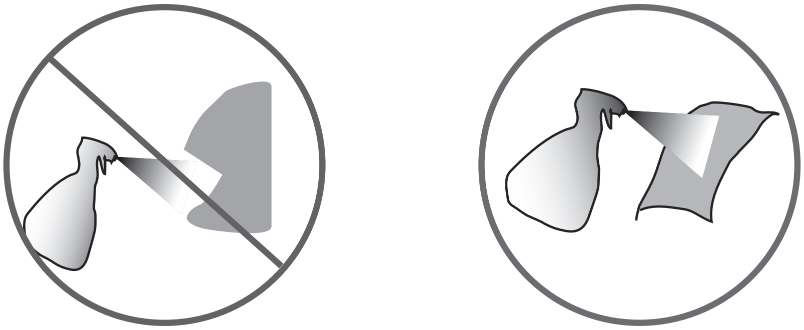


Figure 9-1: HandPunch Cleaning

User Score

Periodically check users' scores (refer to the Read Score section on page 65). Scores should average under 30. Occasionally a user will score above 30. This is not necessarily an indication of poor performance. If a number of scores average over 30, clean the HandPunch and check scores again. If scores remain high, or if users are experiencing frequent rejections, run the Calibration command (see page 55).

Appendix A

Tips for a successful Installation

HandPunch

- Think of the HandPunch as a camera
- Clean the HandPunch before it gets dirty
- Use non-abrasive cleaners such as glass cleaners and non-abrasive and clean cloths
- Make cleaning the HandPunch part of Janitorial program
- Do not remove the foam backing from the wall mounting plate
- Seal any holes made in the wall for wire routing, so that dust will not blow into the HandPunch

Location

- Mount all HandPunchs in a network so that the top of the platen is 40” off of the floor
- If an enrollment HandPunch is used make sure that it is placed with the top platen 40” off of the floor and not sitting directly on top of a desk, this will help to eliminate “bad enrollments”
- Mount the HandPunch so that it is not difficult or dangerous to verify then open the door
- It is not recommended to mount the HandPunch in an area where there is airborne dust, in the path of direct sunlight, or where the HandPunch can be exposed to water or corrosive gasses

Enrollment

- Educate the Enrollee on Hand Geometry
- Explain enrollment process
- Train Enrollee on hand placement
  -Practice placing hand on platen
  -Rotate rings to be stone-up
  -Make sure hand is flat on platen
  -Close finger towards the center of hand
  -Fingers gently touch finger pins
- Let the enrollee enter in their own ID number during the enrollment process, this forces the Enroller to step aside allowing the Enrollee to stand in front of the HandPunch helping to eliminate “bad enrollments”
- If an enrollment HandReader is used make sure that it is placed with the top of the platen 40” off of the floor and not sitting directly on top of a desk, this will help to eliminate “bad enrollments”
- If an enrollment transaction fails:
  -Retrain the user on correct placement and ensure that rings are rotated to be stone-up then

-Try again to enroll the same hand
-Try to enroll the other hand (with the hand placed upside-down so the thumb still contacts the thumb-pin on the platen)

- After enrollment, it is a good idea to let the enrollee enter their ID number and practice a verification transaction to ensure that the enrollment was high-quality.
- If a user consistently fails during verifications days/months/years later, re-enroll the user to ensure a high quality and up-to-date enrollment record.

Communication

- Make sure the Data Convertor is plugged in
- When starting a network for the first time bring one HandPunch up at a time, this is a very easy way to find out where communication problems may exist

Appendix B

Noted Board Configuration Differences

Because of Schlage Biometrics' camera retrofit of the HandPunch some changes have been made to the main PCB and they are listed as follows:

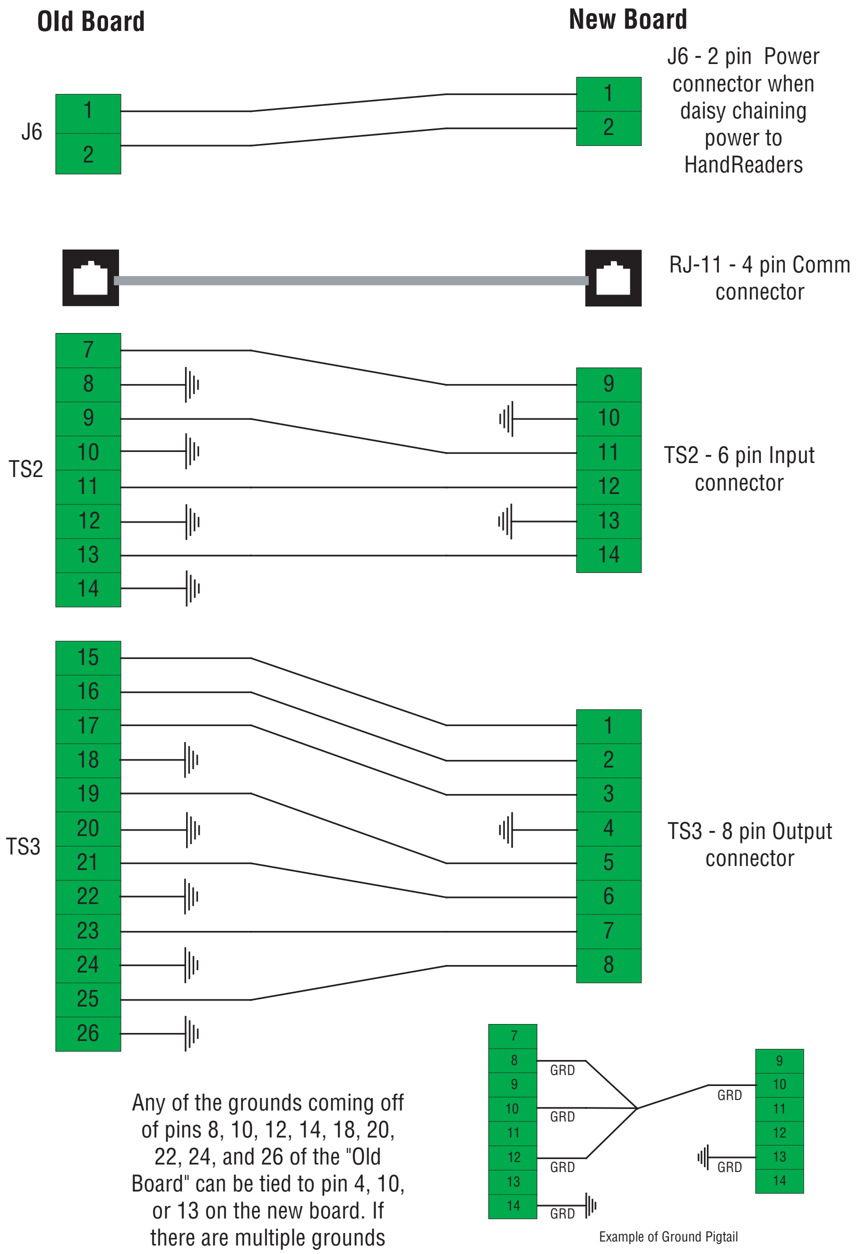
- Dipswitches have been removed
  -comm lines are terminated.
  -RS-485 is set by wiring jumpers.
  -memory is reset with a push-button reset and user interface with keypad and LCD.
- The labeling of the terminal strips have changed. See "Figure 11-1" on page 73.
- The configuration of the terminal strips have changed. See "Figure 11-2" on page 74.
- Power has moved to the right side of the PCB.
- The RSS-232 RJ-45 receptacle has been replaced with a 4 pin Molex connector on the left side of the PCB.
- A 2 pin Molex connector (J5) has been added to the board, next to the reset button, to supply power for the LEDs. This connector should never be unplugged. unless a modem or Ethernet is added to the PCB.
- The upgrading of the memory is now handled through software codes at the HandPunch. Contact Order Entry for memory upgrades.

Terminal Block Labeling

Number	OLD PCB	Number	NEW PCB
1	12-24 VDC (+) OR VAC	**1**	(+) 5 VDC OUTPUT
2	12-24 VDC (-) OR VAC	**2**	DATA/D0
RJ-11	RX-	**3**	CLOCK/D1
RJ-11	RX+	**4**	GROUND
RJ-11	TX-	**5**	LOCK OR CLOCK OUTPUT
RJ-11	TX+	**6**	BELL OR DATA OUTPUT
		7	AUXOUT 1
7	REX SWITCH	**8**	AUXOUT 2
8	GROUND		
9	DOOR SWITCH	**9**	REX SWITCH
10	GROUND	**10**	GROUND
11	AUX IN 1	**11**	DOOR SWITCH
12	GROUND	**12**	AUX IN 1
13	AUX IN 2	**13**	GROUND
14	GROUND	**14**	AUX IN 2
15	(+) 5 VDC OUTPUT	**RJ-11**	RX-
16	DATA/D0	**RJ-11**	RX+
17	CLOCK/D1	**RJ-11**	TX-
18	GROUND	**RJ-11**	TX+
19	LOCK OR CLOCK OUTPUT		
20	GROUND	**1**	12-24 VDC (+) OR VAC
21	BELL OR DATA OUTPUT	**2**	12-24 VDC (-) OR VAC
22	GROUND		
23	AUXOUT 1		
24	GROUND		
25	AUXOUT 2		
26	GROUND		

Figure 11-1

Terminal Block Layout


Old Board
New Board
J6
1
2
1
2
J6 - 2 pin Power connector when daisy chaining power to HandReaders
RJ-11 - 4 pin Comm connector
TS2
7
8
9
10
11
12
13
14
9
10
11
12
13
14
TS2 - 6 pin Input connector
TS3
15
16
17
18
19
20
21
22
23
24
25
26
1
2
3
4
5
6
7
8
TS3 - 8 pin Output connector
GRD
GRD
GRD
GRD
GRD
GRD

Example of Ground Pigtail

Any of the grounds coming off of pins 8, 10, 12, 14, 18, 20, 22, 24, and 26 of the "Old Board" can be tied to pin 4, 10, or 13 on the new board. If there are multiple grounds create a pig tail so that there is only 1 wire going into the terminal block

Figure 11-2

Memory Reset

To reset the memory of the HandPunch follow these steps-

1. Remove power and battery jumper, if a back up is installed
2. Press down on reset button and apply power
3. Release button
4. Reader will boot to

ERASE	**:1 SETUP** **:9 ALL!!!**

- Press 1 to erase setup i.e. address, outputs, passwords, but retain user database and datalogs
- Press 9 to erase everything i.e. HandPunch goes back to factory defaults

Appendix C

Old Board Configuration Information

Wall Plate Installation

1. Loosen the three bottom mounting screws until there is approximately 1/8 inch (3 mm) clearance between the screw head and the wall plate.
2. Remove the HandPunch from its carton.
3. At the base of the HandPunch is a piano hinge with three keyhole shaped slots that correspond with the three lower mounting screws. Align and hang the HandPunch from the three lower mounting screws (see below).

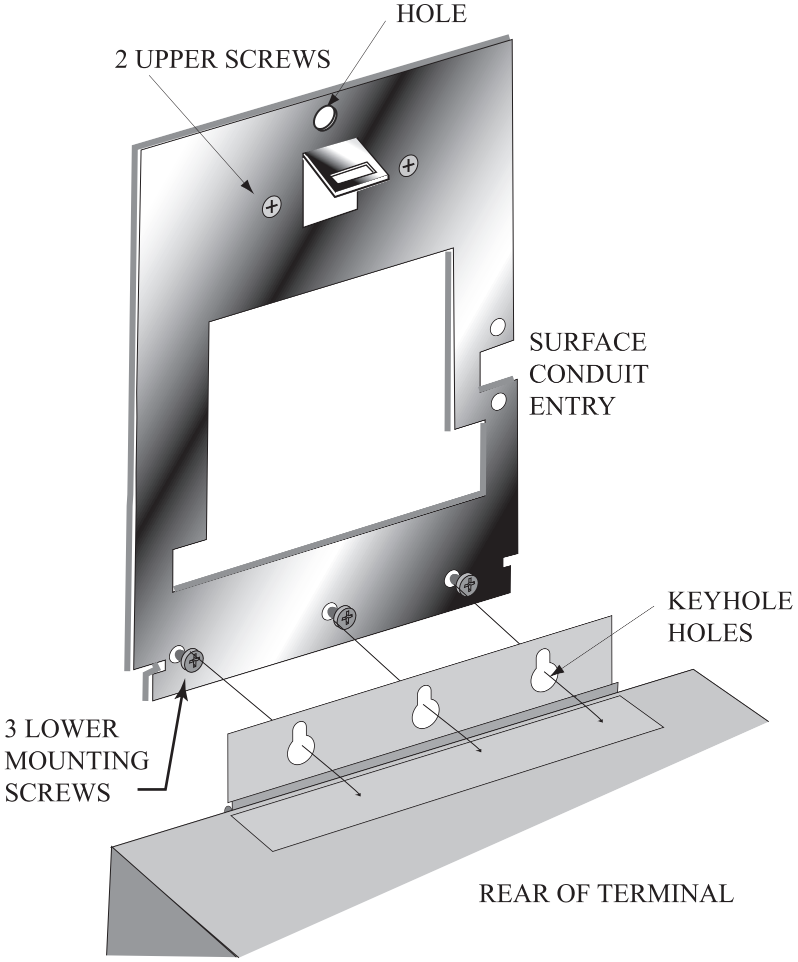


Figure 13-1: Attaching the HandPunch to the Wall Plate

4. Tighten all three lower mounting screws.
5. The HandPunch is now ready for its wiring connections.

Grounding

NOTE Terminal 1 and the center pin of jack J12 are connected together. Terminal 2 and the sleeve of jack J12 are connected together.

NOTE *Use any one of the following ground terminals to make the earth ground connection: 8, 10, 12, 14, 18, 20, 22, 24, or 26. Do* **NOT** *use terminal 2 to establish the earth ground connection; terminal 2 is not directly connected to ground.*

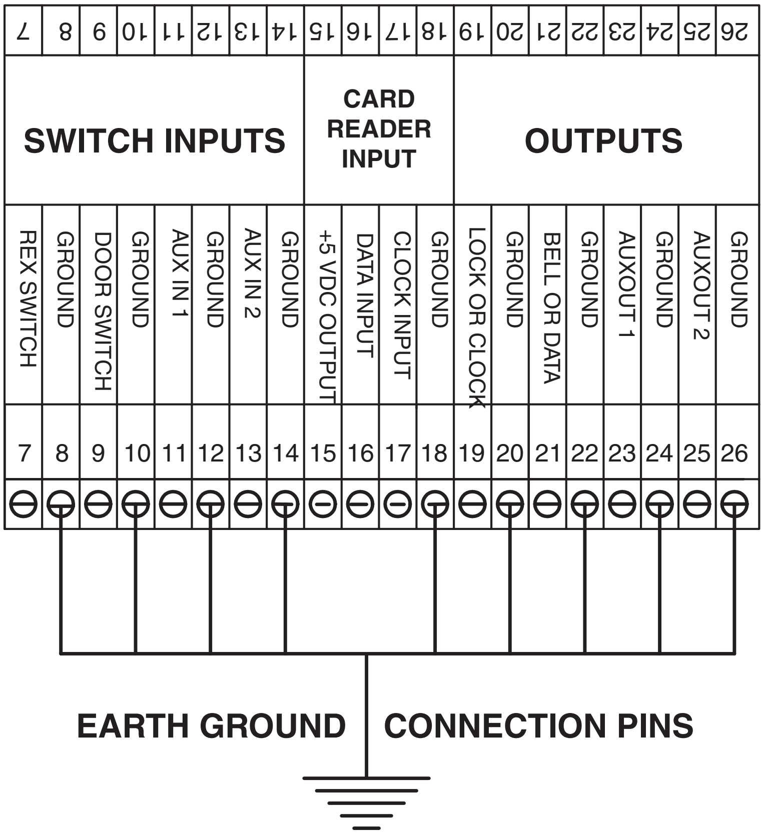


Figure 13-2: Earth Ground Connection Terminals

There are two standard methods for providing earth grounding to HandPunch units:

- earth grounding all units (see 15)
- carrying an earth ground to each unit (see 16)

Earth ground all units when there is a good earth ground source near each unit and/or when there are very long cable runs between units.

Carry an earth ground to each unit when there are no earth grounds convenient to the unit and the unit's power supply is floating.

Wiring Connections

Once the HandPunch is attached to the wall plate the wiring connections to the HandPunch can be made (see Figure 13-3 below).

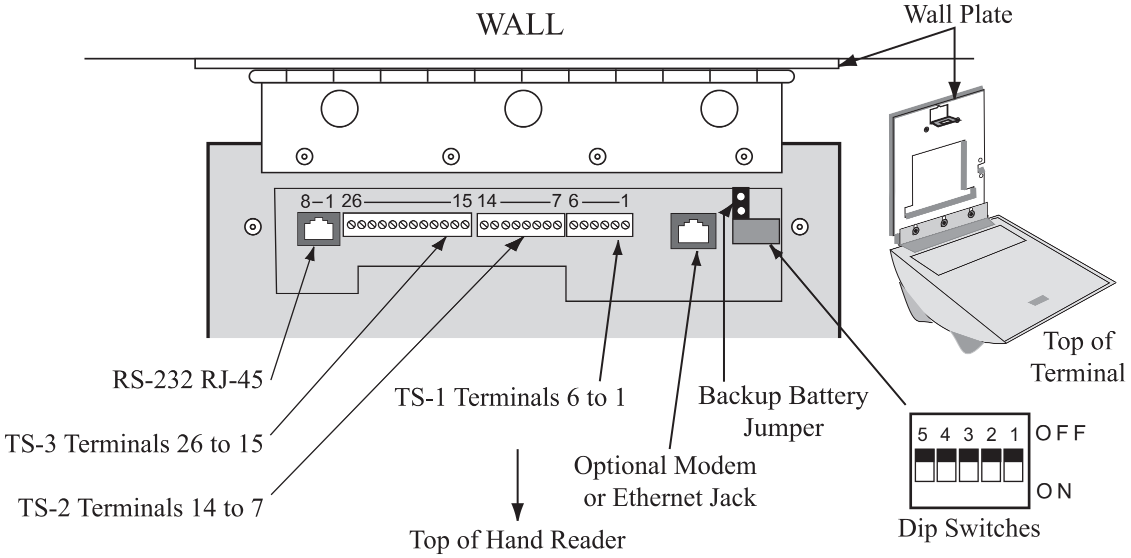


Figure 13-3: Wiring Connections and Dip Switches

Wiring Examples

The following Tables provide the pin outs for the terminal strips on the HandPunch.

- “Table 14” on page 79 provides the pinouts for TS-2 – Input Connections.
- “Table 15” on page 79 provides the pinouts for TS-3 – Card Reader and Output Connections.
- “Table 16” on page 80 provides the pinouts for the RJ-45/RS-232 Serial Printer or Host Computer Connection.
- “Table 17” on page 81 provides the pinouts for the RJ-11/RS-422 HandPunch-to-HandPunch Network Connection.

The following Figures provide pinout diagrams for the RJ connectors.

- Figure 13-4 on 81 provides the pinouts for J3, the RJ-11/RS-422 Network Connection.
- “Figure 13-5” on page 81 provides the pinouts for J8, the RJ-45/RS-232 Serial Printer Connection.

The following Figures provide sample HandPunch wiring diagrams:

- "Figure 13-6" on page 82 provides a sample Bell Output wiring diagram.
- "Figure 13-7" on page 83 provides a sample Door Lock Output wiring diagram.
- "Figure 13-8" on page 84 provides a sample Request to Exit, Door Switch, and Auxiliary Inputs wiring diagram.
- "Figure 13-9" on page 85 provides a sample Auxiliary Outputs wiring diagram.
- "Figure 13-10" on page 86 provides a sample External Card Reader wiring diagram.
- "Figure 13-11" on page 87 provides a sample RS-422 4-Wire Direct-Connect Host PC to HandPunch Network wiring diagram.
- "Figure 13-12" on page 88 provides a sample Host PC to HandPunch Ethernet Network wiring diagram.
- "Figure 13-13" on page 89 provides a sample Host PC to HandPunch Modem Network wiring diagram.
- "Figure 13-14" on page 90 provides a sample Printer or Host PC to HandPunch wiring diagram.

Table 14: TS-2 - Input Connections

Terminal	Connection
7	Request to Exit Input
8	Ground
9	Door Monitor Switch Input (NC Standby)
10	Ground
11	Auxiliary Input 1
12	Ground
13	Auxiliary Input 2
14	Ground

Table 15: TS-3 - Card Reader and Output Connections

Terminal	Connection
15	+5 VDC @ 400 mA Max. Output for External Card Reader
16	Card Reader: Wiegand D0 or Magnetic Stripe Data Input

Table 15: TS-3 - Card Reader and Output Connections

Terminal	Connection
17	Card Reader: Wiegand D1 or Magnetic Stripe Clock Input
18	Card Reader Ground
19	Lock Output or Wiegand D1 or Magnetic Stripe Clock Output
20	Ground
21	Auxiliary Output 0 or Wiegand Data 0 or Magnetic Stripe Data Output
22	Ground
23	Auxiliary Output 1
24	Ground
25	Auxiliary Output 2
26	Ground

Table 16: RJ-45/RS-232 Serial Printer Connection

J8 Pin	Signal	Connection
1	RI	* Ring Indicator Input (from external device)
2	CD	* Carrier Detect Input (from external device)
3	DTR	* Data Terminal Ready Output (to external device)
4	GND	Ground
5	Rx Data	Receive Data Input (from external device)
6	Tx Data	Transmit Data Output (to external device)
7	CTS	* Clear to Send Input (from external device)
8	RTS	* Ready to Send Output (to external device)

* These signals are not currently supported

Table 17: RJ-11/RS-422 Network Connection

J3 Pin	Signal
1	Rx+
2	Rx-
3	Tx-
4	Tx+

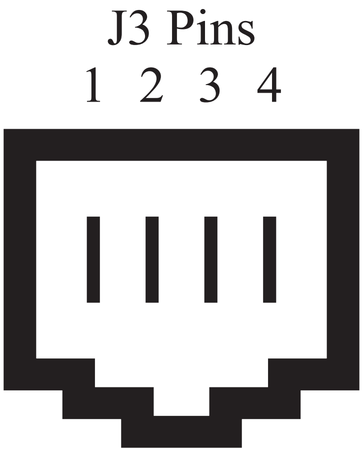


Figure13-4: J3 - RJ-11/RS-422 Jack Pinout

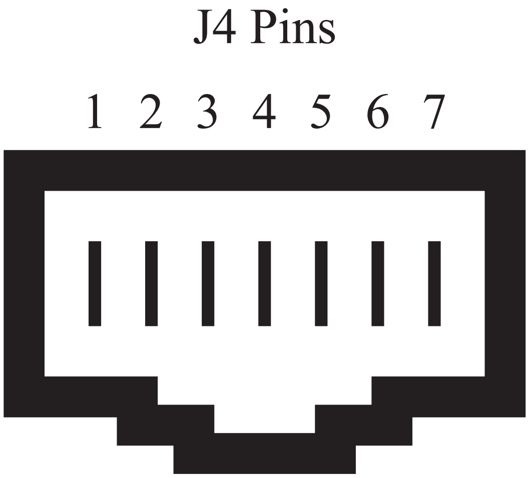
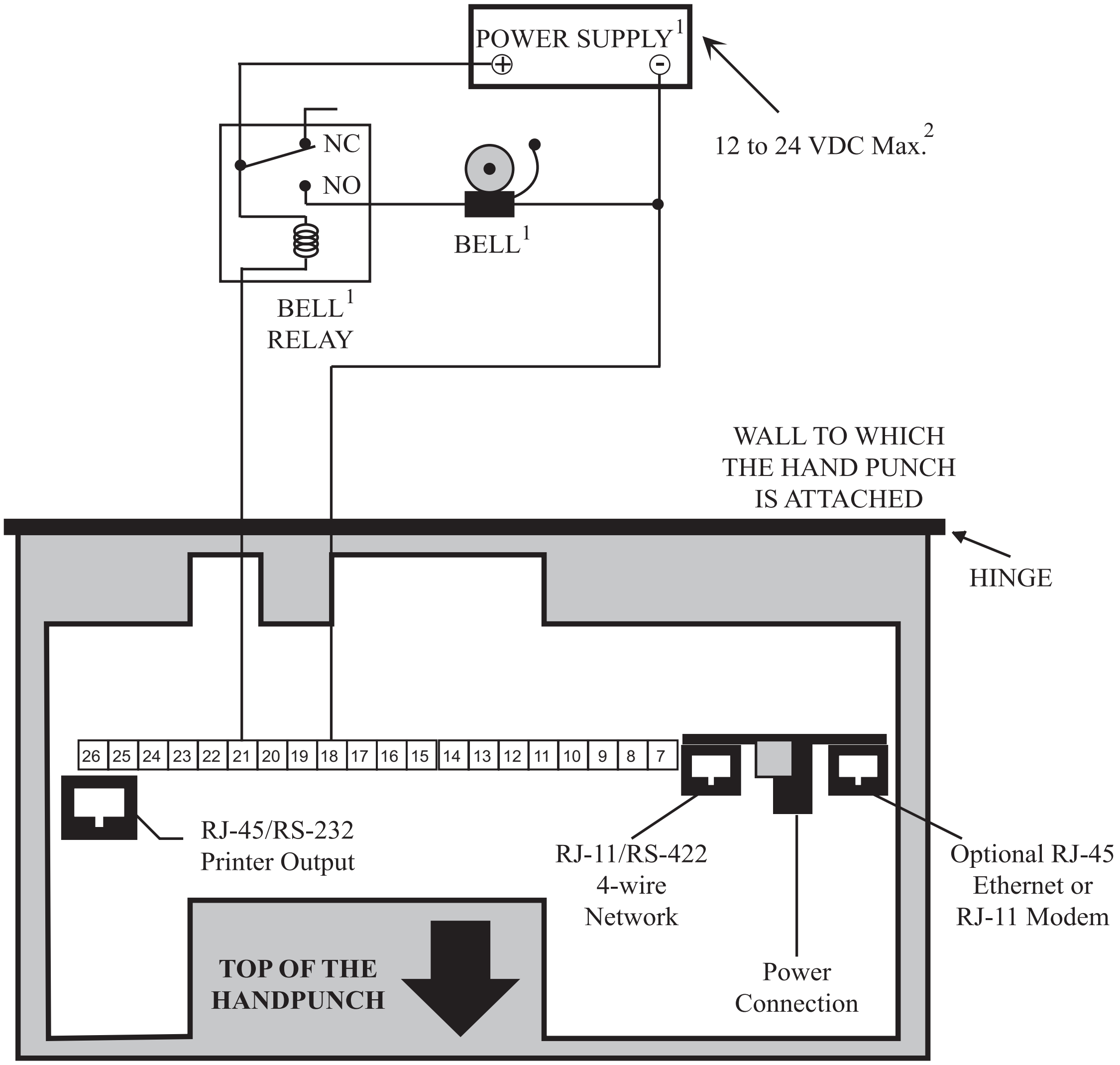


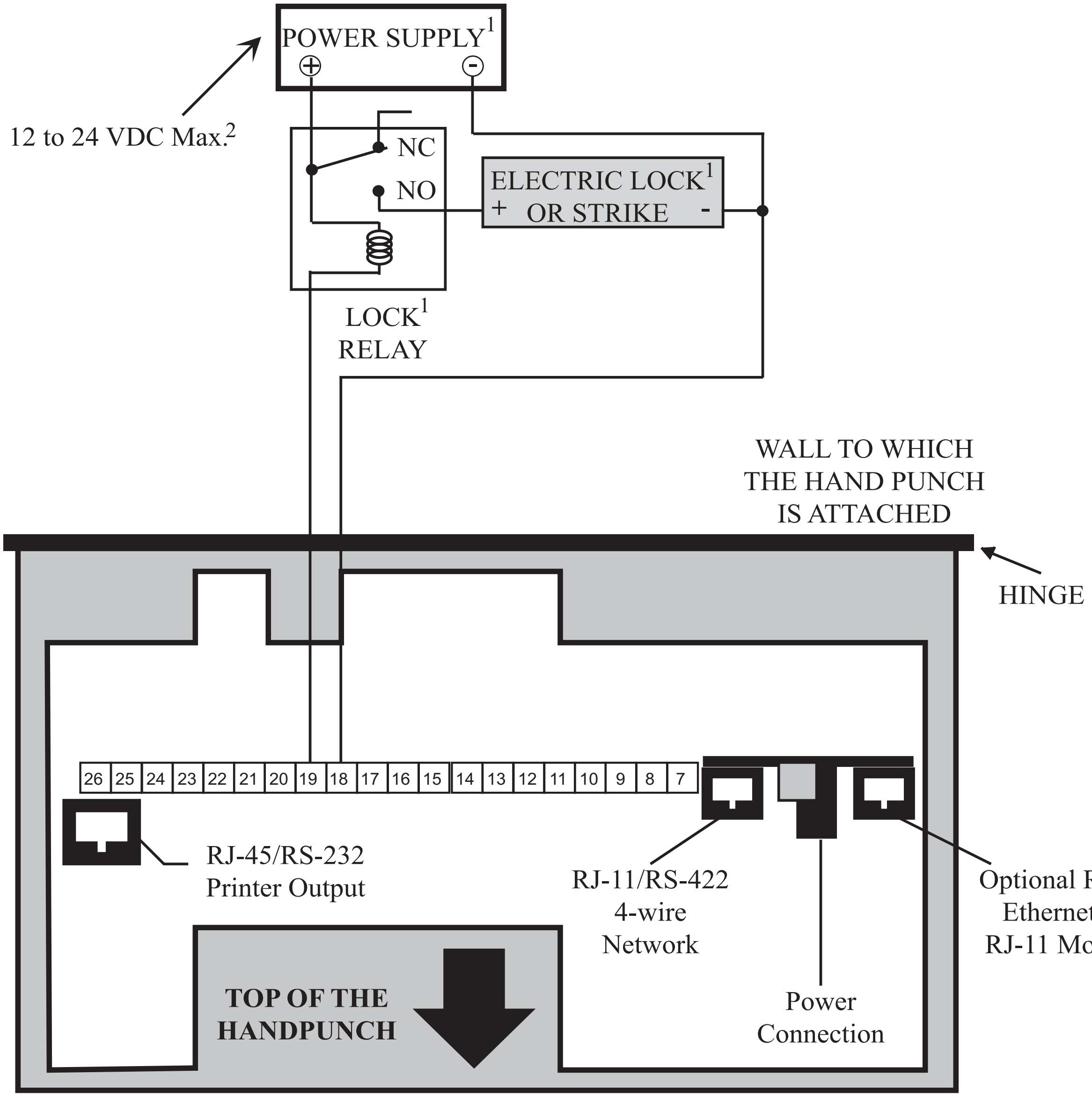
Figure 13-5: J4 - RJ-45/RS-232 Jack Pinout



[1] These components are not supplied by Recognition Systems, Inc.

[2] The Power Supply shall be a UL Listed Limited Current Power Source for UL 294 Installations.

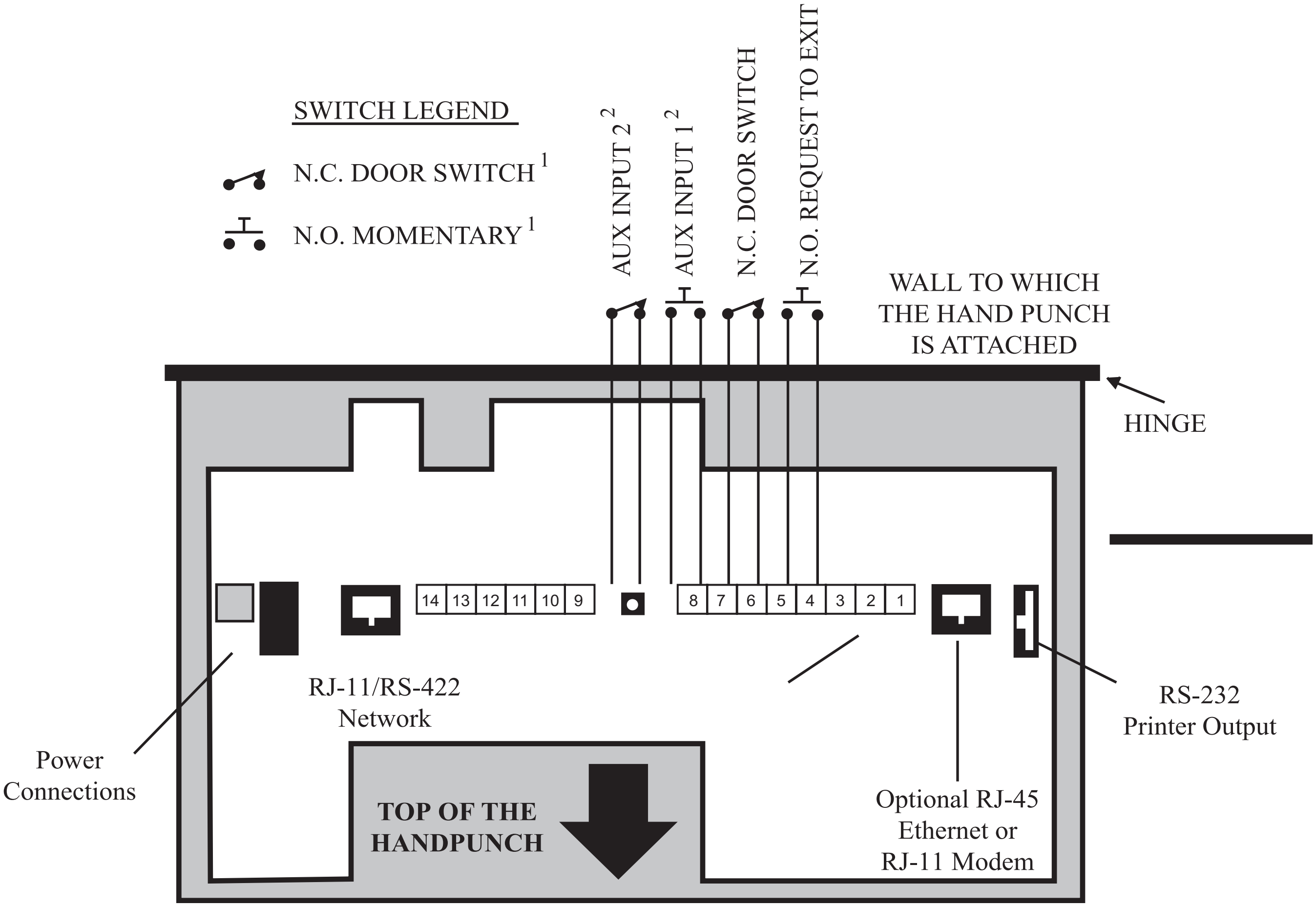
Figure 13-6: Bell Output Wiring Diagram



[1] These components are not supplied by Recognition Systems, Inc.

[2] The Power Supply shall be a UL Listed Limited Current Power Source for UL 294 Installations.

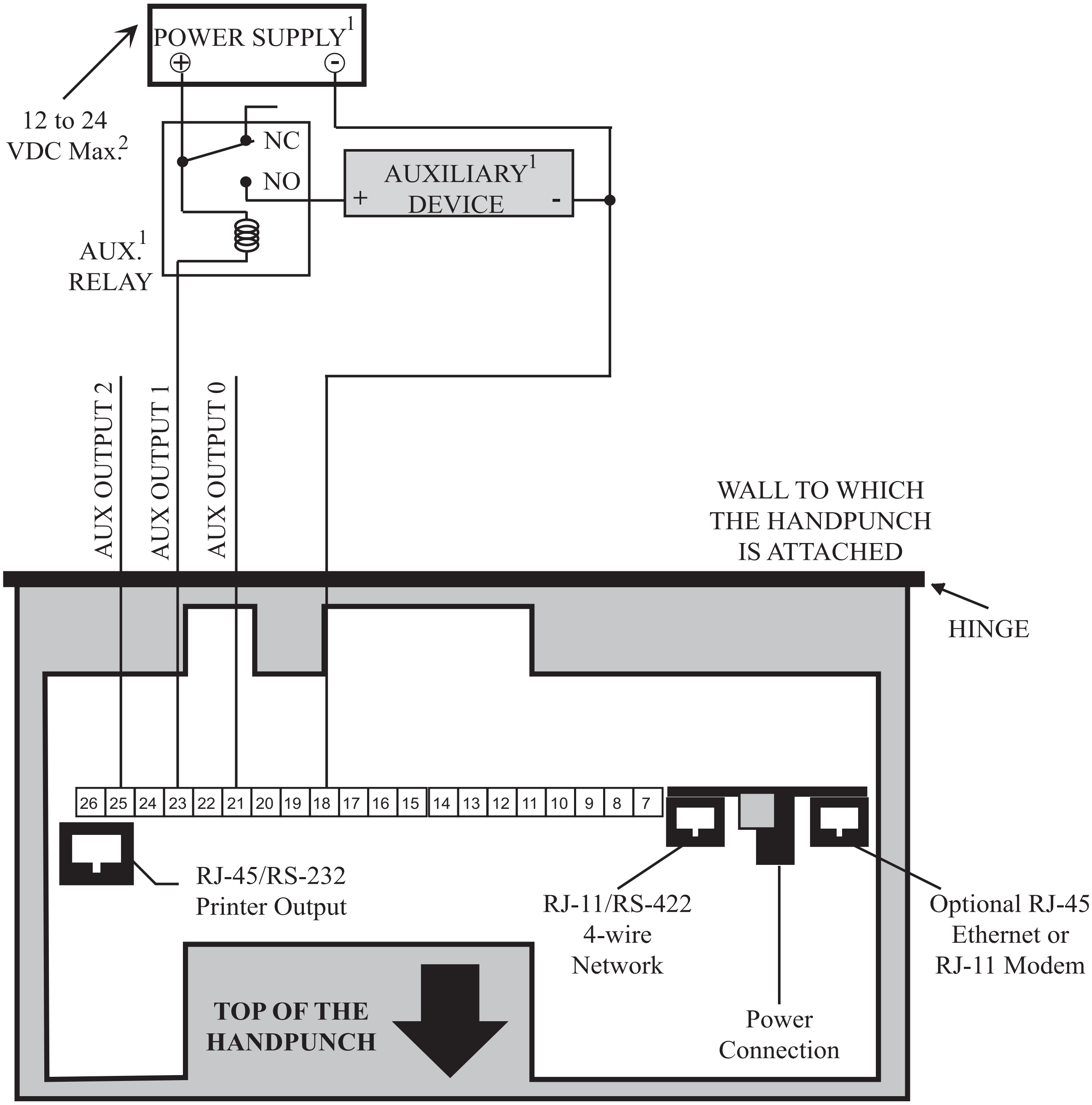
Figure 13-7: Door Lock Output Wiring Diagram



[1] These components are not supplied by Recognition Systems, Inc.

[2] The Aux 1 and Aux 2 input contact states are programmable within the HandPunch unit.

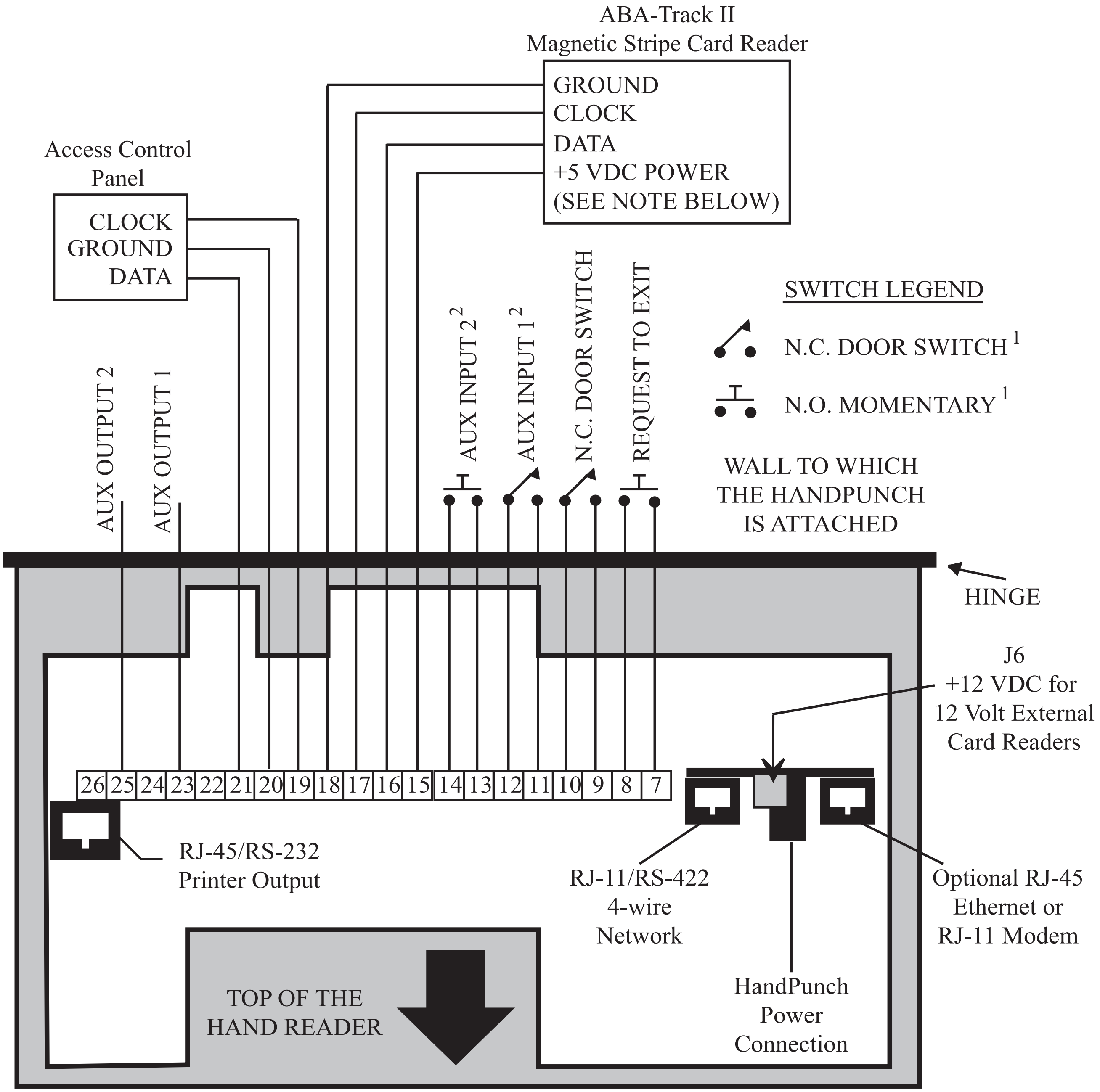
Figure 13-8: Request to Exit, Door Switch, and Auxiliary Inputs Wiring Diagram



[1] These components are not supplied by Recognition Systems, Inc.

[2] The Power Supply shall be a UL Listed Limited Current Power Source for UL 294 Installations.

Figure 13-9: Auxiliary Outputs Wiring Diagram



[1] These components are not supplied by Recognition Systems, Inc.

[2] The Aux 1 and Aux 2 input contact states are programmable within the HandPunch unit.

NOTE: For +12 VDC magnetic stripe readers, connect the magnetic stripe reader power supply to J6 on the Hand Punch.

Figure 13-10: External Card Reader Wiring DIagram

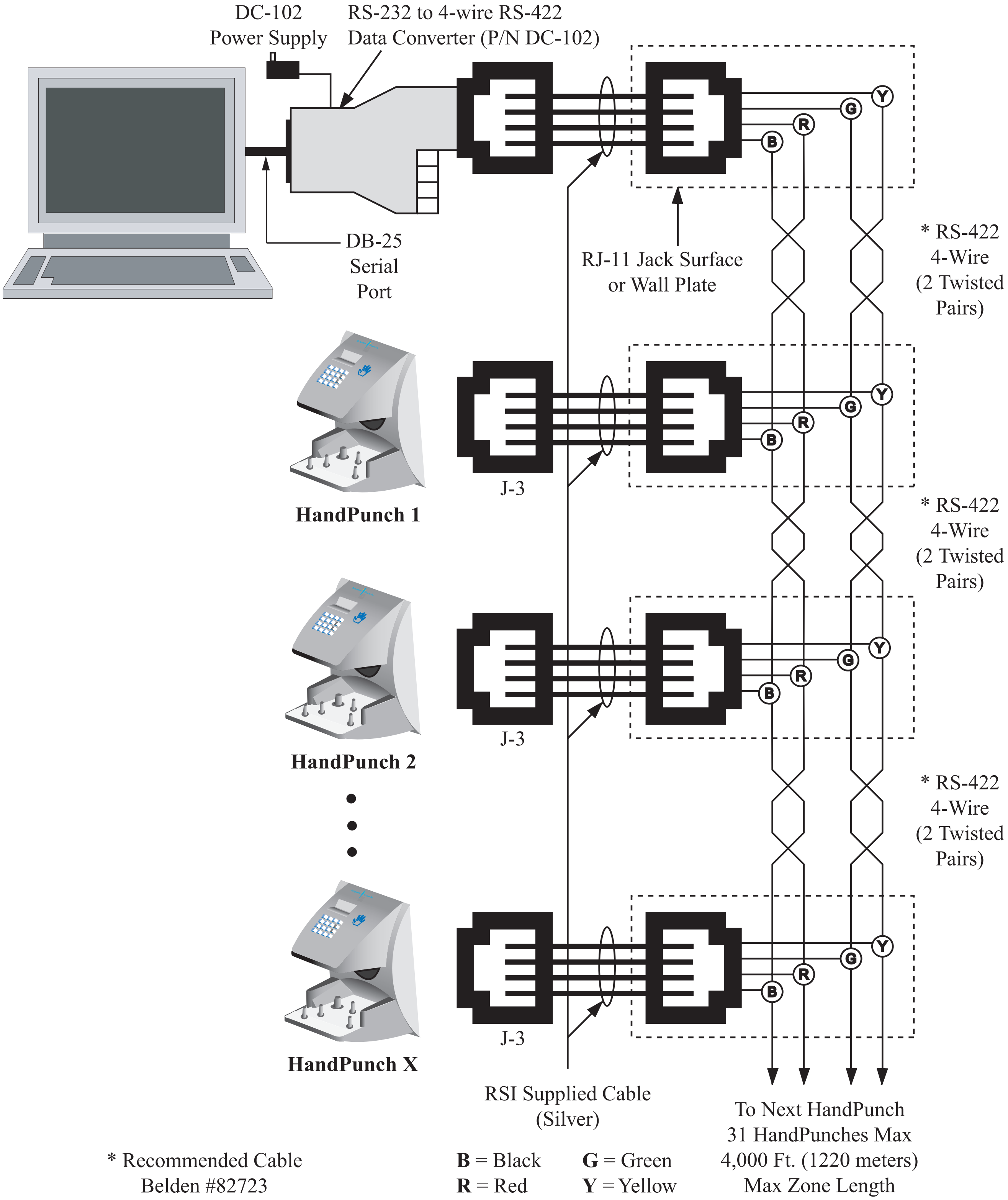


Figure 13-11: RS-422 4-Wire Direct-Connect Host PC to HandPunch Connection

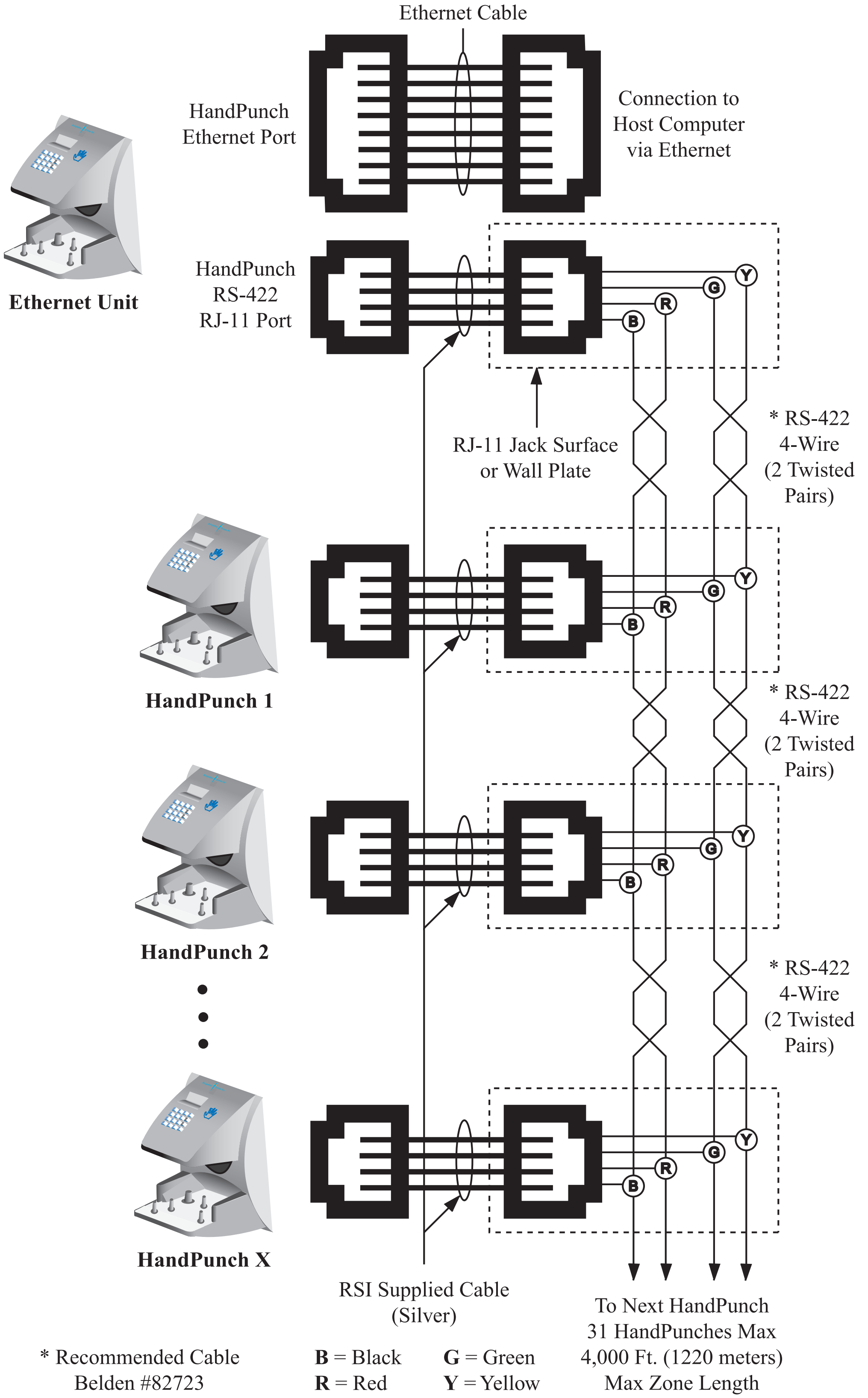


Figure 13-12: Host PC to HandPunch Ethernet Connection

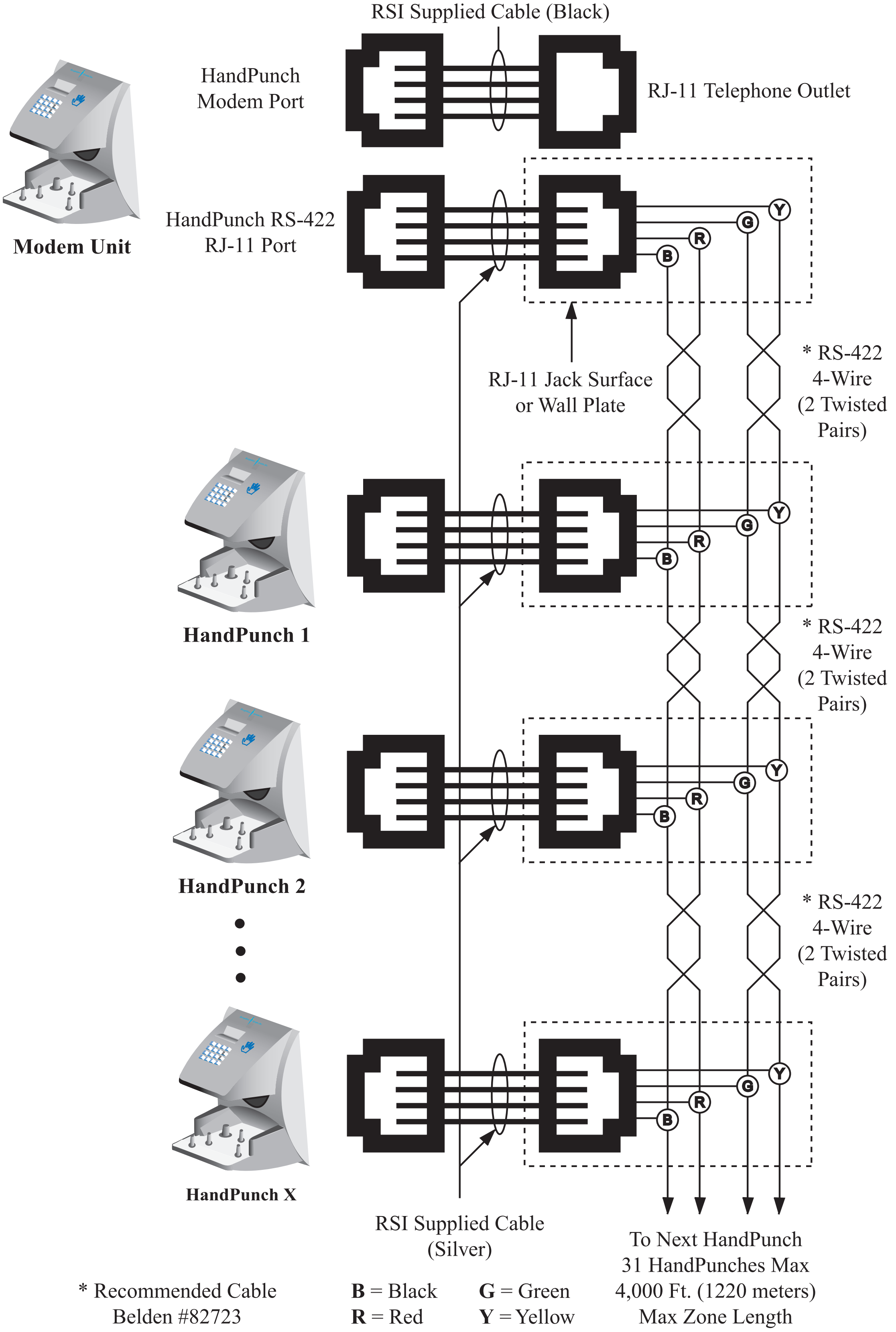
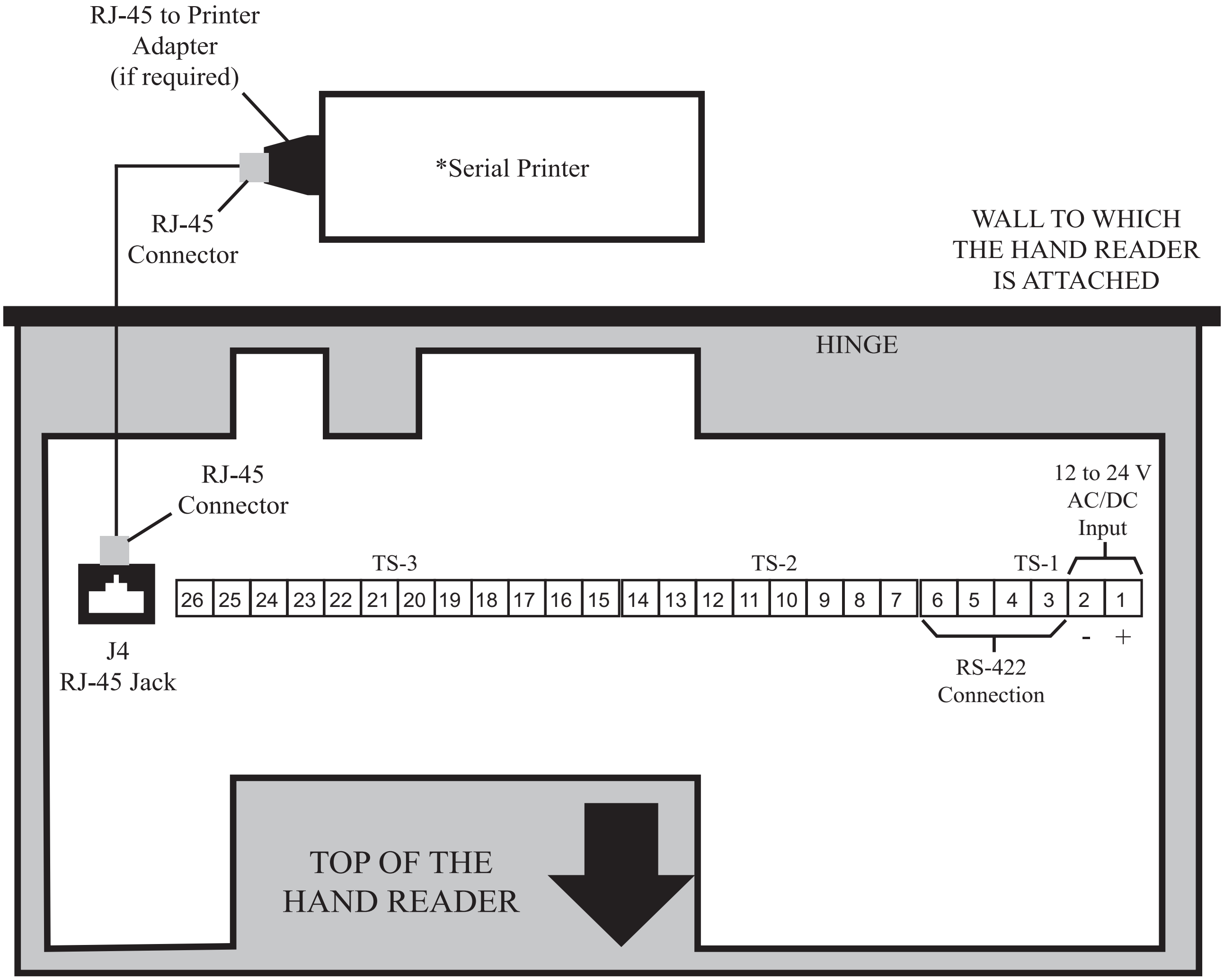


Figure 13-13: Host PC to HandPunch Modem Connection



* These components are not supplied by Recognition Systems, Inc.

Figure 13-14: HandPunch to Serial Printer or Host Computer Wiring Diagram

Setting the DIP Switches

The DIP Switch settings perform three tasks for the HandPunch (see Figure 13-15 below):

- Set End of Line (EOL) Termination to match the type of termination needed by the network.
- Set the Communication Method to match the type of network used.
- Erase Memory to clear HandPunch memory to all factory defaults values and also clear all user memory.

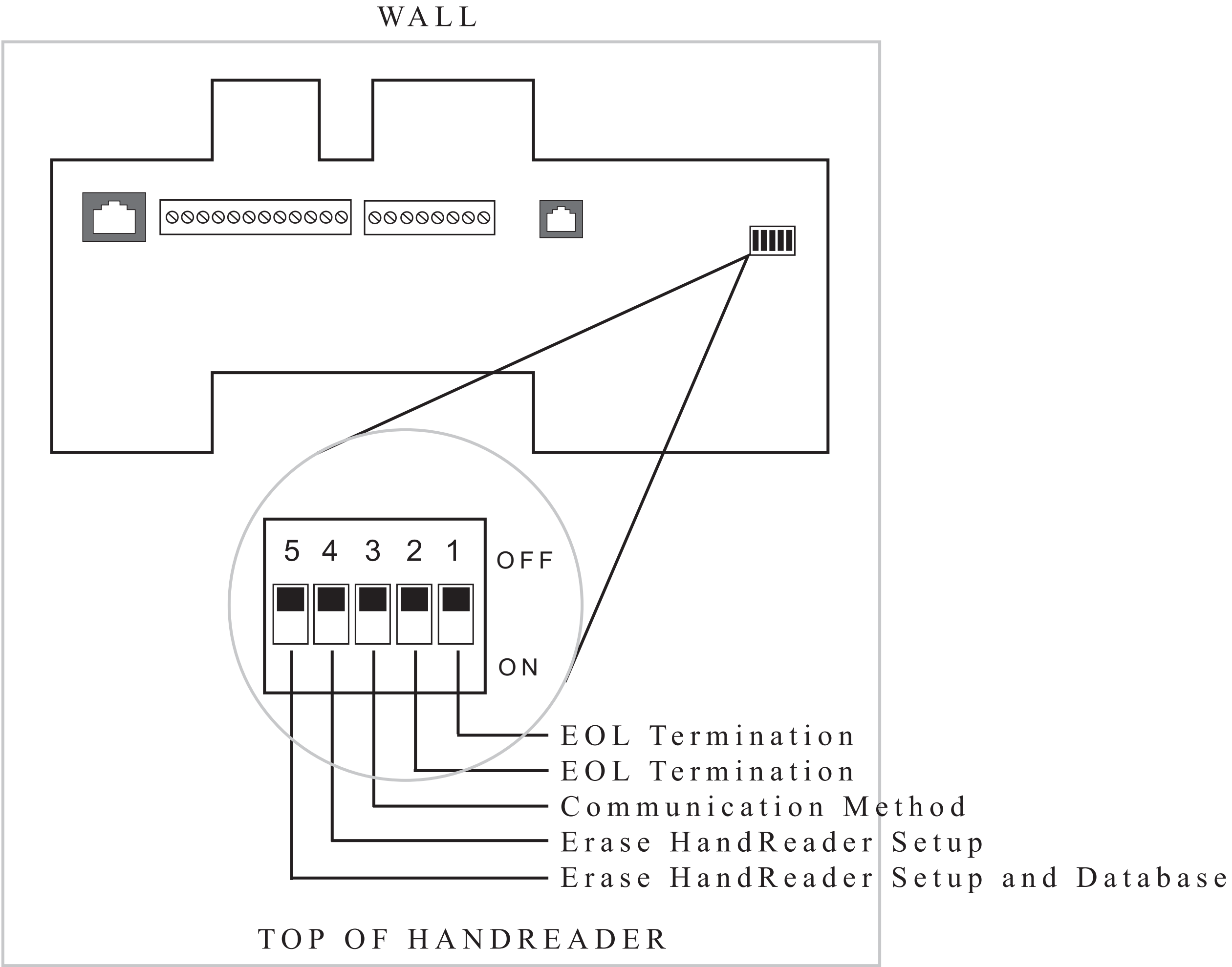


Figure 13-15: HandPunch Dip Switches

End of Line Termination

Termination helps to ensure clean data signals are transmitted through the network wiring. Termination is applied to the end-of-line (EOL) HandPunch in the network daisy-chain. The factory default setting is for EOL termination to be disabled – switches 1 and 2 OFF. Refer to “Figure 13-15” on page 91 for switch ON/OFF positioning.

- To enable EOL termination at a HandPunch, both switches 1 and 2 must be ON.
- To disable EOL termination at a HandPunch, both switches 1 and 2 must be OFF.

EOL Termination must be **enabled** for:

- A single HandPunch terminal installation.
- In a HandPunch Direct-Connect network – the last HandPunch in the daisy-chain (the one farthest from the host computer).
- In a Modem/HandPunch to PC network the HandPunch terminal with the Ethernet option (for communication with the host computer) in the daisy-chain.

EOL Termination must be **disabled** for:

- All HandPunches in the network not identified in teh previous section.
- In an Ethernet/HandPunch to PC network the HandPunch terminal with the Ethernet option (for communication with the host computer) in the daisy-chain.

Communication Method

The communication method dip switch is set ON for factory testing purposes. The factory default setting and for standard operation, switch 3 must be OFF.

- Switch 3 must always be OFF.

Erasing HandPunch Memory

The erase memory function can perform either or both of the following:

- Erase a HandPunch’s configuration data.
- Erase a HandPunch’s user database, transaction buffer, and menus (and messages on the HandPunch 4000).

The factory default setting (and normal operation setting) is set for switches 4 and 5 to be OFF, retaining memory.

!NOTE *If the HandPunch is equipped with the battery backup option, remove shunt J7 in front of the DIP switch array (see “Figure 13-3” on page 78) before proceeding. Replace shunt J7 after completion of the following steps.*

Erasing the HandPunch Setup

Perform the following steps to erase the configuration data but retain the user database.

1. With system power OFF, set switch 4 ON.
2. Turn system power ON and wait for HandPunch boot information to appear on the display.
3. Turn switch 4 OFF.

Erasing the HandPunch Setup and User Database

Perform the following steps to erase both the configuration data and the user database.

1. With system power OFF, set both switches 4 and 5 ON.
2. Turn system power ON and wait 5 seconds.
3. Turn both switches 4 and 5 OFF.

! NOTE *Before putting the HandPunch into service ensure DIP switches 4 and 5 are both OFF. If switches 4 and 5 are not off, the next time the HandPunch's power is cycled the HandPunch's memory will be erased.*

Appendix D

Troubleshooting Guide

Display Messages During Verification

Various messages can appear on the HandPunch’s dispaly during hand verification. These messages are defined in Table 18 below.

Table 18: Display Messages During Verification

Message	Definition
PLACE HAND	The platen is ready to receive your hand for verification.
ID VERIFIED	You are verified, proceed.
REMOVE HAND	Remove your hand and place it on the platen again. Follow proper hand placement rules.
TRY AGAIN	Your attempt was rejected. Repeat verification following proper hand placement rules.
ID REFUSED	Your rejections exceeded the maximum number of tries allowed. Wait until another employee has verified and try again or call your supervisor.
ENTER ID	You entered your ID number incorrectly or your access time is restricted.

- If the display shows **TRY AGAIN**, you are not verified. You may have made an error in entering your ID number or in placing your hand on the platen. Re-enter your ID number and try again, taking care to follow proper hand placement rules (see 64).
- If the display shows **TIME RESTRICTION**, you are not authorized to punch in at this time. If this seems to be in error, contact your supervisor about time restrictions.
- After a pre-programmed number of denied attempts, an ID number will no longer be accepted and the display will appear as follows:

ID INVALID
TEMPORARILY

This is called a “lockout”. Before the rejected ID number can be used again, another employee or a supervisor must successfully verify at the HandPunch.

- If you enter your ID number, but do not place your hand on the platen, the HandPunch will time-out in about 25 seconds. You can immediately end this time-out by the **CLEAR** key.

Beeper and LED Status During Verification

The HandPunch’s beeper and LED status display also displays hand verification information. This information is defined in Table 19 below.

Table 19: Beeper and LED Status During Verification

Operation	Beeps	LED	Meaning
During Keypad Entry	1 per Keystroke	–	Keystroke Accepted
After ID Entry	–	–	OK - Proceed
After ID Entry	2	–	ID Number Not in Database
After Hand Placement	1	Green	ID Verified
After Hand Placement	2	Red	ID Not Verified - Try Again
After Hand Placement	1 Long Continuous	Red	ID Refused

Glossary

Address, IP – An Internet Protocol address is a unique address assigned to a computer for communicating over a LAN/WAN. It is made up of 4 sets of numbers, separated by periods (for example, 123.245.78.901).

Address, HandPunch – A HandPunch Address is a unique identification number assigned to a HandPunch. Each HandPunch on a site must be assigned its own unique address.

AWG – American Wire Gauge is a U.S. standard set of wire conductor sizes. The "gauge" refers to the diameter of teh wire. The higher the gauge number, the smaller the diameter, the thinner the wire, and teh greater the electrical resistance. Thicker, smaller gauge wire carries more current because it has less electrical resistance over a given length. Thicker wire is better for long wire distances.

Daisy-Chain – A Daisy-Chaing is a method of wiring together HandPunch on a network, where the first HandPunch is connected to the second HandPunch, which is connected to the third HandPunch, and so on until the last HandPunch is reached.

End-of-Line (EOL) Termination – EOL Termination is a set of resistors attached to the data lines at the last HandPunch physically connected to a network. These resistors prevent data signal distortion and reflection back across the data lines, improving the integrity of the network connection.

HandPunch Address – see Address, HandPunch.

IP Address – see Address, IP.

Platen – The Platen is the flat surface at the base of the HandPunch, on which a user places his/her hand for enrollment and verification. The platen has guide pins to ensure the user's fingers are consistently positioned correctly.

Template – A Template is a set of data generated for a user. It is made up of the user's enrollment information and any system configuration parameters that are assigned to the user. The template is stored at each HandPunch and can be stored at the host computer with the Time and Attendance software.

Time Zone – A Time Zone is an identified period of time, during which a user is allowed to punch in our out at a HandPunch. Punch attempts outside of that time period are rejected by the HandPunch.

Transaction – A Transaction is any kind of event recorded at a HandPunch. Transactions may include In or Out punches, department transfers, and supervisor edits.

Wiegand™ Reader – The term “Wiegand Reader” has two meanings depending upon its application. A true Wiegand reader reads a specially constructed card made up of small pieces of magnetic wire. As the card is swiped through the reader, the individual bits of wire generate a unique data signal. This data signal is made up of a Facility Code field (typically 8 bits), an ID number field (typically 16 bits), and parity bits (typically 2 bits) for a total of 26 bits of data. Now this 26-bit Wiegand data format has been adopted by a variety of card reader devices for entering user ID data. Other Wiegand formats (for example, 37-bit) are used as well.

Limited Warranty

Schlage Biometrics, Inc. (the “Company”) warrants to the original user the products manufactured by the Company (the “Product”) to be free of defects in material and workmanship for a period of one year from the date of purchase by usch user or 15 months from the date of shipment from the factory, whichever is sooner, provided:

1. The Company has been notified within such period by return of any alleged defective product, free and clear of all liens and encumbrances, to the Company or its authorized dealer, transportation prepaid; and

2. The Product has not been abused, misused, or improperly maintained and/or repaired during such period; and

3. Such defect has not been caused by ordinary wear and tear; and

4. Such defect is not the result of voltage surges/brownouts, lightning, water damage/flooding, fire, explosion, earthquakes, tornadoes, acts of aggression/war, or similar phenomenon; and

5. Accessories used as integral to the Product have been approved by the Company.

The Company shall, at its option, either repair or replace, free of charge, the Product found, upon the Company’s inspection, to be so defective, or if agreed upon, refund the purchase price, less a reasonable allowance for depreciation, in exchange for the Product.

THE COMPANY MAKES NO OTHER WARRANTY AND ALL IMPLIED WARRANTIES INCLUDING ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE ARE LIMITED TO THE DURATION OF THE EXPRESSED WARRANTY PERIOD AS SET FORTH ABOVE.

THE COMPANY’S MAXIMUM LIABILITY THEREUNDER IS LIMITED TO THE PURCHASE PRICE OF THE PRODUCT. IN NO EVENT SHALL THE COMPANY BE LIABLE FOR ANY CONSEQUENTIAL, INDIRECT, INCIDENTAL, OR SPECIAL DAMAGES OF ANY NATURE ARISING FROM THE SAME OR THE USE OF THE PRODUCT.

Schlage Biometrics, Inc. reserves the right to make changes in the design of any of its products without incurring any obligation to make the same change on units previously purchased.

Ingersoll Rand
Security Technologies

Ingersoll Rand's Security Technologies Sector is a leading global provider of products and services that make environments safe, secure, and productive. The Sector's market-leading products include electronic and biometric access control systems; time and attendance and personnel scheduling systems; mechanical locks and portable security, door closures and exit devices, steel doors and frames, architectural hardware and technologies and services for global security markets.

866.861.2480

www.schlage.com www.ingersollrand.com

Schlage
Biometric Solutions
Ingersoll Rand Security Technologies
538 Oakmead Parkway
Sunnyvale, CA 94085
Office: 866-861-2480/512-712-1413 (international)
Fax: 866-303-1794/408-341-4101
E-mail: sbssupport@irco.com

GT-Series

Terminal User's Guide

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and, if not installed and used in accordance with the Installation Manual, may cause unwanted interference to radio communications.

Operation of this equipment in a residential area is likely to cause unwanted interference, in which case the user will be required to correct the interference at the user's own expense.

This Class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numerique de la classe A respecte toutes les exigences du Reglemente sure le materiel brouilleur du Canada.

Document Part Number: 70100-7500 – Revision D – March 2012

Recognition Systems Company, LLC (dba Schlage Biometrics)

Schlage Biometrics reserves the right to change, without notice, product offerings or specifications.

Table of Contents

Introduction 1

Using the GT-Series Terminal

The GT-Series Terminal is the first member of the Schlage G-Series biometric hand geometry time and attendance terminals. The GT-Series Terminal records and stores the three dimensional shape of the human hand for comparison and identity verification. Upon verification, the terminal records the time, date, user ID number and collected time and attendance data and makes this information available for collection by a host computer. The terminal can produce an output to operate an auxiliary device, such as an electronic door lock or signal bell, and it can communicate with a host computer. The terminal also has auxiliary inputs that can be used to control other systems.

A third-party/custom host application communicates with GT-Series Terminals across a TCP/IP network, maintaining and storing data collected by the terminals, analyzing and updating data, maintaining security and initiating alarms as necessary. Access to this data is achieved through a web browser or custom application. The GT-Series Terminal provides employee identification verification and includes the sophisticated operating features one expects in a time and attendance terminal. Because of this unique combination of capabilities, the GT-Series Terminal provides the most accurate and flexible time and attendance data collection terminal available.

Using Biometrics

As with the GT-Series Terminals, Schlage offers hand geometry terminals which are one of the most widely used biometric technologies for time and attendance applications. Hand geometry technology uses the size and shape of the person’s hand to verify the user’s identity. Schlage biometric solutions also offer multi-authentication options. Smart card, proximity and magnetic stripe readers can be integrated into the terminals to provide an extra layer of security customized to the application requirements. Some of the world’s largest providers of time and attendance systems recommend Schlage HandPunch terminals as part of their total solution. By using biometric technology, corporations reduce payroll costs and eliminate “buddypunching” fraud.

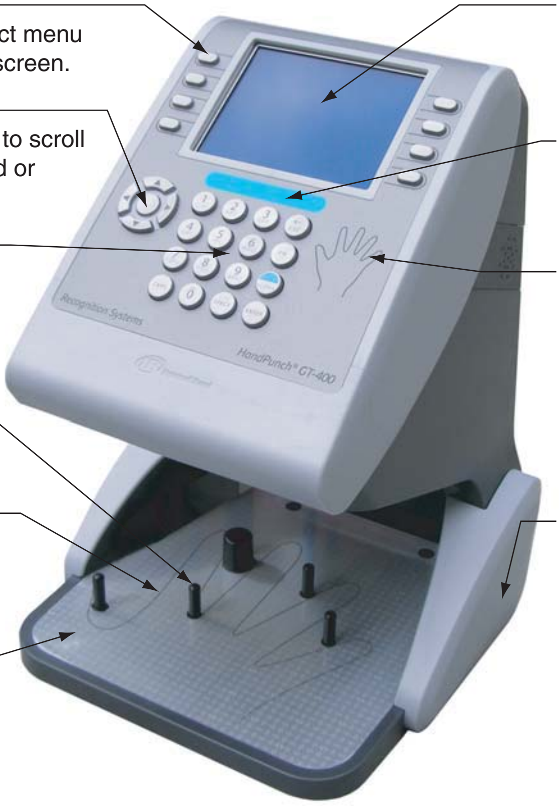
How GT-Series Terminals Operate

The GT-Series Terminal uses low-level infrared light, optics and a CMOS (IC chip) camera to capture a three-dimensional image of the hand. Using advanced microprocessor technology, the terminal converts the image to an encrypted electronic template. It stores the template in a database with the user’s ID number. To gain access, the user enters his or her ID number using the terminal keypad or uses an optional, built-in card reader. The terminal prompts the user to place his or her hand on the terminal’s platen. The terminal compares the hand on the platen with the user’s unique template. If the templates match, the terminal records the transaction for processing.

Verification with GT-Series Terminals

Verification refers to the process of placing the hand on the terminal platen as a part of the authentication process. Authentication consists of entering a user identification number on the terminal's alpha-numeric keypad and verification of the hand.

GT-Series Terminal Features



Function Keys
Function keys are used to select menu options displayed on the LCD screen.

Navigation Keypad
The navigation keypad is used to scroll through lists or to move forward or backward in text fields.

Alpha-Numeric Keypad
The alpha-numeric keypad is used to enter text or numbers into the terminal.

Finger Pins
Finger pins are used to position the hand on the terminal platen.

Hand Placement Outline
The hand placement outline is a visual guide for hand placement on the terminal platen.

Platen
The platen is the surface upon which the hand is placed for verificaton.

LCD Screen
The LCD screen shows menus and messages on the terminal.

LED Bar
The LED bar gives a visual indication of terminal status.

Hand Placement Guide
The hand placement guide gives a visual indication of hand placement on the platen. Red LED indicators light when fingers are not in the correct position in relation to the finger pins.

Side Cover
The side covers are removable to access screw holes for mounting the terminal to the wall plate.

GT-Series Terminal Specifications

Table 1-1: GT-Series Terminal Specifications

Specification	**Description**
Size	8 inches (20.32 cm) wide by 11.18 inches (28.40 cm) high by 7.52 inches (19.10 cm) deep
Weight	5.60 lbs (2.54 kg) – 6.90 lbs (3.13 kg) with optional backup
Power	12 VDC nominal (10.8 to 13.5 VDC), 4.5 Watts max. linear power supply recommended
Transient Protection	8,000 volts – all terminals
Reverse Voltage	on power input
Environment	Operating: 32°F to 113°F (0°C to 45°C) Relative Humidity: 5% to 95%, non-condensing Non-operating (storage): -40°F to 185°F (-40°C to 85°C)
Verification Time	less than one second
Date Retention	3 years using a standard internal lithium battery
Transaction Buffer	memory card-dependant
Baud Rate	9600 to 115200 bps
Communications	TCP/IP over Ethernet – 10/100 Base T
Function Keys	8 programmable soft keys
Alarm Monitoring	Unit Tamper
Relay Output	1 – 250 VAC @ 10A
Battery Backup (optional)	2 hour minimum run time

Reviewing GT Series Terminal Operations

Command Menus

Command menus are the menus in the terminal that are used to configure the terminal. The command menus can be accessed by pressing ← ESC and then ENTER from the Ready screen. If the terminal is a new terminal and has no users, the command menus will immediately appear. After the administrator has been created and enrolled, verification will be required to access the command menus.

Using the GT Series Terminal Keypad

There are three types of keys used to make entries into the terminal. Each will be indicated in this guide as shown below.

Table 1-1: Types of Terminal Keys and Corresponding Symbols

Type of Key	Location and Purpose	Symbol
Function Key	These keys are located on both sides of the terminal screen. They are used to navigate through the command menus	⬭
Alpha-Numeric Key	These keys are located in the terminal keypad. They are used to enter letters and numbers into the terminal.	1 .-+
Navigation Pad	These keys are located to the left of the terminal keypad. They are used to navigate through lists displayed on the terminal screen. The middle key can be used as an "Enter" or "Select" key.	◎

Important Information for Installers and Terminal Administrators 2

NOTE: Field installers and terminal administrators should read this section thoroughly before attempting to install or configure a GT-Series Terminal site. It explains important concepts and lists required administrative terminal operations.

Network Setup and Ethernet Switches

For best performance, it is recommended that you use ethernet switches to connect the terminal(s) to the host, rather than ethernet hubs. Using ethernet hubs to connect the terminal(s) to the host may lead to terminal instability. If instability is encountered while using ethernet hubs, you may need to reboot the terminal(s).

➡ ***See "Rebooting the Terminal Using the Terminal Interface" on page 53 for more information.***

Power-on and Shutdown Precautions

- If your terminal is equipped with a backup battery, it should be connected after power has been applied to the terminal.

➡ ***See "Making Back Board Connections" on page 31 for more information.***

- The network (ethernet) cable must be connected to the terminal before applying power. The terminal establishes itself on the network during start-up. You will not be able to communicate with the terminal if the cable is not connected before applying power. Other connections, including optional USB, or serial or auxiliary relay connections, should also be made before applying power.

❗ ***The terminal must not be disconnected from its power source without shutting down the application first. See "Shutting Down the Terminal" on page 44 for more information.***

Using the Terminal Command Menu

The terminal command menu allows you to manage your terminal and perform a variety of associated administrative tasks. To be able to access command mode you must be enrolled with administrative level privileges (level 5).

➡ ***It is assumed that the first person to use a new terminal would be the administrator. As such, the first person to access the Command Menu will by default be able to access this menu.***

➡ ***See "Command Menu Reference" on page 55 for more information.***

Synchronizing the Reader Before Enrolling Any Users

The reader must be synchronized with a host server before creating any content, such as enrolling users. If users are created on a reader before the first synchronization, those users will be deleted from the reader.

➡ ***See "Sync Now" on page 108 for more information.***

Terminal Configuration Options

There are three ways to configure a new terminal. The table below lists each of the three methods for terminal network setup, as well as information on which situations to which each method best applies.

➡ ***Terminal configuration tasks are described in more detail in "Network Mode Configuration" on page 37.***

❗ ***When the terminal is configured for network connection any existing data (including users) will be deleted.***

Figure 2-1 Terminal Configuration Options

Setup Option	Do I need to use this?	When do I use it?	Usage Guidelines
GManager or equivalent. (Your customized Host Application which uses the Discovery feature)	Yes, if: 1. The terminal has application software installed on it OR 2. The default BSP or application software that comes on the terminal needs to be updated No, if 1. The terminal already has the BSP and application software on it AND 2. No upgrades to the terminal's BSP or application software are required	During terminal software updates or terminal start-up with a computer.	When there are a number of terminals in varying physical or geographical locations (but on the same LAN) the GManager Discovery feature can set them up quickly and efficiently.
Terminal Web Server	Yes, if the GManager discovery feature was not used to configure the terminal. No, if the GManager discovery feature was used to configure the terminal.	After the terminal application has started, from a web browser.	The web server is one of the is the fastest ways to set up terminals, provided that the application is already present on the terminal.
Terminal Command Menus	Yes, if the GManager discovery feature was not used to configure the terminal. No, if the GManager discovery feature was used to configure the terminal.	After the terminal application has started, using the terminal's keypad.	If the GManager discovery feature and the terminal web server are not viable options, then the terminal's user interface can be used.

Start-up Sequence

When you apply power to a terminal, it goes through the start-up sequence. First the operating system loads. Then the terminal checks to see if there are any software updates (from the host application). Finally, the terminal application loads.

The table below describes the stages of the start-up sequence and the available options for configuration (shown in the red columns):

Configuration Options

Stage	Description	Terminal Behavior	GManager Discovery Feature	Command Menus	Web Server	Options
1	Operating System Loading	LED Flash Cycle				N/A
2	Software Update	Single beep, followed by messages on the terminal screen	Yes**			Press FN for more time Press ESC and ENTER to skip this stage.
3	Terminal Application	"Enter ID", date and time displayed on the terminal screen		Yes	Yes	N/A
4	Terminal Synchronization					N/A

**Each connection attempt may take up to three (3) minutes. During that time, the terminal may appear to be unresponsive. Wait for three (3) minutes for the terminal's processes to time out before attempting to perform any other actions.

The following steps describe the stages of the start-up sequence:

1. Operating System Loading
   - Description: Terminal screen illuminates and LED bar cycles through its colors
   - Duration: 30 seconds
   - Completion: the LED bar turns blue

2. Software Update

   ➡ ***If you are opting to use the GManager Discovery feature to configure your terminal, you would use it during this stage. This feature is not available if you are using a new "out-of-the-box" terminal which has not yet been configured in GManager.***

   - Description: The terminal checks the host server to see if it needs to download any updates to its software. This application functions only if the terminal is connected to a network that is also running a host application. Software updates should be loaded into the host application.
   - Duration: 1 second (if skipped) up to 10 minutes (if configured here and software is downloaded)
   - Completion: if not skipped, it is completed when no updates are found on the host server

3. Terminal Application loads

   ➡ ***If you are opting to use the terminal's web server or terminal command menus to configure your terminal, you would use one or the other after this stage.***

   - Description: The time and attendance application starts
   - Duration: approximately 2+ minutes
   - Completion: the date and time are displayed on the terminal LCD

4. Terminal Synchronization

   - The terminal performs a full synchronization with the host application.

   ➡ ***See "Sync Now" on page 108 for more information.***

Server Network Considerations With Firewalls/Security Software

Your network configuration may be configured with firewalls or security software that is designed to report or deny certain operations. For this reason, certain features and commands in the GT-Series Terminal (listed below) may not work, or cause the terminal to be inoperable if your network denies those actions. These include:

- The terminal's XML-RPC server

  ➡ ***See "XMLRPC Svr Setup" on page 78 and "Set XMLRPCSvr Port" on page 77 for more information.***
- The terminal's web server

  ➡ ***See "Set WebSvr Port" on page 79 for more information.***
- The terminal's CLI server (if accessed outside of telnet)

  ➡ ***See "CmdLine Setup" on page 62 for more information.***

  ➡ ***If the CLI is accessed with telnet, it will function normally.***

If you want to use any of these features, it is recommended that you test them on your network to make sure that they function before using them in a live installation. If any of these features do not work, they can easily be disabled through the terminal command menus, or through your host application. None of these features are required for database synchronization.

Clearing Interactions

Interactions that have *not* been sent are saved on the terminal indefinitely. Therefore, interactions must be periodically purged in order to make room for new interactions. The terminal administrator should create a schedule for purging interactions.

If interactions are not cleared on a schedule, and the SD card gets close to being full, the terminal will display the message, “SD Card Capacity Low”. This message will occur first when the SD Card capacity is 30% full. When this message is displayed, interactions should be cleared immediately. The reader will stop accepting punches when it is 45% full.

❗ ***If the SD card becomes full, users will not be able to punch until the interactions are cleared. Administrator operations and command menu accesses are not affected when SD card is full***

The Delete Sent Interactions function will clear only those interactions that have been sent to the host application. See “Delete Sent Interactions” on page 111 for more information.

Precautions When Moving a Terminal Between Different Hosts

➡ ***The following information assumes that you, as the administrator, have familiarized yourself with OBJIDs and managing a terminal’s database. For more information on these topics, see the GT-Series Terminal Terminal Network Guide.***

Before disconnecting a terminal from one host and connecting to another host, the terminal’s database must be reset.

> ***IMPORTANT:*** ***If you do not delete a terminal’s database, it will have objects with OBJIDs assigned in a range that the previous host application assigned, and which the new (current) host application has no knowledge. As such, you could potentially corrupt your new host database with objects that have duplicate OBJIDs.***

Use one of the following options when moving a reader to another host:

1. Delete the reader database before changing the host.
2. Reset the reader database to factory settings using the reader GUI.
3. Change the logical name of the reader on the new host to which you will connect the reader.

Terminal Installation 3

GT-Series Terminal Installation

Terminal Placement

The recommended height for the terminal's platen is between 40 and 48 inches (102 - 122 cm) from the finished floor. This height conforms to the Americans with Disabilities Act (ADA) standards (40 inches is recommended for ADA standards). All terminals within a site should be placed at the same height.

The terminal should be out of the path of pedestrian and vehicular traffic.

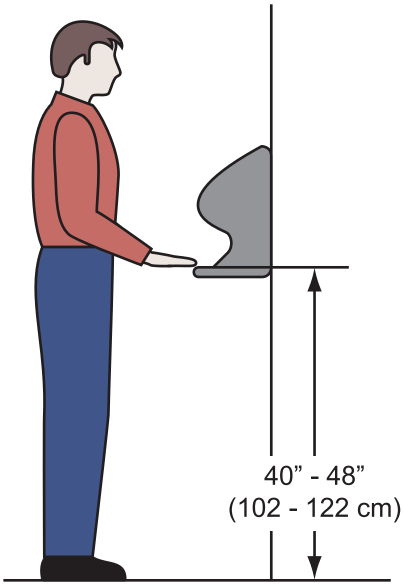


Figure 3.2— GT-Series Terminal Installation Height

Make sure that the terminal is not exposed to excessive airborne dust, direct sunlight, water or chemicals.

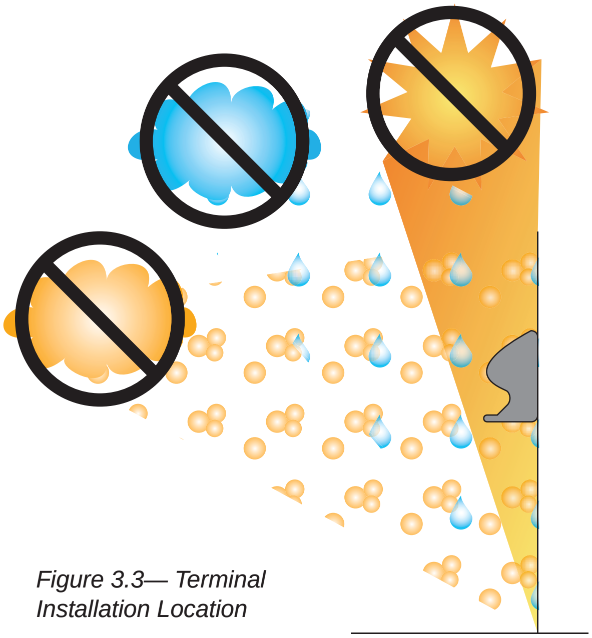


Figure 3.3— Terminal Installation Location

Removing the Terminal from the Box

1. Remove any accessories from the box.
2. Remove the packing materials from the top of the terminal.
3. Life the terminal from the box. Do not touch the underside of the terminal face.

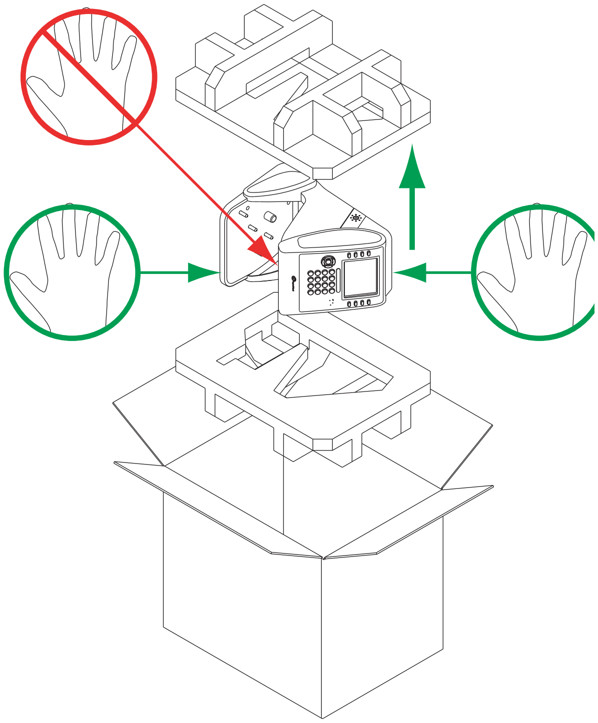


Figure 3.4— Removing the Terminal from the box

Wall Preparation

❗ ***These directions and provided hardware are for installation on a hollow wall only. For installation on a solid wall, other means should be used.***

1. Measure and mark a point 49 inches (124.5 cm) from the surface of the finished floor.

➡ ***This point is used by the leveling hole where the top-center point of the terminal should be mounted. At 49 inches, the unit's platen will be 40 inches from the floor.***

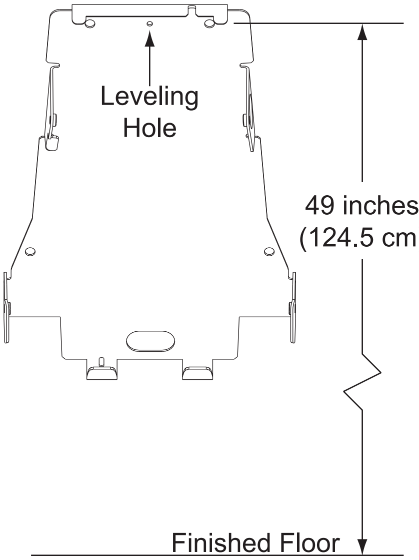


Figure 3.5— Measurements for Terminal Installation

2. Drive a small nail into the wall at the mark.

➡ ***For a solid wall, pre-drill a 1/8" hole. Insert nail into the hole.***

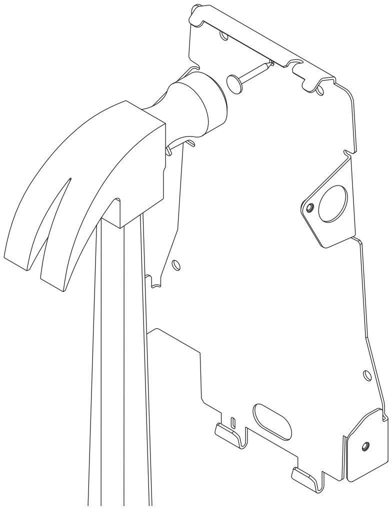


Figure 3.6— Leveling the Terminal (Step 1)

3. Hang the wall plate from the leveling hole located near the top of the wall plate.
4. Use a bubble level to ensure that the wall plate is level.

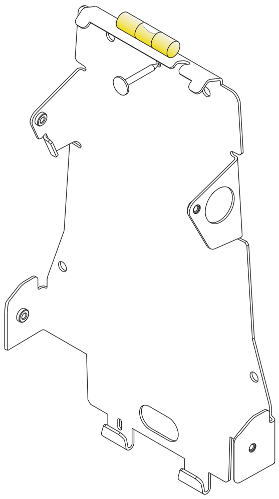


Figure 3.7— Leveling the terminal (step 2)

5. Mark the location of the two upper mounting holes and the two lower mounting holes.

➡ ***For a concealed wiring connection through the wall, mark the rear cable entry hole on the wall plate.***

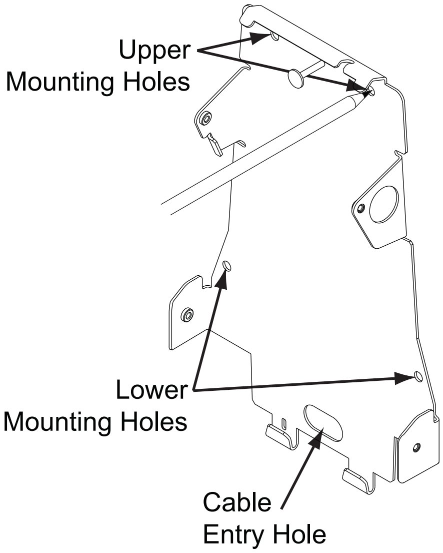


Figure 3.8— Marking to mount the holes

6. Remove the wall plate and nail.
7. Drill upper and lower mounting holes.

   For a concealed wiring connection, drill a 1/2” hole in the center of the outlined rear cable entry hole.

➡ ***Additional holes may be drilled to enlarge the hole for concealed wiring connection if necessary.***

8. Clear all dust and debris away from the terminal mounting location.

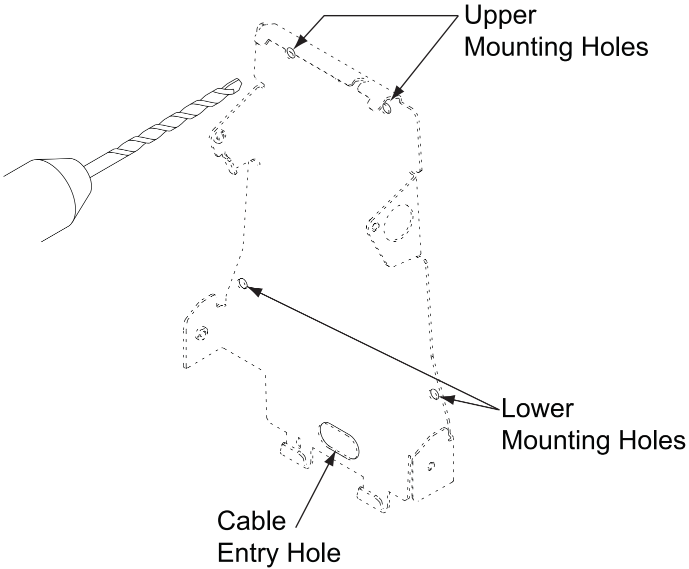


Figure 3.9— Drill holes

Attaching the Wall Plate

❗ ***These directions and provided hardware are for installation on a hollow wall only. For installation on a solid wall, other means should be used.***

1. Pull all wires through holes in wall (if necessary) and make sure wires are clear of wall plate.
2. Install the four fasteners that have been provided into the mounting hole locations. Then use the four provided screws to attach the plate to the wall.

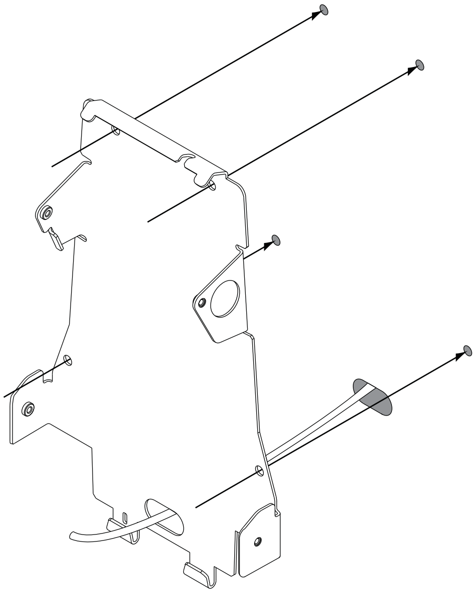


Figure 3.10— Attaching the Wall Plate

Hang Terminal and Run Wires

1. If the side covers are attached to the terminal, they must be removed before hanging the terminal on the wall plate.

➡ ***See "Removing/Installing Side Covers" on page 34 for more information.***

2. Slide slots in terminal over hooks on wall plate. Allow terminal to rest against the wall while performing the following steps.

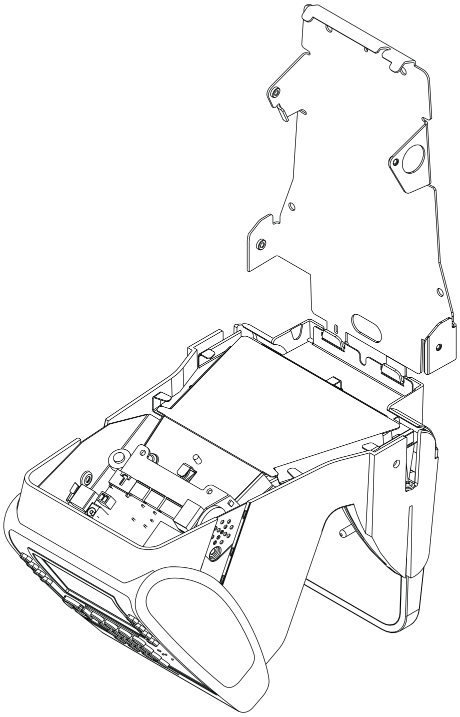


Figure 3.11— Hang the terminal from the Wall Plate

3. There are several options for running the wiring a. Run wiring through hole in wall plate.
   a. Run wiring through hole in wall plate.
   b. Run wiring through slot in terminal.
   c. Run wiring through battery cover (material removal required).

➡ ***If using option c, locate indentation in battery cover, drill 1/4” hole in battery cover indentation and use utility knife to remove excess material.***

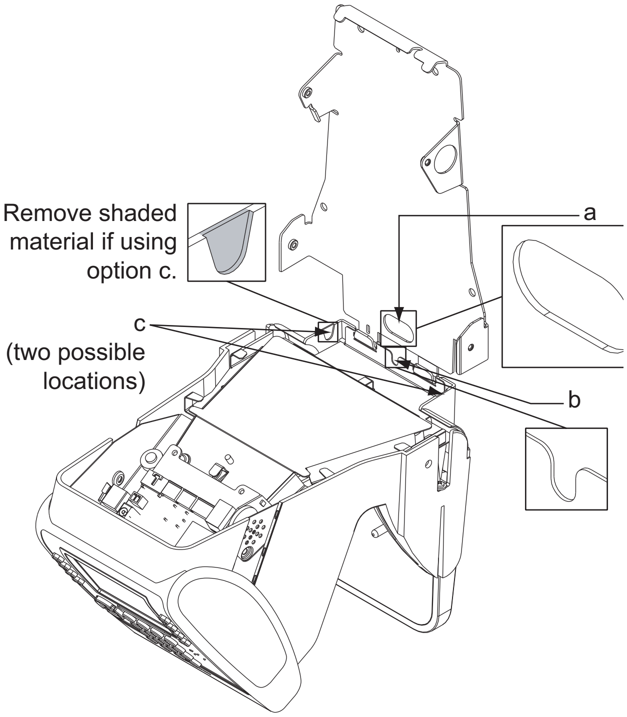


Figure 3.12— Terminal Wiring Options

4. Tuck wires under tabs on terminal to minimize risk of crimping wires.
5. Follow all local electrical codes when routing wire and making the terminal connections.

➡ ***For concealed wiring, pull the terminal wiring through the 1\2” cable entry hole.***

➡ ***Ensure there is at least twelve inches of extra cable beyond what is needed to make the required connections to the back board.***

➡ ***For conduit wiring, pull an extra twelve inches of cable through the conduit beyond what is needed to make the required connections to the back board.***

➡ ***You may need to run the cable and then attach the connectors in order to fit cables through necessary holes and/or slots.***

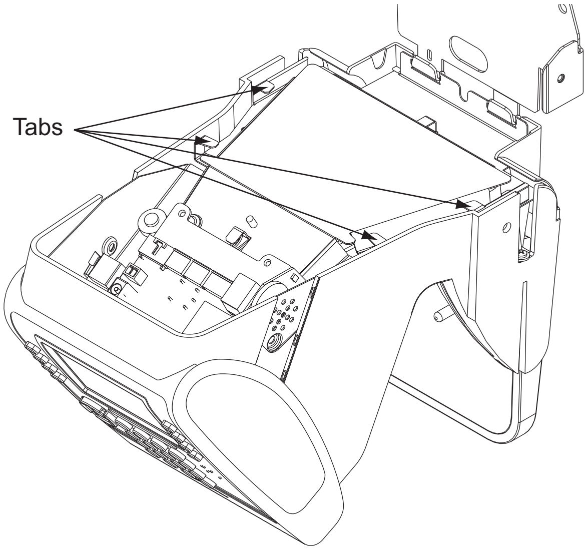


Figure 3.13— Wire Tabs

Making Back Board Connections

Use caution when making connections to the back board to avoid damage. Be aware of possible damage due to electrostatic discharge (ESD). ESD is of particular concern when working on carpeted surfaces and in dry environments. Use a ground strap to minimize ESD concerns.

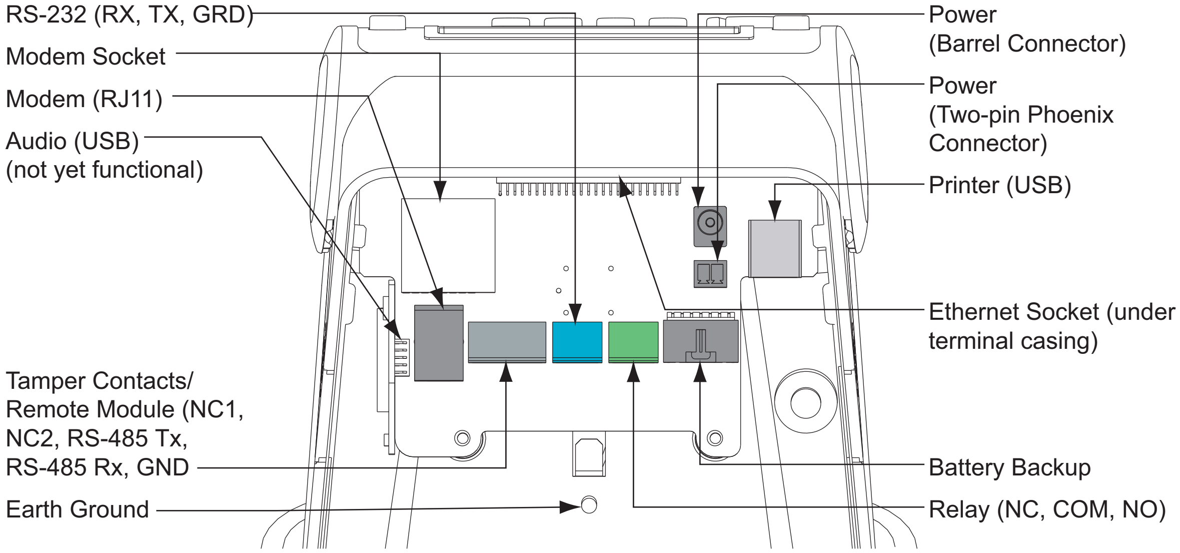
DO NOT apply power until you are ready to configure the terminal!

DO NOT connect backup battery (if using) until after main power has been supplied!

1. Connect the earth ground. The earth ground connection is made to the ground pin on the terminal. Bundle all ground connections into one crimp lug and attach the lug to the ground pin with a 8-32 nut.
2. Connect the ethernet cable to the ethernet connection socket inside the terminal casing.
3. DO NOT apply power until you are ready to configure the terminal! Connect the P1 plug to the twisted pair per the following: Pin 1: Ground, Pin 2: Power.

➡ ***See "Important Information for Installers and Terminal Administrators" on page 17 for details.***

4. If using the optional backup battery, locate the backup battery relay, but DO NOT connect backup battery until after the main power has been connected.
5. Make other back board connections as necessary. Use the diagram below as a reference.



Back Board Connections

Attaching the Ferrite Clip

The ferrite clip must be attached to the terminal's power cord in order to be FCC-compliant.

1. Make a loop in the power cord approximately six (6) inches from the power supply.

➡ ***The loop will keep the clip from sliding on the power cord.***

2. Clamp the ferrite clip over the loop. Make sure the tabs fully engage.

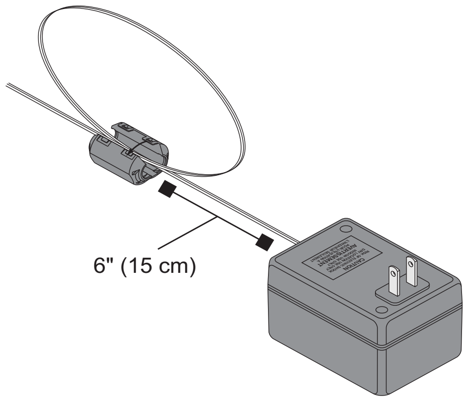


Figure 3.14— Attaching the Ferrite Clip

Printer Setup (Optional)

You may want to install a printer to provide a paper receipt of each user booking. A booking is the interaction that is recorded each time a user punches in or out of the terminal.

➡ ***The print format on the booking receipt can be customized. See "Print Setup" on page 59 for more information.***

➡ ***If you want to install a printer after initial terminal setup, you will need to shut down the terminal first and then perform the following steps. See "Shutting Down the Terminal" on page 44 for more information.***

➡ ***At the time this user's guide was printed, only the Epson USB Receipt printer is supported.***

1. Connect the receipt printer to the terminal's USB port.
2. Power on the receipt printer.

❗ ***The receipt printer must be powered on and connected to the terminal via the USB port before the terminal is powered on.***

After you have powered on and configured the terminal, perform the following:

1. Enable PrintBookings.

➡ ***See "Set PrintBookings" on page 60 for more information.***

2. Set the baud rate.

➡ ***See "Set Baud Rate" on page 60 for more information.***

3. Enable printing on the host application.

By default, the terminal will print the following on the receipt:

- Date and time of booking
- User name
- User's credential ID
- Verification result
- Punch status (in or out)

Removing/Installing Side Covers

The side covers must be removed in order to attach the terminal to the wall plate.

➡ ***The terminal may be shipped without the side covers attached.***

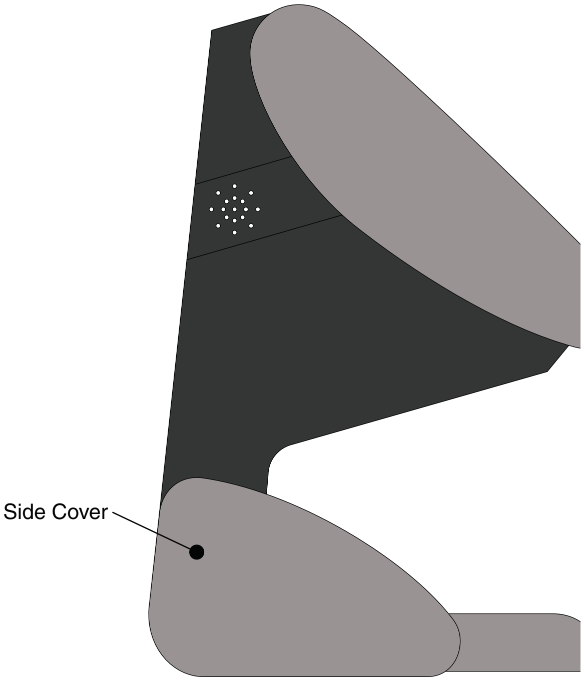


Figure 3.15— Terminal covers

Removing Side Covers

1. Locate slot on bottom of side cover. Insert a small screwdriver into slot.
2. Rotate screwdriver gently. Side cover will pop off.

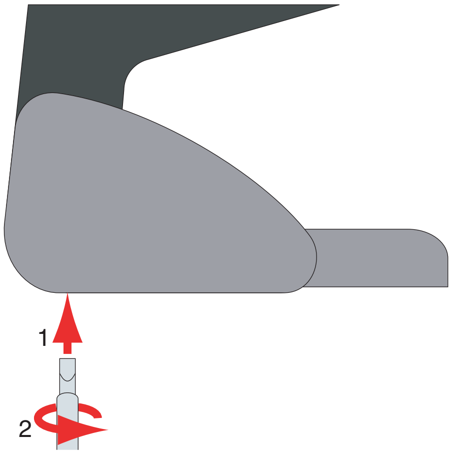


Figure 3.16— Removing the side covers

Installing Side Covers

1. Place outside ridge of side cover under edge of terminal body.
2. Rotate side cover toward terminal body and snap into place.

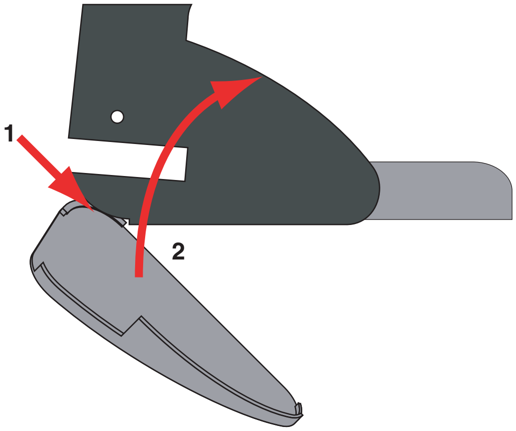


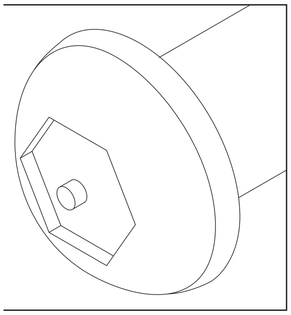
Figure 3.17— Installing the side covers

Attaching the Terminal to the Wall Plate

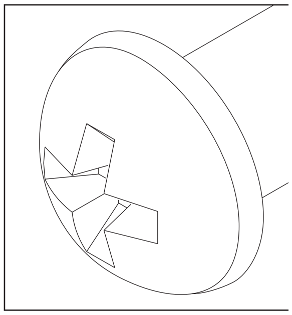
Remove any dust and debris from the mounting site before attaching the terminal. Dust and debris can seriously affect the performance of the terminal.

1. Choose the standard Phillips head screws or the security head screws for installation.

A special tool is required to install and remove a security head screw.



Security Head Screw



Phillips Head Screw

2. Terminal should already be hanging from wall plate.
3. Rotate terminal toward the wall plate. Make sure not to pinch or damage any wiring.
4. Make sure that the screw holes in the body of the terminal are aligned with the screw holes in the wall plate.
5. Install two (2) screws into the lower screw holes.
6. Attach side caps.

See "Installing Side Covers" on page 35 for more information.

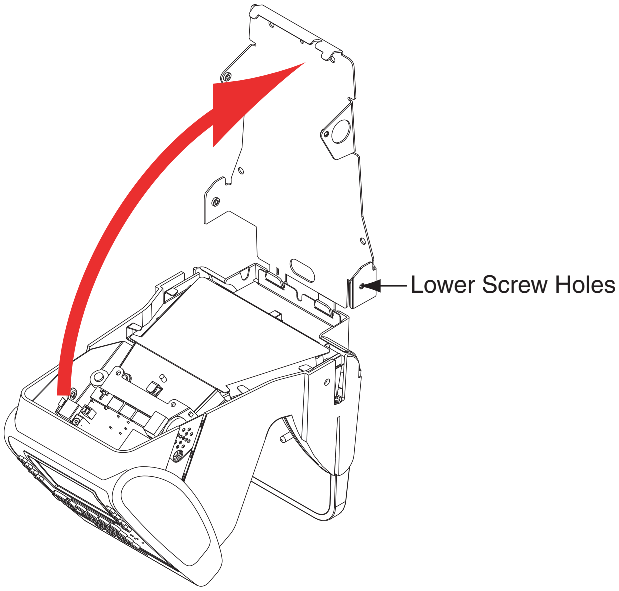


Figure 3.18— Closing the Terminal

Setting Up the GT-Series Terminal 4

Network Mode Configuration

You can configure terminals for network mode in 3 ways, as described in this chapter:

- Using the terminal command menus from the terminal user interface
- Using the terminal's web server
- Using your host application's customized interface (if provided)

➡ ***For a comparison of the three options, see "Terminal Configuration Options" on page 19 for more information.***

After configuring the terminal, you can then verify that the reader is configured properly to synch with the host. This is described in "Verifying Synchronization with the Host Application" on page 40.

NOTE: Make sure that your host application is running and your terminal is powered up before configuring the terminal. You must logged in as the administrator in order to configure a terminal.

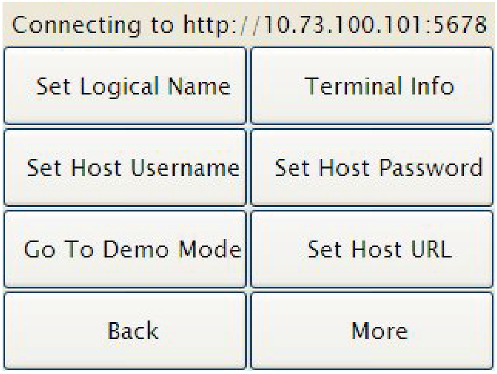
! ***Do not apply power to the terminal until you understand the network setup procedures.***

NOTE: The terminal should be synchronized with the host application before creating any content on the terminal. If content is created on the terminal before it is synchronized with the host application, content may be lost when synchronization occurs.

Using the Terminal's Command Menus for Configuration

If the terminal is not yet configured, only the command menus that are needed to configure a terminal for synchronization will be displayed when ESC and ENTER are pressed. See Figure 4-1.

Figure 4-1 Using the Network Setup Menu for Terminal Configuration



Connecting to http://10.73.100.101:5678

1. Configure the following terminal network settings using the terminal interface:
   - Set Host Password

     Use the alpha-numeric keypad to enter the host password. The password must match the password of a valid host account.

     See "Set Host Password" on page 74 for more information.
   - Set Host URL

     Use the alpha-numeric keypad to enter the host URL (Host Server's IP address). The entire address must be entered (including "http://").
     Example: http://192.168.1.25.

     See "Set Host URL" on page 75 for more information.
   - Set Logical Name

     Use the alpha-numeric keypad to enter the name of the terminal. It must match the name of the terminal created on the host server.

     See "Set Logical Name" on page 71 for more information.
   - Set Host Username

     Use the alpha-numeric keypad to enter the username. It must match a username of a valid host account.

     See "Set Host Username" on page 72 for more information.
2. Wait until the terminal LED turns blue, indicating host application has been found.
3. Verify the date and time on the terminal. They will agree with the host logical terminal locale time setup if the terminal is synchronizing.
4. If necessary, verify database synchronization.

   See "Verifying Synchronization with the Host Application" on page 40 for more information.

Using the Terminal's Web Server for Terminal Configuration

1. Open an internet browser.
2. Enter the terminal's IP address in the URL address bar using the format:

   `http://`<*terminal IP address*>

   Example: `http://100.73.100.193`

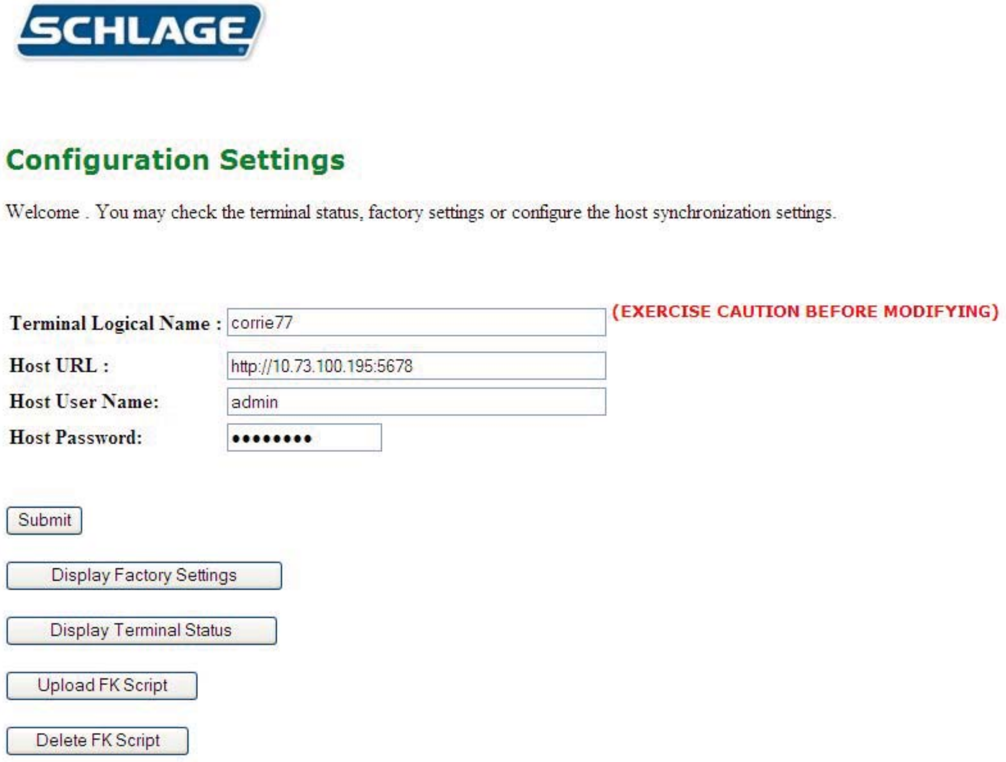
   - If the terminal has never been on a network the terminal default IP address is 192.168.1.110.
   - If the terminal has previously been on a network, it will have been automatically assigned an IP address through DHCP. You can find this information by using the terminal status menu option on the reader. (See "Check the Terminal Status in the Terminal Command Menus" on page 40).

3. The web server home page will prompt you for a Credential ID and an EPIN. On initial startup, the default Credential ID is `root` and the EPIN is `Schlage538`.

   NOTE: This login account (root, Schlage538) will automatically self-destruct when the terminal completes its first synchronization or when there is a valid Administrator created for the reader. Any future attempts to log in to the terminal's web server must be with a valid administrator user record, and the user record must contain a user-determined EPIN.

4. From the web server main page (Figure 4-2) set the terminal logical name, which must be the identical logical name set during terminal creation on the host application. The logical name can be found through the host or by checking the terminal status on the reader (see "Check the Terminal Status in the Terminal Command Menus" on page 40).

Figure 4-2 Terminal Web Server Main Page



Configuration Settings

Welcome . You may check the terminal status, factory settings or configure the host synchronization settings.

Terminal Logical Name : corrie77 (EXERCISE CAUTION BEFORE MODIFYING)

Host URL : http://10.73.100.195:5678

Host User Name: admin

Host Password: ••••••••

5. Set the Host URL to `http://`*`host machine's IP address`*.
6. Set the Host User Name to the user name set during the host application installation.
7. Set the Host password to the password set during the host application installation.
8. Click **Submit**.
9. An update confirmation should appear indicating that the entered fields were updated.
10. Click **Back**.

11. Check the LED bar to ensure it has turned blue. (This may take a minute.)
12. Click on **Display Terminal Status**.
13. Check the DB Synchronization Status field to verify that a DBSync was completed successfully.

Using Your Customized Host Application (GManager) for Terminal Configuration

If your site has a customized host application (similar to the sample GManager host application provided with the GT-Series Integration Package) you can use this interface to configure your terminals. See your host application documentation for details.

Verifying Synchronization with the Host Application

There are a number of ways to quickly verify that your terminal is synchronizing with the host application, as described in the following sections.

Check the Terminal Status in the Terminal Command Menus

1. Press ⬭ Maintenance Menu.
2. Press ⬭ Terminal Status.
3. Scroll down until you can view DBSync Status and confirm that it displays *DBSync Completed*.

Change the Ready Screen Message

From the host application:

1. Change the ready string for the terminal
2. Run Sync Now.

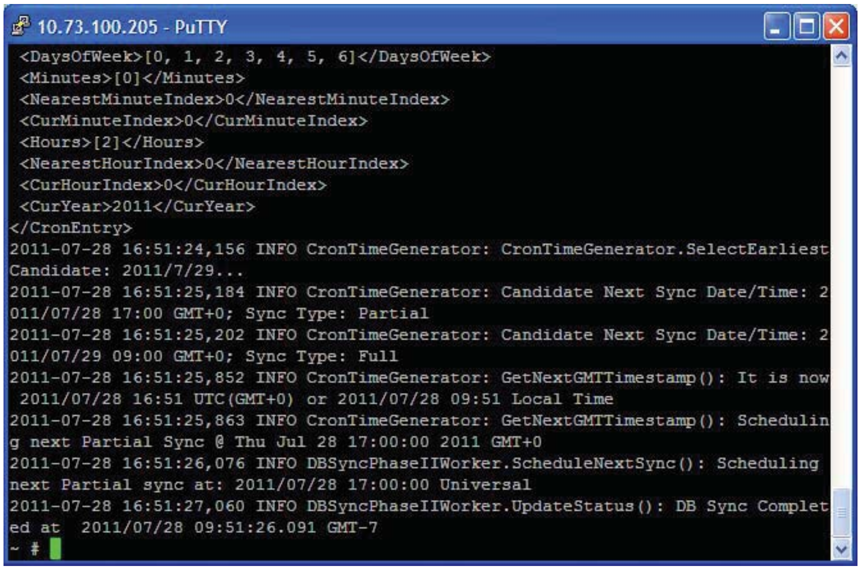
At the terminal, look at the LCD and verify that the ready string has changed

Check the RSITerm.log File From a Telnet Session

1. Start a telnet session with the terminal.

   See “Using Telnet” on page 125 for more information.
2. Type `cd /RecogSys/ZODB` and press **Enter**.
3. Type `cat RSITerm.log` and press **Enter**. Figure 4-3 shows an example of a successful DB Sync of the terminal.

Figure 4-3 Terminal Log File After Successful DB Sync



```
 <DaysOfWeek>[0, 1, 2, 3, 4, 5, 6]</DaysOfWeek>
 <Minutes>[0]</Minutes>
 <NearestMinuteIndex>0</NearestMinuteIndex>
 <CurMinuteIndex>0</CurMinuteIndex>
 <Hours>[2]</Hours>
 <NearestHourIndex>0</NearestHourIndex>
 <CurHourIndex>0</CurHourIndex>
 <CurYear>2011</CurYear>
</CronEntry>
2011-07-28 16:51:24,156 INFO CronTimeGenerator: CronTimeGenerator.SelectEarliest
Candidate: 2011/7/29...
2011-07-28 16:51:25,184 INFO CronTimeGenerator: Candidate Next Sync Date/Time: 2
011/07/28 17:00 GMT+0; Sync Type: Partial
2011-07-28 16:51:25,202 INFO CronTimeGenerator: Candidate Next Sync Date/Time: 2
011/07/29 09:00 GMT+0; Sync Type: Full
2011-07-28 16:51:25,852 INFO CronTimeGenerator: GetNextGMTTimestamp(): It is now
 2011/07/28 16:51 UTC(GMT+0) or 2011/07/28 09:51 Local Time
2011-07-28 16:51:25,863 INFO CronTimeGenerator: GetNextGMTTimestamp(): Schedulin
g next Partial Sync @ Thu Jul 28 17:00:00 2011 GMT+0
2011-07-28 16:51:26,076 INFO DBSyncPhaseIIWorker.ScheduleNextSync(): Scheduling
next Partial sync at: 2011/07/28 17:00:00 Universal
2011-07-28 16:51:27,060 INFO DBSyncPhaseIIWorker.UpdateStatus(): DB Sync Complet
ed at  2011/07/28 09:51:26.091 GMT-7
~ #
```

Demo Mode Configuration

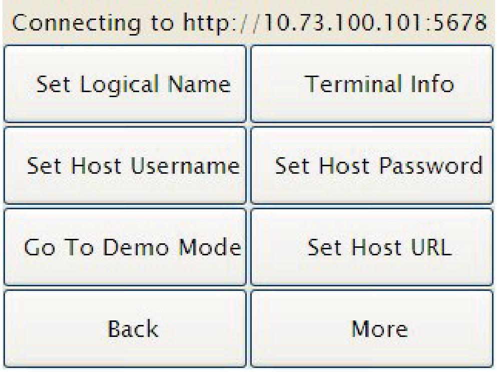
➡ ***If a terminal has never been connected to a host, you can switch directly from Terminal Mode to Demo Mode. If a Terminal has already been connected to a host and synchronized successfully, you can only switch directly to StandAlone Mode.***

NOTE: When the terminal is started for the first time, the Network Connection Setup screen will be displayed. When the terminal is not connected to a host application, synchronization will not occur and the terminal can be switched to Demo mode. For more information about using Demo Mode, see "Go to StandAlone or Demo Mode" on page 73.

You must logged in as the administrator in order to configure a terminal in Demo Mode.

1. Press ← ESC and then ENTER to access the Network Setup Screen. See Figure 4-4.

Figure 4-4 Network Setup Screen

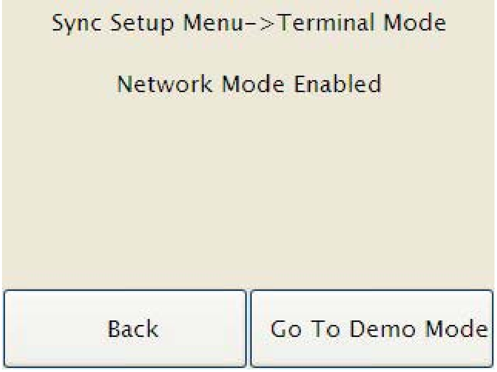


Connecting to http://10.73.100.101:5678

2. Press ⬭ Go to Demo Mode.

3. Press ⬭ Go to Demo Mode again. See Figure 4-5.

Figure 4-5 Selecting the Go To Demo Mode Option

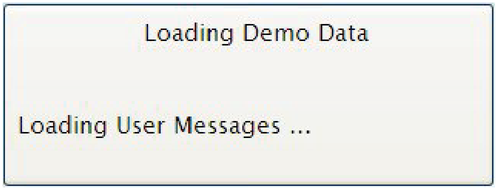


Sync Setup Menu–>Terminal Mode

Network Mode Enabled

4. Wait until the Terminal screen displays messages informing you that the reader is loading the pre-load Terminal databases, after which the terminal returns to the ready screen. See Figure 4-6.

Figure 4-6 Demo Mode Confirmation Message



Loading Demo Data

Loading User Messages ...

5. Configure the following terminal settings:

   ➡ ***The following settings can only be used when the terminal is in Demo mode or Standalone. Once you leave Demo Mode, these setting values will not be used in Network mode; instead they will be set by your host application.***

   a. Set Locale Time Zone.

      See “Set LocaleTimezone” on page 63 for more information.

   b. Set the date.

      See “Set Terminal Date” on page 61 for more information.

   c. Set the time.

      See “Set Terminal Time” on page 63 for more information.

Creating the Terminal Administrator Account

The first time the terminal is booted up, there are no user accounts. The first user account that is assigned to the terminal will be the terminal administrator account (with an authority level of 5). This can be changed later, but this account must be created before any other actions can be performed.

➡ ***The first user can be created using the host application. Once the user is assigned to the terminal, the user will be added to the terminal when the terminal synchronizes for the first time.***

➡ ***It is recommended that you create an EPIN for the terminal administrator account at this time. This will allow the terminal's web server to be used once the terminal is online. "Edit EPIN" on page 96 for more information.***

The terminal administrator account is created in the same way as other user accounts. This account can be created either from the terminal or from the host application. To create the terminal administrator account from the terminal, use the following instructions:

1. Add and enroll yourself as the administrator.

   ➡ ***See "Creating and Enrolling Users" on page 48 for more information.***

2. Change the authority level to 5.

   ➡ ***See "Edit Authority" on page 49 for more information.***

Shutting Down the Terminal

❗ ***DO NOT remove power without completing the shut down sequence!***

❗ ***If you have a terminal with the backup battery option, disconnect the main power first, then disconnect the battery.***

Shutting Down the Terminal Using the Terminal Interface

1. Log in to the terminal as an administrator.

   See "Creating the Terminal Administrator Account" on page 44 for more information.

2. Press ⬭ Maintenance Menu.
3. Press ⬭ Shutdown.
4. Wait until the LED bar is no longer lit.
5. You can now safely remove power from the terminal.

Shutting Down the Terminal Using Telnet

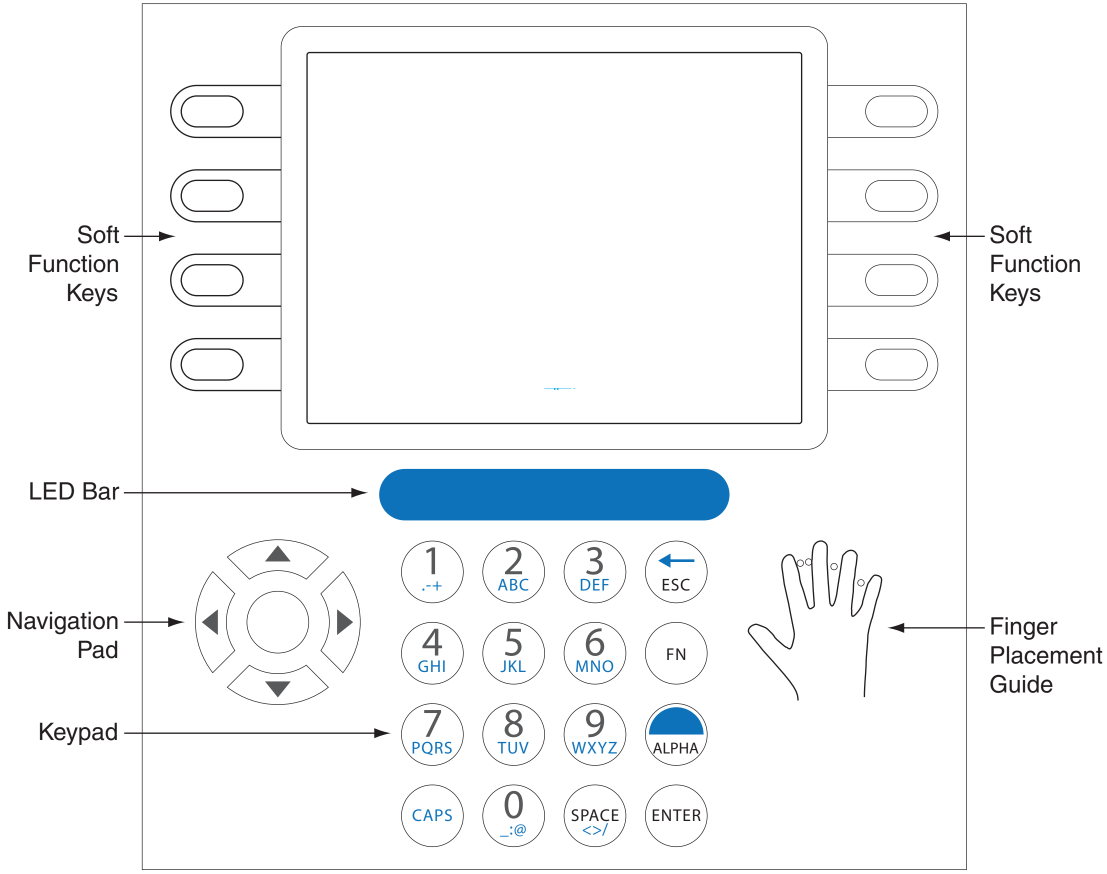
If the terminal cannot be shut down using the terminal interface use telnet to do so. See "Shutting Down the Terminal Via Telnet" on page 129.

Basic Operations 5

Reviewing the Terminal Front Panel and Interface

Figure 5-1 shows the front panel of the GT-Series terminal.

Figure 5-1 Front Panel of the GT-Series Terminal



Startup Screen

GT-Series Terminal Startup Screen

The first time you boot up the terminal, the "Hand" logo will appear. The hand logo will disappear after the terminal is completely booted.

Terminal Operation Tips and Tricks

Before using the terminal for basic operations, it is recommended that you review the following tips and tricks for a more successful experience with the GT-Series Terminal.

Terminal Time-Outs

The terminal will go back one screen level after ten (10) seconds of inactivity. The terminal will return to the default screen after thirty (30) seconds of inactivity. If you have been performing a function and fail to press a key for thirty (30) seconds, you will need to log in as an administrator again and start over.

Entering Text

- When you are using the keypad to enter text, such as a last name, press ALPHA to switch to alpha mode. Press CAPS to switch to capital letters. If you need to enter the same letter twice, wait a few seconds to proceed to the next letter, or use the navigation keys ◎ to proceed to the next letter.
- The navigation keys ◎ can be used to move between characters in alpha-numeric entry fields.
- Press ← ESC and ENTER from any command menu to return to the default screen.

Navigating a Long List

The terminal can sometimes contain long lists of items, such as time formats or users. There are some shortcuts that are useful for navigating through these lists.

- Press (FN) and (0) to skip to the top of the list.
- Press (FN) and (9 WXYZ) to skip to the end of the list.
- Press (FN) and (▼) to page down.
- Press (FN) and (▲) to page up.

Accessing Command Menus

Before performing any programming operations, you must be logged into the terminal as an administrator.

Administrator Authentication

Depending on the GT-Series Terminal model/configuration, use the appropriate set of instructions below.

Recommendation: Create an EPIN for the Terminal Administrator

As a best practice, you should create an EPIN for the terminal administrator. If the biometric camera encounters a failure, the terminal administrator will be able to access the command menus through use of the EPIN.

GT-Series Terminal Authentication

1. Press (← ESC) and then (ENTER).
2. When prompted, enter your Credential ID for the administrator account.
3. Place your hand for verification.
4. After successful verification, the COMMAND STRUCTURE menu will display from which you can make the appropriate menu selections.

Creating and Enrolling Users

Creating an ID Numbering System

An ID numbering system should be created before entering the first user into the terminal. ID Numbers (RPINs) are used during user enrollment and verification. Use the following guidelines when designing an ID numbering system.

- Each user must have a unique ID number (RPIN).
- All RPINs should be the same length.

➡ ***By making all RPINs the same length, users will not have to press ENTER after entering their RPIN, which can expedite processing. To do so, use the Set ID Length option as described in "Set ID Length" on page 64 for more information.***

- The RPIN should be as short as possible so users can remember their ID number. To make sure you will have enough unique RPINs, determine the length of RPIN by determining the number of users needed.

➡ ***For example, if you have 10,000 or less users, use a four-digit RPIN. If you have more than 10,000 users, use a five-digit RPIN.***

Creating a User from the Terminal

➡ ***If possible, it is more efficient to create users by using your host application. Refer to your host application documentation for more information.***

➡ ***See "Add User" on page 100 for more information.***

1. Log into the terminal as an administrator.

   See "Administrator Authentication" on page 47 for more information.

2. Press ⬭ User Management.
3. Press ⬭ Add User.
4. Enter the user's RPIN and press ENTER.
5. If the terminal is running in standalone mode, the screen will display "Host Unavailable/Create New User/Are You Sure?" Press ⬭ YES.
6. If you are ready to enroll the user at this time, go to the next section "Enrolling a User".

Enrolling a User

1. Ensure the user has been created in the terminal.

   See "Add User" on page 100 for more information.

2. Log into the terminal as an administrator.

See “Administrator Authentication” on page 47 for more information.

3. Press ⬭ User Management.
4. Press ⬭ List Users.
5. Scroll to the name of the user you wish to enroll using ◎. Press the middle navigational key to select the user.
6. Press ⬭ Enroll User.
7. Follow the prompts on the terminal screen for hand placements. You will be prompted to place your hand three times.

➡ ***If needed, a user can also be enrolled without using hand verification. See “No Hand Enroll” on page 95 for more information***

Setting User Data

Most user data can be set at the host application and passed to the terminal through synchronization. See your host application documentation for more information.

Edit Timezone

➡ ***See “Edit Timezone” on page 57 for more information.***

1. Log into the terminal as an administrator.

   See “Administrator Authentication” on page 47 for more information.
2. Press ⬭ User Management.
3. Press ⬭ List Users.
4. Scroll to the name of the user you wish to edit using ◎. Press the middle navigational key to select the user.
5. Scroll to the timezone listing using ◎. Press the middle navigational key to change the timezone.
6. Press ⬭ List Timezone.
7. Scroll to the timezone you want to add to the user profile using ◎. Press the middle navigational key to select the timezone.

Edit Authority

➡ ***See “Edit Authority” on page 86 for more information.***

1. Log into the terminal as an administrator.

See “Administrator Authentication” on page 47 for more information.

2. Press ⬭ User Management.
3. Press ⬭ List Users.
4. Scroll to the name of the user you wish to edit using ◎. Press the middle navigational key to select the user.
5. Scroll to the authority listing using ◎. Press the middle navigational key to edit the authority level.
6. Enter the appropriate authority level for the user (1-5).

Add Credential

➡ ***See “Add Credential” on page 94 for more information.***

1. Log into the terminal as an administrator.

   See “Administrator Authentication” on page 47 for more information.
2. Press ⬭ User Management.
3. Press ⬭ List Users.
4. Scroll to the name of the user you want to edit using ◎. Press the middle navigational key to select the user.
5. Press ⬭ More.
6. Press ⬭ Credential Menu.
7. Press ⬭ Add Credential.
8. Press ⬭ RPIN.
9. Press ⬭ Enter.

Edit Threshold

4 ➡ ***See “Edit Threshold” on page 88 for more information.***

1. Log into the terminal as an administrator.

   See “Administrator Authentication” on page 47 for more information.
2. Press ⬭ User Management.
3. Press ⬭ List Users.

4. Scroll to the name of the user you wish to edit using ◎. Press the middle navigational key to select the user.
5. Scroll to the threshold listing using ◎. Press the middle navigational key to edit the threshold level.
6. Enter the threshold.
7. Press ⬭ Enter.

Edit Name

➡ ***See "Edit Name" on page 85 for more information.***

1. Log into the terminal as an administrator.

   See "Administrator Authentication" on page 47 for more information.
2. Press ⬭ User Management.
3. Press ⬭ List Users.
4. Scroll to the name of the user you wish to edit using ◎. Press the middle navigational key to select the user.
5. Scroll to the name field you want to edit (First Name or Last Name) using ◎. Press the middle navigational key to select the name field.
6. Edit the name.
7. Press ⬭ Enter to accept the changes.

Remove a User

➡ ***See "Remove User" on page 92 for more information.***

1. Log into the terminal as an administrator.

   See "Administrator Authentication" on page 47 for more information.
2. Press ⬭ User Management.
3. Press ⬭ List Users.
4. Scroll to the name of the user you wish to remove using ◎. Press the middle navigational key to select the user.
5. Press ⬭ More.
6. Press ⬭ Remove User.
7. Press ⬭ YES.

Setting Date and Time

➡ ***Setting a terminal's date and time using the terminal can only be done when the terminal is in Demo mode; otherwise these settings are made by the host application when in Network mode.***

Set Locale Timezone

4 ➡ ***See "Set LocaleTimezone" on page 63 for more information.***

1. 1. Log into the terminal as an administrator.

   See "Administrator Authentication" on page 47 for more information.
2. Press ⬭ Setup Menu.
3. Press ⬭ General Setup.
4. Press ⬭ Set Locale Timezone.
5. Press ⬭ Set Locale TZ.
6. Scroll to the appropriate time zone using ◎. Press the middle navigational key to select the time zone.

Set Terminal Date

4 ➡ ***See "Set Terminal Date" on page 61 for more information.***

NOTE: Set Terminal Date is available only when you are in Demo mode or Standalone mode.

1. Log into the terminal as an administrator.

   See "Administrator Authentication" on page 47 for more information.
2. Press ⬭ Setup Menu.
3. Press ⬭ General Setup.
4. Press ⬭ More.
5. Press ⬭ Set Terminal Date.
6. Enter the current date.
7. Press ⬭ Enter.

Set Terminal Time

➡ ***See "Set Terminal Time" on page 63 for more information.***

NOTE: Set Terminal Time is available only when you are in Demo mode or Standalone mode.

1. Log into the terminal as an administrator.

   See "Administrator Authentication" on page 47 for more information.

2. Press ⬭ Setup Menu.
3. Press ⬭ General Setup.
4. Press ⬭ More.
5. Press ⬭ Set Terminal Time.
6. Enter the current time.
7. Press ⬭ Enter.

User Authentication

1. When prompted, enter your Credential ID for the administrator account.
2. Place your hand for verification.

Checking the Terminal Software Version

The terminal software version can be obtained using the Terminal Status command menu.

➡ ***See "Terminal Status" on page 110 for more information.***

Updating the Terminal Software

Updates to the terminal software can be applied to the terminal using the host application (if permitted by your custom host application). Refer to your host application documentation for more information.

Rebooting the Terminal Using the Terminal Interface

1. Log in to the terminal as an administrator.

   See "Administrator Authentication" on page 47 for more information.

2. Press ⬭ Maintenance Menu.
3. Press ⬭ Reboot.

The terminal will shut down and reboot automatically. If the terminal cannot be rebooted using the terminal interface, use telnet. See “Rebooting the Terminal Via Telnet” on page 129.

Command Menu Reference 6

Reviewing the Command Menu

The following page is a map of all the commands that can be accessed on the terminal. Each command is described in detail in the following sections of this guide.

Command Menu Structure

Setup Menu

Timezone Menu

- Edit Timezone
  - List TZIDs
- List Timezones
- Add Timezone

Print Setup

- Set PrintBookings
- Set Baud Rate

General Setup

- Set Beeper
- CmdLine Setup
- Set Time&Attend
- Set Door Unlock Time
- Set LocaleTimezone
  - Set LocaleTZ
- Set ID Length
- More
  - Set Duration to Retain Sent
  - Set CR Terminator String
  - Set Lunch Punch Lockout Secs
  - Set Terminal Date**
  - Set Terminal Time**
  - Set LogFile Size Factor
  - Set CR Num of Prefix Chars

Holiday Menu

- Edit Holiday
  - List Holidays
- List Holidays
- Add Holiday

Network Mode Setup

- Set Logical Name
- Set Host Username
- Go to Demo Mode***
  - Go to Demo Mode
- Go to StandAlone Mode
  - Go to StandAlone Mode
- Set Web Server
- Set Host Password
- Set Host URL
- More
  - Set CLISrv Port
  - Set XMLRPCSvr Port
  - XMLRPC Svr Setup
  - Set WebSvr Port
  - Set Static/DHCP
    - StaticIP
      - IPADDR
      - DNS1
      - DNS2
      - NETMASK
      - GATEWAY
  - Set RealTime Interaction

Display Setup

- Set CompanyName
- Date Time Format
  - Set Time Format
  - Set Date Format
- Set Ready String
- Set Language

User Management

Edit User

- First Name
- Last Name
- Enroll Status
- Authority
- Last Score
- Threshold
- Verify Status
- Timezone
- User Status
- Enroll User
- Last Booking
- More
  - Generate Punch
  - Remove User
  - Credential Menu
    - List Credentials
    - Add Credentials
  - No Hand Enroll
  - Edit EPIN
  - Access Grant Menu
    - Edit Access Grant
    - List Access Grant
    - Add Access Grant
  - List Bookings

List Users (see *Edit User* for submenus)

Add User (see *Edit User* for submenus)

Security Menu

Clear UserDB

Factory Settings

Set Reject Threshold

- Set Reject Threshold
- Credential Logging Enabled
- Restore Factory Password

Clear Setup

Biometric Setup

- Min High Res Update Count
- Placements Per Try
- Number of Tries
- Template Resolution

Set Passwords

- Set CLI Access Pwd

More

- Set Credential Logging Flag
- Restore Factory Password

Maintenance Menu

Partial Sync Now

Sync Now

Reboot

Terminal Status

Delete Sent Interactions

Shutdown

Last Punch

FKScript List*

Timecard Approval

Accrual Balances

Cancel Meal

Lunch Punch

Time Off Request

Transfer-ValidList

Command Menu Notes:

**Available in Demo Mode only*
***Available in Demo Mode or Stand Alone Mode only.*

**** The* ***Go to Demo Mode*** *command is available only when you have not yet gone into Network Mode.*

Setup Menu

Timezone Menu

A timezone is a period of time during which user access to the terminal is granted.

Every user must have a timezone assigned, either directly or through a group, in order to access the terminal. The timezones 0 (Always) and 61 (Never) are created by default. If a user is assigned timezone 0 (Always), the user always has access to the terminal. If the user is assigned timezone 61 (Never), the user never has access to the terminal.

Timezones are created with intervals. An interval is defined by start time, duration and days of week. Each timezone may have multiple intervals.

Edit Timezone	
Edits a timezone that already exists on the terminal. Select the timezone and then edit the designed interval(s) to change the timezone.	**Default:** None **Range:** None **Dependencies:** None **Who:** A terminal administrator can edit a timezone at any time

1. Log into the terminal as an administrator.

   ➡ ***See "Administrator Authentication" on page 47 for more information.***

2. Press ⬭ Setup Menu.
3. Press ⬭ Timezone Menu.
4. Press ⬭ List Timezones.
5. Highlight the timezone you want to edit using ⊕. Press the middle key to select the timezone.
6. Press ⬭ List TZIntervals.
7. Scroll to the interval you want to edit using ⊕ . Press the middle key to select the interval.
8. To remove the interval, press ⬭ Remove TZInterval, then press ⬭ YES.
9. To edit the start time of the interval, press ⬭ Edit StartTime. Enter the start time and Press ⬭ Enter.
10. To edit the days of the week for which the interval is effective, Press ⬭ Edit DOW.
11. Press to toggle each day of the week desired. Then press (ENTER).
12. To edit the duration, press ⬭ Edit Duration. Enter the duration and press ⬭ Enter.

List Timezones

Lists all the timezones for the terminal.

Default: None

Range: None

Dependencies: None

Who: A terminal administrator can list a timezone at any time.

1. Log into the terminal as an administrator.

   ➡ ***See "Administrator Authentication" on page 47 for more information.***

2. Press ⬭ Setup Menu.
3. Press ⬭ Timezone Menu.
4. Press ⬭ List Timezones.
5. From here, many other functions can be accessed. See the other topics in this section for more information.

Add Timezone

Creates an access timezone for the terminal. To create a timezone, first enter an ID, and then add the start time, duration and days to create an interval. Timezones can have many intervals.

Default: 0 (Always)

Range: None

Dependencies: None

Who: A terminal administrator can add a timezone at any time.

1. Log into the terminal as an administrator.

   ➡ ***See "Administrator Authentication" on page 47 for more information.***

2. Press ⬭ Setup Menu.
3. Press ⬭ Timezone Menu.
4. Press ⬭ Add Timezone.
5. Enter the timezone ID (any positive number not previously used).
6. Press ⬭ Enter.
7. Press ⬭ AddTZInterval.
8. Enter the start time.
9. Press ⬭ Enter.
10. Enter the duration.
11. Press ⬭ Enter.
12. Press ⬭ for each day of the week to add to the interval. (Each press toggles the day on or off.)
13. Press ENTER.

Print Setup

The Print Setup menu is used to configure print settings. This information is only necessary when a printer is connected to the terminal.

➡ ***See "Printer Setup (Optional)" on page 33 for more information.***

Set PrintBookings

Enables or disables printing of each booking. A booking is the interaction that is recorded when a user punches in or out of the terminal. The display of this menu will indicate the current state of the Set PrintBookings option. If it is disabled, press Enable to enable PrintBookings. If it is enabled, press Disable to disable it.

Default: Disabled

Range: None

Dependencies: A printer must be connected to the terminal in order to print bookings.

Who: A terminal administrator should set this option during initial terminal setup. his option can be changed at any time

1. Log into the terminal as an administrator.

   ➡***See "Administrator Authentication" on page 47 for more information.***

2. Press ⬭ Setup Menu.
3. Press ⬭ Print Setup.
4. Press ⬭ Set PrintBookings.
5. Press ⬭ Enable/Disable.

Set Baud Rate

Sets the baud rate (data transmission speed) to be used for the printer. Enter the proper baud rate for your printer. Consult the documentation that came with your printer to determine the proper baud rate.

➡***This setting must match the baud rate setting of the printer that is used to print data from the terminal.***

Default: 9600

Range: None

Dependencies: None

Who: A terminal administrator should set this option to match the printer's baud rate during initial terminal setup.

1. Log into the terminal as an administrator.

   ➡***See "Administrator Authentication" on page 47 for more information.***

2. Press ⬭ Setup Menu.
3. Press ⬭ Print Setup.
4. Press ⬭ Set Baud Rate.
5. Scroll to the baud rate that matches the baud rate of the printer.
6. Press ⬭ Enter.

General Setup

Set Terminal Date	
Sets the date. This setting can only be made in Demo mode.	**Default:** None **Range:** None **Dependencies:** None **Who:** A terminal administrator should set the date of a terminal in Demo mode during initial setup.

➡ ***The terminal must be in Demo Mode in order to use the following instructions.***

1. Log into the terminal as an administrator.

   ➡ ***See "Administrator Authentication" on page 47 for more information.***

2. Press ⬭ Setup Menu.

3. Press ⬭ General Setup.

4. Press ⬭ More.

5. Press ⬭ Set Terminal Date using the format MM DD YYYY (Example: 23 32 59.)
6. Enter the current date.

7. Press ⬭ Enter.

CmdLine Setup

Enables or disables command line interface (CLI) access to the terminal. The display of this menu will indicate the current state of the CmdLine Setup option. If it is disabled, press Enable to enable CLI access. If it is enabled, press Disable to disable it. This option should normally be disabled for security reasons.

Default: Enabled

Range: None

Dependencies: None

Who: A terminal administrator, application developer/tester or any individual under the guidance of a technical support representative can disable or enable CLI for troubleshooting, testing or debugging purposes.

1. Log into the terminal as an administrator.

   ➡ ***See "Administrator Authentication" on page 47 for more information.***

2. Press ▭ Setup Menu.
3. Press ▭ General Setup.
4. Press ▭ CmdLine Setup.
5. Press ▭ Enable/Disable.

Set Time&Attend

Enables or disables time and attendance mode for the terminal. When enabled, the user will be prompted to punch in or out before the hand verification. When disabled, the user will not be given the choice to punch in or out and the terminal or host will automatically punch the user in or out. This menu will display the current state of the Time and Attendance Mode option.

Default: Disabled

Range: None

Dependencies: None

Who: A terminal administrator should set this option during initial setup of the terminal.

1. Log into the terminal as an administrator.

   ➡ ***See "Administrator Authentication" on page 47 for more information.***

2. Press ▭ Setup Menu.
3. Press ▭ General Setup.
4. Press ▭ Time&Attend.
5. Press ▭ Enable/Disable.

Set Terminal Time

NOTE: Set Terminal Time is used to set the time only on a terminal running in Demo mode. Otherwise, the terminal will acquire the time from the host application.

Using the keypad, enter the time using the following format: hh mm ss based on a 24-hour clock.

Default: None

Range: None

Dependencies: None

Who: A terminal administrator should set the time of a terminal running in Demo mode during initial terminal setup.

1. Log into the terminal as an administrator.

   ➡ ***See "Administrator Authentication" on page 47 for more information.***

2. Press ⬭ Setup Menu.
3. Press ⬭ General Setup.
4. Press ⬭ More.
5. Press ⬭ Set Terminal Time using the format HH MM SS. (Example: 23 35 59.)
6. Enter the current time.
7. Press ⬭ Enter.

Set LocaleTimezone

Sets the time zone of a terminal based on the locality of the terminal itself. Otherwise, the terminal will acquire the time zone from the host application. Select the time zone from the menu that matches your locality.

Default: GMT-8 (Pacific Standard Time)

Range: None

Dependencies: None

Who: A terminal administrator should set the LocaleTZ of a terminal during initial terminal setup.

1. 1. Log into the terminal as an administrator.

   ➡ ***See "Administrator Authentication" on page 47 for more information.***

2. Press ⬭ Setup Menu.
3. Press ⬭ General Setup.
4. Press ⬭ Set Locale Timezone.
5. Scroll to the time zone you want to use by using ◎. Press the middle key to select the time zone.

Set ID Length

If you set an ID length, the terminal will automatically accept an ID entry once the correct number of digits have been entered. This setting can help expedite the processing of users, especially when user volume is high.

➡***All IDs in the system cannot exceed this length. If an ID exceeds this length, a user will not be able to enter the ID.***

Default: 6

Range: None

Dependencies: None

Who: A terminal administrator can set this feature to the desired length at any time.

1. Log into the terminal as an administrator.

   ➡***See "Administrator Authentication" on page 47 for more information.***

2. Press ⬭ Setup Menu.
3. Press ⬭ General Setup.
4. Press ⬭ Set ID Length.
5. Press ⬭ the ID length.
6. Press ⬭ Enter.

Set LogFile Size Factor

Defines a percentage of disk space (the SD card) to be used for the log file. When that size is exceeded the terminal will automatically create a backup of that log file and a new log file will be generated. The backup log will be located in the same directory (RecogSys/ZODB).

Default: 3%

Range: 0%-80%

Dependencies: None

Who: A terminal administrator can define the disk space used by the log file to optimize the memory management in the terminal. An administrator may wish to increase the logging capacity if the overall database is small, or decrease the logging capacity if the database is large.

1. Log into the terminal as an administrator.

   ➡ ***See "Administrator Authentication" on page 47 for more information.***

2. Press ▭ Setup Menu.
3. Press ▭ General Setup.
4. Press ▭ More.
5. Press ▭ Set LogFile Size Factor.
6. Enter the LogFile Size Factor.
7. Press ▭ Enter.

Set CR Num of Prefix Chars

Defines the number of prefix characters in a barcode credential ID.

Default: 2

Range: None

Dependencies: None

Who: A terminal administrator may set the prefix characters to comply with site specifications.

1. Log into the terminal as an administrator.

   ➡ ***See "Administrator Authentication" on page 47 for more information.***

2. Press ⬭ Setup Menu.
3. Press ⬭ General Setup.
4. Press ⬭ More.
5. Press ⬭ Set CR Num of Prefix Chars.
6. Enter the CR Num of Prefix Chars.
7. Press ⬭ Enter.

Set Door Unlock Time

Defines the time, in seconds, that the relay (J5 connector) will fire and remain active after verification. Press Set Door Unlock Time and define the time in seconds, starting from verification, that the relay will fire and remain active. This may be used to unlock a door to which a terminal is attached or to activate any other device attached to the relay

Default: 0

Range: None (0 is defined as OFF)

Dependencies: None

Who: A terminal administrator can set the amount of time the relay will fire and remain active.

1. Log into the terminal as an administrator.

   ➡ ***See "Administrator Authentication" on page 47 for more information.***

2. Press ⬭ Setup Menu.
3. Press ⬭ General Setup.
4. Press ⬭ Set Door Unlock Time.
5. Enter the door unlock time in seconds.
6. Press ⬭ Enter.

Set CR Terminator String

Defines a barcode credential’s terminator string. Press Set CR Terminator String and set the string as necessary.

Default: 3232000

Range: None

Dependencies: None

Who: A terminal administrator can define barcode terminator strings to comply with site specifications.

1. Log into the terminal as an administrator.

   ➡ ***See “Administrator Authentication” on page 47 for more information.***

2. Press ⬭ Setup Menu.
3. Press ⬭ General Setup.
4. Press ⬭ More.
5. Press ⬭ Set CR Terminator String.
6. Enter the CR terminator string.
7. Press ⬭ Enter.

Set Beeper

Enables or disables the audible beep on the terminal. The display of this menu will indicate the current state of the beeper. If it is disabled, press Enable to enable the beeper. If it is enabled, press Disable to disable it.

Default: Enabled

Range: None

Dependencies: None

Who: A terminal administrator can enable or disable the beeper at any time.

1. Log into the terminal as an administrator.

   ➡ ***See “Administrator Authentication” on page 47 for more information.***

2. Press ⬭
3. Press ⬭ Setup Menu.
4. Press ⬭ General Setup.
5. Press ⬭ Set Beeper.
6. Press ⬭ Enable or Disable.

Set Duration to Retain Sent

Defines the length of time (in days) to retain sent interactions in the terminal.

Default: 30

Range: None

Dependencies: None

Who: Terminal administrators can set the amount of time to retain sent interactions on the terminal.

1. Log into the terminal as an administrator.

   ➡ ***See "Administrator Authentication" on page 47 for more information.***

2. Press ▭ Setup Menu.
3. Press ▭ General Setup
4. Press ▭ More
5. Press ▭ Set Duration to Retain Sent
6. Enter the Duration to Retain Sent Interactions.
7. Press ▭ Enter.

Set Lunch Punch Lockout Secs

Defines number of seconds to lock out lunch punches after a user executes a lunch punch.

Default: 0

Range: 0 - 7200 (in seconds)

Dependencies: None

Who: A terminal administrator can set the lunch punch lockout duration at any time.

1. Log into the terminal as an administrator.

   ➡ ***See "Administrator Authentication" on page 47 for more information.***

2. Press ▭ Setup Menu.
3. Press ▭ General Setup
4. Press ▭ More
5. Press ▭ Set Lunch Punch Lockout Secs.
6. Enter Lunch Punch Lockout Duration in Seconds.
7. Press ▭ Enter.

Holiday Menu

Holidays are used to provide a break in a normal timezone.

Edit Holiday

Edits holidays already set up in the terminal. The holiday end date, begin date, end time, begin time and name may all be edited.	**Default:** 30 **Range:** None **Dependencies:** None **Who:** A terminal administrator can edit a holiday at any time.

1. Log into the terminal as an administrator.

   ➡ ***See "Administrator Authentication" on page 47 for more information.***

2. Press ⬭ Setup Menu.
3. Press ⬭ Holiday Menu.
4. Press ⬭ List Holidays.
5. Scroll to the appropriate holiday using ◎. Press the middle key to select the holiday.
6. Press ⬭ Edit End Date, Edit Begin Date, Edit End Time, Edit Begin Time or Edit Name.
7. Enter a new value for the field you have selected.
8. Press ⬭ Enter.
9. Repeat step 6 through step 8 until all desired fields have been edited.

List Holidays

Lists all holidays defined for the terminal.

Default: None

Range: None

Dependencies: None

Who: A terminal administrator can list holidays at any time.

1. Log into the terminal as an administrator.

   ➡ ***See "Administrator Authentication" on page 47 for more information.***

2. Press ⬭ Management Menu.
3. Press ⬭ Holiday Menu.
4. Press ⬭ List Holidays.
5. From here, many other functions can be accessed. See the other topics in this section for more information.

Add Holiday

Sets and configures holidays for the terminal. Enter the holiday name, start time and end time to build a holiday.

Default: None

Range: None

Dependencies: None

Who: A terminal administrator can add holidays at any time.

1. Log into the terminal as an administrator.

   ➡ ***See "Administrator Authentication" on page 47 for more information.***

2. Press ⬭ Management Menu.
3. Press ⬭ Holiday Menu.
4. Press ⬭ Add Holidays.
5. Enter the name of the holiday.
6. Press ⬭ Enter.
7. Enter the holiday start date and time.
8. Press ⬭ Enter.
9. Enter the holiday end date and time.
10. Press ⬭ Enter.

Network Setup

The Network Setup menu is used to configure information that will be used by the terminal to communicate with the host application. This information is only necessary when the terminal is used in network mode.

<table>
<tr><th colspan="2">Set Logical Name</th></tr>
<tr><td>Sets the name of the terminal on the TCP/IP network. If the terminal will be running in network mode, this name must match the logical name for the terminal recorded in the host application for synchronization to occur.</td><td><b>Default:</b> G-Series-Handreader
<b>Range:</b> 6-25 alphanumeric characters
<b>Dependencies:</b> None
<b>Who:</b> An administrator should set a logical name during initial terminal setup.</td></tr>
<tr><td colspan="2">1. Log into the terminal as an administrator.
➡ <b><i>See “Administrator Authentication” on page 47 for more information.</i></b>
2. Press ⬭ Setup Menu.
3. Press ⬭ Network Setup.
4. Press ⬭ Set LogicalName.
5. Enter the logical name for the terminal.
6. Press ⬭ Enter.</td></tr>
</table>

Set Host Username

The host user name is used to authenticate with the host application. This user name must match a valid user account user name on the host application in order for synchronization to occur.

Default: None

Range: None

Dependencies: None

Who: A network administrator should set the host user name during initial terminal setup

1. Log into the terminal as an administrator.

   ➡***See "Administrator Authentication" on page 47 for more information.***

2. Press ⬭ Setup Menu.
3. Press ⬭ Network Setup.
4. Press ⬭ Set HostUser.
5. Enter the user name for the host application.
6. Press ⬭ Enter.

Go to StandAlone or Demo Mode

The display of this menu indicates the current mode of the terminal as follows:

- Go To StandAlone Mode is only displayed when the terminal is running in network mode. To put the terminal in standalone mode, press Go To StandAlone Mode. When the terminal is in standalone mode, no synchronization with the host application will occur.
- Go To Demo Mode is only displayed when the terminal is running in standalone or networked mode. To put the terminal in Demo mode, press Go To Demo Mode. when the terminal is in Demo mode, no synchronization with the host application will occur.
- Go To Network Mode is only displayed when the terminal is running in standalone mode or Demo mode. To put the terminal in network mode, press Go To Network Mode. When the terminal is in network mode, the terminal will attempt to synchronize with the host application.

Default: None

Range: None

Dependencies: None

Who: A network administrator can change this setting at any time.

1. Log into the terminal as an administrator.

   ➡ ***See "Administrator Authentication" on page 47 for more information.***

2. Press ⬭ Setup Menu.
3. Press ⬭ Network Setup.
4. Press ⬭ Go To Demo Mode/StandAlone Mode/Go To Network Mode.
5. Press ⬭ Go To Demo Mode/StandAlone Mode/Go To Network Mode (again).

Set WebServer

Enables or disables the terminal's web server. If the terminal will be used in network mode, the web server should be enabled. The display of this menu will indicate the current state of the web server.

Default: Enabled

Range: None

Dependencies: None

Who: A network administrator should set the WebServer during initial terminal setup.

1. Log into the terminal as an administrator.

   ➡***See "Administrator Authentication" on page 47 for more information.***

2. Press ⬭ Setup Menu.
3. Press ⬭ press Network Setup.
4. Press ⬭ Set WebServer.
5. Press ⬭ Enable or Disable.
6. Reboot the terminal. (The new setting will not take effect until the terminal is rebooted.)

   ➡***See "Rebooting the Terminal Using the Terminal Interface" on page 53 for more information.***

Set Host Password

The host password is used to authenticate with the host application. This password must match a valid user account password on the host application in order for synchronization to occur.

Default: None

Range: None

Dependencies: None

Who: A network administrator should set the host password during initial terminal setup.

1. Log into the terminal as an administrator.

   ➡***See "Administrator Authentication" on page 47 for more information.***

2. Press ⬭ Setup Menu.
3. Press ⬭ Network Setup.
4. Press ⬭ Set HostPassword.
5. Enter the host password.
6. Press ⬭ Enter.

Set Host URL

The HostURL is used to authenticate with the host application. This URL must match URL of the host application in order for synchronization to occur.

Default: http://127.0.0.1

Range: None

Dependencies: None

Who: A network administrator should set HostURL during initial terminal setup.

1. Log into the terminal as an administrator.

   ➡ ***See "Administrator Authentication" on page 47 for more information.***

2. Press ⬭ Setup Menu.
3. Press ⬭ Network Setup.
4. Press ⬭ Set HostURL.
5. Enter the host URL (complete URL, starting with "http://").
6. Press ⬭ Enter.

Set CLISvr Port

Set CLISrv Port defines the port that will be used connect to the terminal’s Command Line Interface (CLI).

Default: 8090

Range: None

Dependencies: Site’s network specifications

Who: A terminal administrator may change the port from the default to comply with site specifications.

1. Log into the terminal as an administrator.

   ➡ ***See “Administrator Authentication” on page 47 for more information.***

2. Press ⬭ Setup Menu.
3. Press ⬭ Network Setup.
4. Press ⬭ More.
5. Press ⬭ Set CLISrv Port.
6. Enter the CLI server port.
7. Press ⬭ Enter.
8. Reboot the terminal.

➡ ***See “Rebooting the Terminal Using the Terminal Interface” on page 53 for more information.***

Set XMLRPCSvr Port

Set XMLRPCSvr Port defines the port that will to connect to the terminal’s XMLRPC server.

Default: 8085

Range: None

Dependencies: Site network specifications

Who: A terminal administrator may change the port from the default to comply with site specifications.

1. Log into the terminal as an administrator.

   ➡ ***See “Administrator Authentication” on page 47 for more information.***

2. Press ⬭ Setup Menu.
3. Press ⬭ Network Setup.
4. Press ⬭ More.
5. Press ⬭ Set XMLRPCSvr Port.
6. Enter the XMLRPC server port.
7. Press ⬭ Enter.
8. Reboot the terminal.

➡ ***See “Rebooting the Terminal Using the Terminal Interface” on page 53 for more information.***

<table>
<tr><th colspan="2">XMLRPC Svr Setup</th></tr>
<tr><td>XMLRPC Svr Setup enables or disables the XMLRPC server. The display of this menu will indicate the current state of the XML-RPC server. If it is disabled, press enable to enable the XML-RPC server. If it is enabled, press disable to disable it.</td><td><b>Default:</b> Enabled
<b>Range:</b> None
<b>Dependencies:</b> None
<b>Who</b>: A network administrator should set the XML-RPC server during initial terminal setup.</td></tr>
<tr><td colspan="2">1. Log into the terminal as an administrator.
➡ <b><i>See “Administrator Authentication” on page 47 for more information.</i></b>
2. Press ▭ Setup Menu.
3. Press ▭ Network Setup.
4. Press ▭ More.
5. Press ▭ Set XMLRPC Svr Setup Port.
6. Press ▭ to Enable (or Disable).
7. Reboot the terminal.
➡ <b><i>See “Rebooting the Terminal Using the Terminal Interface” on page 53 for more information.</i></b></td></tr>
</table>

Set WebSvr Port

Set WebSvr Port defines the port you will use to connect to the terminal’s Web Server.

Default: 80

Range: None

Dependencies: None

Who: A terminal administrator may change the web server port from default to comply with a site’s network specifications.

1. Log into the terminal as an administrator.

   ➡ ***See “Administrator Authentication” on page 47 for more information.***

2. Press ⬭ Setup Menu.
3. Press ⬭ Network Setup.
4. Press ⬭ More.
5. Press ⬭ Set WebSvr Port.
6. Enter the web server port.
7. Press ⬭ Enter.
8. Reboot the terminal.

   ➡ ***See “Rebooting the Terminal Using the Terminal Interface” on page 53 for more information.***

Set Static/DHCP

Set Static/DHCP is used to either set a static IP address for the terminal or to use DHCP. If DHCP is enabled, enter an IP address to switch to static. If static is enabled, press DHCP to switch to DHCP.

NOTE: Switching from DHCP to Static IP (or vice versa) will force a reboot.

Default: DHCP

Range: 0-255

Dependencies: None

Who: A network administrator should set Static/DHCP during initial terminal setup.

1. Log into the terminal as an administrator.

   ➡ ***See "Administrator Authentication" on page 47 for more information.***

2. Press ⬭ Setup Menu.
3. Press ⬭ Network Setup.
4. Press ⬭ More.
5. Press ⬭ Static/DHCP.
6. Do one of the following:

   a. At this point, DHCP is enabled. The IP address will be displayed on the screen.

   b. To enable a static IP address, press ⬭ Static IP.

      1. To edit the IP address, highlight IPADDR using ◎. Press the middle key to select the IPADDR list item.
      2. Press ⬭ Edit and enter the IP Address. Press ⬭ Confirm.
      3. To edit the DNS1, DNS2, NETMASK, or GATEWAY values, repeat the previous 2 steps. (in b.1 and b.2).

Set RealTimeInteraction

When Set Real Time Interaction is enabled, the terminal will send interactions as they happen (in real time). When Real Time Interaction is disabled, the terminal will send interactions only when a synchronization takes place. The display of this menu will indicate the current state of Real Time Interactions. If it is disabled, press enable to enable Real Time Interactions. If it is enabled, press disable to disable it.	**Default:** Enabled **Range:** None **Dependencies:** None **Who:** A terminal administrator should enable or disable Real Time Interaction to conform to the site design requirements.

1. Log into the terminal as an administrator.

   ➡ ***See "Administrator Authentication" on page 47 for more information.***

2. Press ⬭ Setup Menu.
3. Press ⬭ Network Setup.
4. Press ⬭ More.
5. Press ⬭ RealTimeInteraction.
6. Press ⬭ to Enable (or Disable).

Display Setup

The Display Setup menu is used to configure information that is displayed on the LCD screen.

Set Company Name

The Company Name is the first line of text that is displayed on the terminal screen. It can be changed to any line of text.	**Default:** Schlage Biometrics **Range:** None **Dependencies:** None **Who**: A terminal administrator can set the company name at any time.

1. Log into the terminal as an administrator.

   ➡ ***See "Administrator Authentication" on page 47 for more information.***

2. Press ⬭ Setup Menu.
3. Press ⬭ Display Setup.
4. Press ⬭ Set Company Name.
5. Enter the company name and press ⬭ Enter.

Set Time Format

Sets the time format that will be used to display the time on the terminal screen.

Default: HH:MM:SS

Range: None

Dependencies: None

Who: A terminal administrator can set a time format at any time.

1. Log into the terminal as an administrator.

   ➡ ***See "Administrator Authentication" on page 47 for more information.***

2. Press ⬭ Setup Menu.
3. Press ⬭ Display Setup.
4. Press ⬭ Date Time Format.
5. Press ⬭ Set Time Format.
6. Scroll to the format you want to use by using ◎. Press the middle key to select the time format.

Set Date Format

Sets the date format that will be used to display the date on the terminal screen.

Default: MM/DD/YYYY

Range: None

Dependencies: None

Who: A terminal administrator can set a date format at any time.

1. Log into the terminal as an administrator.

   ➡ ***See "Administrator Authentication" on page 47 for more information.***

2. Press ⬭ Setup Menu.
3. Press ⬭ Display Setup.
4. Press ⬭ Date Time Format.
5. Press ⬭ Set Date Format.
6. Scroll to the format you want to use by using ◎. Press the middle key to select the date format.

Set Ready String

The Ready String is the line of text that is displayed below the company name on the terminal screen. It can be changed to any line of text.

Default: ***Enter ID***

Range: None

Dependencies: None

Who: A terminal administrator can set a ready string at any time.

1. Log into the terminal as an administrator.

   ➡ ***See "Administrator Authentication" on page 47 for more information.***

2. Press ⬭ Setup Menu.
3. Press ⬭ Display Setup.
4. Press ⬭ Set Ready String.
5. Enter the ready string.
6. Press ⬭ Enter.

Set Language

Set Language is used to change language on the terminal. Note: English (EN) is the only supported language for this release.

Default: EN

Range: None

Dependencies: None

Who: A terminal administrator should set this value during initial configuration of the terminal.

1. Log into the terminal as an administrator.

   ➡ ***See "Administrator Authentication" on page 47 for more information.***

2. Press ⬭ Setup Menu.
3. Press ⬭ Display Setup.
4. Press ⬭ Set Language..
5. Scroll to the format you want to use by using ◎. Press the middle key to select the desired language.

User Management

Edit User

Edits a user that is already entered in the terminal.

Default: None

Range: None

Dependencies: None

Who: A terminal administrator can edit a user in the terminal at any time.

1. Log into the terminal as an administrator.

   ➡ ***See "Administrator Authentication" on page 47 for more information.***

2. Press ⬭ User Management
3. Press ⬭ Edit User.
4. Press ⬭ List Users.
5. Scroll to the appropriate user using ◎ . Press the middle key to select the user.
6. From here, many other functions can be accessed. See the other topics in this section for more information..

List Users

List Users displays a table showing all users associated with the terminal. The table also displays the RPIN, user authorization and in/out status.

➡ ***This information is only accurate to within the last host synchronization.***

Default: None

Range: None

Dependencies: None

Who: A terminal administrator can list a user in the terminal at any time.

1. Log into the terminal as an administrator.

   ➡ ***See "Administrator Authentication" on page 47 for more information.***

2. Press ⬭ User Management
3. Press ⬭ List Users.
4. From here, many other functions can be accessed. See the other topics in this section for more information..

Edit Name

Edit Name is used to change a user’s name. First name, last name and middle name are edited separately.

Default: None

Range: None

Dependencies: None

Who: A terminal administrator can change a user’s name in the terminal at any time.

1. Log into the terminal as an administrator.

   ➡ ***See “Administrator Authentication” on page 47 for more information.***

2. Press ⬭ User Management
3. Press ⬭ List Users.
4. Scroll to the appropriate user using ◎ . Press the middle key to select the user.
5. Scroll to the name you want to edit and use ◎ to select the name.
6. Make any necessary changes to the name.
7. Press ⬭ Enter.

Enroll Status

This option displays the user’s enroll status information such as high/low resolution template and EPIN usage.

Default: None

Range: None

Dependencies: None

Who: A terminal administrator can view a user’s enrollment status at any time.

1. Log into the terminal as an administrator.

   ➡ ***See “Administrator Authentication” on page 47 for more information.***

2. Press ⬭ User Management
3. Press ⬭ List Users.
4. Scroll to the appropriate user using ◎ . Press the middle key to select the user.
5. Scroll to the Enroll Status option to view enrollment information for this user.

Edit Authority

Changes the authority level of a user. Authority level determines which level of command menu a user may access. The terminal administrator account must have level 5 authority. Users have authorization based on their authority level as follows:

- Last Punch
- Last Punch, User Management
- Last Punch, User Management, Maintenance
- Last Punch, User Management, Maintenance, Setup
- Last Punch, User Management, Maintenance, Setup, Security

Default: 1

Range: 1-5

Dependencies: None

Who: A terminal administrator can change the authority level associated with a user's profile at any time.

1. Log into the terminal as an administrator.

   ➡ ***See "Administrator Authentication" on page 47 for more information.***

2. Press ⬭ User Management
3. Press ⬭ List Users.
4. Scroll to the name of the user for which you want to change the authority using ◎ . Press the middle key to select the user.
5. Scroll to the authority listing using ◎. Press the middle key to select the authority.
6. Enter the authority level.
7. Press ⬭ Enter.

<table>
<tr><th colspan="2">Last Score</th></tr>
<tr><td>This option displays the user’s last score, which reflects how accurately the user’s hand is placed on the platen.
For more information about hand scores, see “Understanding Hand Read Scores” on page 120.</td><td><b>Default:</b> None
<b>Range:</b> Scores above 50 may indicate improper hand placement
<b>Dependencies:</b> None
<b>Who:</b> A terminal administrator can view a user’s last hand score at any time.</td></tr>
<tr><td colspan="2">1. Log into the terminal as an administrator.
➡<b><i>See “Administrator Authentication” on page 47 for more information.</i></b>
2. Press ⬭ User Management
3. Press ⬭ List Users.
4. Scroll to the appropriate user using ◎ . Press the middle key to select the user.
5. Scroll to the Last Score option to view hand score information for this user.</td></tr>
</table>

Edit Threshold

Each time a user verifies at the terminal, a number that represents the closeness of the match between the template (created at enrollment) and the actual hand is recorded. The threshold is a number that represents how close the match must be for successful verification. The threshold is generally set at the terminal level. If a particular user cannot verify under the terminal's threshold, a personal threshold may be set at the user level. In this way, the level of security is not compromised for all users on the terminal.

➡ ***A threshold set at the user level will override the threshold set at the terminal level.***

➡ ***If a threshold is set at the user level to be a value of "0", the terminal threshold level will be set to the default value of "75" automatically.***

Default: 75

Range: 10-255

Dependencies: None

Who: A terminal administrator can edit the threshold at any time.

1. Log into the terminal as an administrator.

   ➡ ***See "Administrator Authentication" on page 47 for more information.***

2. Press ⬭ User Management
3. Press ⬭ List Users.
4. Scroll to the name of the user for which you want to edit the threshold using ✥ . Press the middle key to select the user.
5. Scroll to the authority listing using ✥. Press the middle key to edit the threshold.
6. Enter the threshold.
7. Press ⬭ Enter.

Verify Status

This option displays the user's status. A value of true indicates that the user is active; a value of false indicates that the user is inactive.

Default: None

Range: None

Dependencies: None

Who: A terminal administrator view a user's status at any time.

1. Log into the terminal as an administrator.

   ➡ ***See "Administrator Authentication" on page 47 for more information.***

2. Press ⬭ User Management
3. Press ⬭ List Users.
4. Scroll to the appropriate user using ◎ . Press the middle key to select the user.
5. Scroll to the Verify Status option to view user status.

Edit Timezone

Changes the timezone that is associated with a user's profile. Select the user. Then select the timezone you want to associate with that user's profile.

Default: None

Range: None

Dependencies: None

Who: A terminal administrator can change the timezone associated with a user's profile at any time.

1. Log into the terminal as an administrator.

   ➡ ***See "Administrator Authentication" on page 47 for more information.***

2. Press ⬭ User Management
3. Press ⬭ List Users.
4. Scroll to the name of the user for which you want to edit the timezone using ◎ . Press the middle key to select the user.
5. Scroll to the timezone option using ◎. Press the middle key to edit the timezone.
6. Enter the desired timezone and press ⬭ Enter.
7. Scroll to the timezone you want to associate with the user using ◎. Press the middle key to select the timezone.

Edit User Status

Changes a user’s status from active to inactive. (Inactive users are those which are not able to use a terminal until their status is changed to active.)

Default: Active

Range: None

Dependencies: None

Who: A terminal administrator can change a user’s status at any time.

1. Log into the terminal as an administrator.

   ➡ ***See “Administrator Authentication” on page 47 for more information.***

2. Press ⬭ User Management
3. Press ⬭ List Users.
4. Scroll to the name of the user for which you want to edit the user status using ◎ . Press the middle key to select the user.
5. Press ⬭ Disable to change a user’s status to Inactive, or press ⬭ Enable to change a user’s status to active.

Enroll User

Enroll User records a user’s hand template for verification. After the user has been entered into the terminal, a terminal administrator should instruct the user on correct hand placement.

Default: None

Range: None

Dependencies: User must be entered into the terminal before enrollment. The user must be present for enrollment.

Who: A terminal administrator can enroll a user after the user has been entered into the terminal.

1. Log into the terminal as an administrator.

   ➡ ***See “Administrator Authentication” on page 47 for more information.***

2. Press ⬭ User Management
3. Press ⬭ List Users.
4. Scroll to the name of the user you want to enroll using ◎ . Press the middle key to select the user.
5. Press ⬭ Enroll User.
6. Follow the prompts on the terminal screen for hand placement.

Last Booking

Shows information about the user’s last booking, or log- in.

➡ ***This information is only accurate to within the last host synchronization.***

Default: None

Range: None

Dependencies: None

Who: A terminal administrator can display the last booking at any time.

1. Log into the terminal as an administrator.

   ➡ ***See “Administrator Authentication” on page 47 for more information.***

2. Press ⬭ User Management

3. Press ⬭ List Users.

4. Scroll to the name of the user for which you want to view the last booking using ⊙ . Press the middle key to select the user.

5. Press ⬭ Last Booking.

Generate Punch

Generates a punch for a given user.

Default: None

Range: None

Dependencies: None

Who: A terminal administrator can generate a punch for a user at any time.

1. Log into the terminal as an administrator.

   ➡ ***See “Administrator Authentication” on page 47 for more information.***

2. Press ⬭ User Management

3. Press ⬭ List Users.

4. Scroll to the name of the user for whom you want to generate a punch using ⊙ . Press the middle key to select the user.

5. Press ⬭ More.

6. Press ⬭ Generate Punch.

Remove User

Removes a user from the terminal if the user no longer requires access.

➡ ***When using this function to remove a user, user is not removed from the host application database. See the documentation that came the host application for more information.***

Default: None

Range: None

Dependencies: None

Who: A terminal administrator can remove a user at any time.

1. Log into the terminal as an administrator.

   ➡ ***See "Administrator Authentication" on page 47 for more information.***

2. Press ⬭ User Management
3. Press ⬭ List Users.
4. Scroll to the name of the user you which to enroll using ◎ . Press the middle key to select the user.
5. Press ⬭ More.
6. Press ⬭ Remove User.
7. Press ⬭ YES.

List Credentials

Lists all credentials associated with a user. Select the user and then select List Credentials.

Default: None

Range: None

Dependencies: None

Who: A terminal administrator can list the credentials for a user at any time.

1. Log into the terminal as an administrator.

   ➡ ***See “Administrator Authentication” on page 47 for more information.***

2. Press ⬭ User Management
3. Press ⬭ List Users.
4. Scroll to the name of the user you wish to want to list credentials using ◎. Press the middle key to select the user.
5. Press ⬭ More.
6. Press ⬭ Credential Menu.
7. Press ⬭ List Credential.
8. Credentials can be edited from this menu. See the other topics in this section for more information.

Add Credential

Adds any type of credential to a user’s profile. Select the user. Then select the type of credential to add to the profile.

➡ ***A user can have multiple credential IDs of different types, provided that the user has only 1 credential ID for a given credential type.***

Default: None

Range: None

Dependencies: None

Who: A terminal administrator can add a new credential at any time.

1. Log into the terminal as an administrator.

   ➡ ***See “Administrator Authentication” on page 47 for more information.***

2. Press ⬭ User Management
3. Press ⬭ List Users.
4. Scroll to the name of the user for which you want to add a credential using ✥. Press the middle key to select the user.
5. Press ⬭ More.
6. Press ⬭ Credential Menu.
7. Press ⬭ Add Credential.
8. Scroll to the type of credential you want to add using ✥. Press the middle key to select the credential type.

No Hand Enroll

Enrolls a user who cannot perform the standard hand enrollment or verification, or to enroll a user who is not present. If the user has previously enrolled using the standard enrollment procedures, the hand template will be deleted after no hand enrollment. If the user needs to go back to using hand verification, the user must be re-enrolled using the normal enrollment process.

➡ ***See "Enroll User" on page 90 for more information.***

Default: None

Range: None

Dependencies: User must be entered into the terminal before the user can be enrolled.

Who: A terminal administrator can enroll a user using no hand enroll at any time.

1. Log into the terminal as an administrator.

   ➡ ***See "Administrator Authentication" on page 47 for more information.***

2. Press ▭ User Management
3. Press ▭ List Users.
4. Scroll to the name of the user you wish to enroll using ◎ . Press the middle key to select the user.
5. Press ▭ More.
6. Press ▭ No Hand Enroll.
7. Enter the EPIN.
8. Press ▭ Enter.

Edit EPIN

An EPIN is used for verification if the HPU becomes non-functional. Select the user. Then add an EPIN to the user.

❗ ***An EPIN should be used as an emergency backup function only when the HPU fails. EPIN is not intended for regular use as it will compromise security.***

Default: None

Range: None

Dependencies: User must be entered into the terminal before an EPIN can be added.

Who: A terminal administrator can add an EPIN to any user's profile.

1. Log into the terminal as an administrator.

   ➡ ***See "Administrator Authentication" on page 47 for more information.***

2. Press ⬭ User Management
3. Press ⬭ List Users.
4. Scroll to the name of the user you wish to add an EPIN using ✥ . Press the middle key to select the user.
5. Press ⬭ More.
6. Press ⬭ Edit EPIN.
7. Enter the EPIN.
8. Press ⬭ Enter.

Edit Access Grant

Edits an access grant for particular user. Access grants are used to grant access to a user for a particular, recurring time period. Access grants override timezones. Select the user. Then select the access grant you want to edit. ➡ ***Access grants and timezones should not be used in the same site.***	**Default:** None **Range:** None **Dependencies:** None **Who:** A terminal administrator can edit an access grant at any time.

1. Log into the terminal as an administrator.

   ➡ ***See "Administrator Authentication" on page 47 for more information.***

2. Press ⬭ User Management

3. Press ⬭ List Users.

4. Scroll to the name of the user for which you want to edit the access grant using ◎. Press the middle key to select the user.

5. Press ⬭ More.

6. Press ⬭ Access Grant Menu.

7. Press ⬭ List Access Grants.

8. Scroll to the access grant you want to edit using ◎. Press the middle key to select the access grant.

9. Choose one of the following:

   a. Press ⬭ Remove AccessGrant to remove the access grant. Press ⬭ YES.

   b. Press ⬭ Edit StartTime to edit the start time. Enter the start time and press ⬭ Enter.

   c. Press ⬭ Edit DOW to edit the day of the week. Press ⬭ to toggle each day of the week and/or holiday.

   d. Press ⬭ Edit Duration to edit the duration. Enter the duration and press ⬭ Enter.

List Access Grants

Lists all access grant for a particular user. Access grants are used to grant access to a user for a particular, recurring time period. Access grants override timezones.

➡ ***Access grants and timezones should not be used in the same site.***

Default: None

Range: None

Dependencies: None

Who: A terminal administrator can list access grants at any time.

1. Log into the terminal as an administrator.

   ➡ ***See "Administrator Authentication" on page 47 for more information.***

2. Press ⬭ User Management
3. Press ⬭ List Users.
4. Scroll to the name of the user for which you want to list access grants using ◎. Press the middle key to select the user.
5. Press ⬭ More.
6. Press ⬭ Access Grant Menu.
7. Press ⬭ List Access Grants.
8. From here, many other functions can be accessed. See the other topics in this section for more information.

Add Access Grants

Adds an access grant particular user. Access grants are used to grant access to a user for a particular, recurring time period. Access grants override timezones. Select the user. Then add an access grant to the user.

➡ ***Access grants and timezones should not be used in the same site.***

Default: None

Range: None

Dependencies: None

Who: A terminal administrator can add access grants at any time.

1. Log into the terminal as an administrator.

   ➡ ***See "Administrator Authentication" on page 47 for more information.***

2. Press ⬭ User Management
3. Press ⬭ List Users.
4. Scroll to the name of the user for which you want to edit access grants using ◎. Press the middle key to select the user.
5. Press ⬭ More.
6. Press ⬭ Access Grant Menu.
7. Press ⬭ Add Access Grants.
8. Enter the start time using the format HH MM SS (Example: 13 22 59.)
9. Enter the duration using the format HH MM SS.
10. Press ⬭ Enter.
11. Press ⬭ to toggle each day of the week and/or holiday.

List Bookings

Lists all of the bookings (such as punches) for a particular user.

➡ ***This information is only accurate to within the last host synchronization.***

Default: None

Range: None

Dependencies: None

Who: A terminal administrator can list bookings for a user at any time.

1. Log into the terminal as an administrator.

   ➡ ***See "Administrator Authentication" on page 47 for more information.***

2. Press ⬭ User Management
3. Press ⬭ List Users.
4. Scroll to the name of the user for whom you want to list bookings using ⊙. Press the middle key to select the user.
5. Press ⬭ More.
6. Press ⬭ List Bookings.

Add User

Creates a new user profile in the terminal. Enter the user's RPIN credential. Other properties may be configured after the user is added.

Default: None

Range: None

Dependencies: None

Who: A terminal administrator can add users at any time.

1. Log into the terminal as an administrator.

   ➡ ***See "Administrator Authentication" on page 47 for more information.***

2. Press ⬭ User Management
3. Press ⬭ Add User.
4. Enter the RPIN.
5. Press ⬭ Enter.

   ➡ ***The terminal must check the host system at this point to ensure that the RPIN is not already in use. This process can sometimes take a while to complete. Wait until the next screen appears before pressing any other buttons.***

6. At this point, the user has been added. To configure other properties for this user (or to enroll the user) see the other topics listed in this section.

Security Menu

Clear Setup

Clear Setup

❗ ***Use caution when performing this function! All settings will be restored to factory settings. This action cannot be undone!***

Clear Setup can be used to restore all of the settings on the terminal back to their original state. Clear Setup will perform the following actions:

- All setup values will be returned to defaults (including sync settings)
- All databases will be cleared (for example, user database, interaction databases, etc.)

Default: None

Range: None

Dependencies: None

Who: A terminal administrator can use Clear Setup at any time.

1. Log into the terminal as an administrator.

   ➡ ***See "Administrator Authentication" on page 47 for more information.***

2. Press ⬭ Security Menu.
3. Press ⬭ Clear Setup.
4. Press ⬭ YES.

Biometric Setup

The Biometric Setup Menu is used to configure the level of security at the terminal. Biometric security is determined by a combination of template resolution and the number of access tries.

Min High Res Update Count

**Indicates the minimum number of time the terminal must update its high resolution template before switching to high resolution template verifications automatically.

➡ *****This option is currently not in use since all supported terminals are high resolution terminals.***

Default: NA

Range: NA

Dependencies: NA

Who: NA

1. Log into the terminal as an administrator.

   ➡ ***See “Administrator Authentication” on page 47 for more information.***

2. Press ⬭ Security Menu.
3. Press ⬭ Biometric Setup.
4. Press ⬭ Min High Res Count.
5. Enter the Set Min High Resolution Update Count.
6. Press ⬭ Enter (or Clear to cancel).

Placements Per Try

Placements Per Try defines the number of hand placements allowed during a verification attempt.

➡ ***A “try” is the presentation of a credential ID during a verification attempt. A “placement” is the presentation of a hand to the GT-Series terminal during a verification attempt.***

Default: 3

Range: 1-99

Dependencies: None

Who: A terminal administrator specifies this value in coordination with Number of Tries to indicate how forgiving the terminal will be during verification.

1. Log into the terminal as an administrator.

   ➡ ***See “Administrator Authentication” on page 47 for more information.***

2. Press ⬭ Security Menu.
3. Press ⬭ Biometric Setup.
4. Press ⬭ Placements/Try.
5. Enter the number of placements per try.
6. Press ⬭ Enter.

Number of Tries

Number of Tries defines the number of verification attempts allowed for a user. Once the number of tries has been exceeded, the credential ID will be locked out until a terminal administrator verifies at the terminal. For increased security, use a lower number. For increased convenience, use a higher number.

➡ ***A try is the presentation of a credential ID during a verification attempt. A placement is the presentation of a hand to the hand reader during a verification attempt.***

Default: 3

Range: 1-99

Dependencies: None

Who: A terminal administrator specifies this value in coordination with Placements Per Try to indicate how forgiving the terminal will be during verification.

1. Log into the terminal as an administrator.

   ➡ ***See "Administrator Authentication" on page 47 for more information.***

2. Press ⬭ Security Menu.
3. Press ⬭ Biometric Setup.
4. Press ⬭ Number of Tries.
5. Enter the number of tries.
6. Press ⬭ Enter.

Template Resolution

Sets the template resolution to High or Non-biometric. Set this option to High for Biometric terminals. Set this option to non-biometric for those terminals you run in Non-biometric mode (those terminals which do not use hand recognition in order to use the terminal). In non-biometric mode, terminals can use both an RPIN and EPIN (if an EPIN has been created) or an RPIN only (if an EPIN has not been created).

Default: NA

Range: NA

Dependencies: NA

Who: An administrator can use this setting at any time, as needed.

1. Log into the terminal as an administrator.

   ➡ ***See "Administrator Authentication" on page 47 for more information.***

2. Press ⬭ Security Menu.
3. Press ⬭ Biometric Setup.
4. Press ⬭ Template Resolution.
5. Scroll to and select High or Non-biometric by using ◈.

Set Passwords

Set Passwords	
Sets the password for command line access to the terminal. CLI access is only available if all other conditions for enabling CLI access have been met.	**Default:** Schlage538 **Range:** Must match host application password **Dependencies:** Other conditions for CLI access be met before command line access to the terminal will be available. **Who:** An application developer can change the CLI access password to enhance security, or as a troubleshooting, testing or debugging step.

1. Log into the terminal as an administrator.

   ➡ ***See "Administrator Authentication" on page 47 for more information.***

2. Press ⬭ Security Menu.
3. Press ⬭ Set Passwords.
4. Press ⬭ Set CLI Access Pwd.
5. Enter the CLI access password.
6. Press ⬭ Enter.

Clear UserDB

Clear UserDB

Clear UserDB will remove all users from the terminal.

❗ ***This function cannot be undone. However, all users will be restored to the terminal the next time the terminal synchronizes with a host application.***

Default: None

Range: None

Dependencies: None

Who: A terminal administrator can use Clear UserDB to remove all users from the terminal.

1. Log into the terminal as an administrator.

   ➡ ***See "Administrator Authentication" on page 47 for more information.***

2. Press ⬭ Security Menu.
3. Press ⬭ Clear UserDB.
4. Press ⬭ YES.

Factory Settings

Factory Settings

Factory Settings is a list of useful information about the factory settings of the terminal. Factory settings cannot be edited. The following list will be displayed:

- User Capacity: number of users that can be stored
- BPUType: type of biometric processing unit
- BoardRevision: version of the internal hardware
- MemorySizeMB: total capacity of the SD card
- SerialNum: serial number
- Model: model number
- Credential Reader Type: all available credential reader types

Default: None

Range: None

Dependencies: None

Who: A terminal administrator can use Factory Settings to view the factory settings of the terminal, most likely as a troubleshooting step.

1. Log into the terminal as an administrator.

   ➡ ***See "Administrator Authentication" on page 47 for more information.***

2. Press ⬭ Security Menu.
3. Press ⬭ Factory Settings.

Reject Threshold

At each verification attempt, the hand placement is compared to the user template. A score that reflects how closely the placement and the template match is assigned. The lower the score, the closer the match. The reject threshold defines the minimum score that must be attained for verification.

Reject Threshold

Sets the global biometric reject threshold for all users enrolled in the terminal who do not have an individual reject threshold.

For increased security or decreased FAR (False Acceptance Rate), use a lower number. For increased convenience or decreased
FRR (False Rejection Rate), use a higher number.

➡ ***A reject threshold set at the user level will override this setting.***

Default: 75

Range: 30-255

Dependencies: None

Who: A terminal administrator should set this value during initial configuration of the terminal. A terminal administrator can also change this value at an existing site if there is a need to increase security or user convenience.

1. Log into the terminal as an administrator.

   ➡***See “Administrator Authentication” on page 47 for more information.***

2. Press ▭ Security Menu.
3. Press ▭ Set Reject Threshold.
4. Enter the reject threshold.
5. Press ▭ Enter.

Set Credential Logging Flag

Set Credential Logging Flag

This setting is mainly used for debugging purpose. When enabled, the credential/Barcode information of all users will logged into the Terminal log file.

Default: Enabled

Range: None

Dependencies: None

Who: A terminal administrator can set Credential Logging Enabled at any time.

1. Log into the terminal as an administrator.

   ➡ ***See "Administrator Authentication" on page 47 for more information.***

2. Press ⬭ Security Menu.
3. Press ⬭ More.
4. Press ⬭ Set Credential Logging Flag.
5. Press ⬭ to Enable (or Disable).

Restore Factory Password

Restore Factory Password

Use this option to restore the factory password for a given terminal.

Default: Enabled

Range: None

Dependencies: None

Who: A terminal administrator can restore the factory password at any time.

1. Log into the terminal as an administrator.

   ➡ ***See "Administrator Authentication" on page 47 for more information.***

2. Press ⬭ Security Menu.
3. Press ⬭ More.
4. Press ⬭ Restore Factory Password and press ⬭ YES to confirm.

Maintenance Menu

Partial Sync Now

If changes to users are made to the terminal that need to be immediately implemented, Partial Sync Now can be used. Partial Sync Now will start a database synchronization process between the terminal and host application as soon as possible. Only user adds and edits are transferred during Partial Sync Now. No users will be removed during Partial Sync Now. Note that only changes made after previous sync will be synchronized

Default: None

Range: None

Dependencies: None

Who: A terminal administrator can use Partial Sync Now to synchronize user data immediately.

1. Log into the terminal as an administrator.

   ➡ ***See "Administrator Authentication" on page 47 for more information.***

2. Press ⬭ Maintenance Menu.
3. Press ⬭ Partial Sync Now.

Sync Now

If changes are made to the terminal that need to be immediately implemented, Sync Now can be used. Sync Now will start a database synchronization process between the terminal and host application as soon as possible.

Default: None

Range: None

Dependencies: None

Who: A terminal administrator can use Sync Now to synchronize user data immediately.

1. Log into the terminal as an administrator.

   ➡ ***See "Administrator Authentication" on page 47 for more information.***

2. Press ⬭ Maintenance Menu.
3. Press ⬭ Sync Now.

Reboot

Reboot will perform a CPU reset of the terminal. Pressing Reboot will start the reboot process. The reader will appear to power down and then start the boot-up process.

Default: None

Range: None

Dependencies: None

Who: An application developer/tester (or any individual under the guidance of a technical support representative) can reboot the terminal as a troubleshooting, testing or debugging step.

1. Log into the terminal as an administrator.

   ➡ ***See “Administrator Authentication” on page 47 for more information.***

2. Press ▭ Maintenance Menu.
3. Press ▭ Reboot.
4. Press ▭ Yes to reboot (or ▭ No to discontinue reboot request).

Terminal Status

The information contained in the Terminal Status menu is tremendously important in troubleshooting a terminal problem. The first step of determining the cause of nearly any problem with the terminal is knowing what software versions the terminal is running and verifying that those versions are expected or up to date.

Default: None

Range: None

Dependencies: None

Who: A terminal administrator can access this information at any time.

The following information will be displayed:

- TerminalIP: the IP address of the terminal
- LogicalName: the unique logical named assigned to the terminal
- AppVersion: the application software version.
- BSPVersion: the version of the board OS used by this terminal.
- CommLibVer: the version of the communications library used by this terminal software.
- HPUVersion: the version of the HPU
- SyncProtocolVersion: the sync protocol version number for the terminal.
- UserCount: the number of users that are stored in this terminal.
- Interactions: the number of interactions that have not yet been sent to the host.
- SentInteractions: the number of interactions that have been sent by the terminal to the host.
- AcceptingPunches: Specifies if the terminal is accepting punches.
- LastSyncTimeStamp: the last DB Sync timestamp.
- NextScheduledDBSync: the next time the terminal is to sync
- BackupBatteryOn: indicates whether the Terminal is running on Battery power
- TotalDiskSpace: the total amount of space on the SD card.
- UsedDiskSpace: the amount of space that has been used on the SD card.
- AvailableDiskSpace: the amount of space left on the SD card.
- 1aWkrStatus: Status of the DBSync worker thread used to send Interactions to the host
- PhaseIIWkrStatus. Status of the DBSync worker thread used to pull the updates from the host
- PurgeEvalPackWkrStatus: Status of the DBSync worker thread used to evaluate the sent interactions for purging purposes
- BootPartition: current (Primary/Secondary) partition from which the Terminal is booted
- BootedGolden: indicates whether the Terminal has booted from a partition set in the factory
- PrimaryPartitionVersion: Version of the BSP on Primary partition
- SecondaryPartitionVersion: Version number of the Secondary Partition
- GoldenPartitionVersion: Version number of the Golden Partition
- APSVersion: Version number of the APS
- XMLLIBVersion: Version number of the XMLLIB partition
- UBootVersion: Uboot version

1. Log into the terminal as an administrator.

   ➡***See "Administrator Authentication" on page 47 for more information.***

2. Press ⬭ Maintenance Menu.

3. Press ⬭ Terminal Status.

4. You can navigate though the status list by using✥.

Delete Sent Interactions

Delete Sent Interactions also clears sent interactions from the database on the terminal. The database contains all interactions with the terminal. Only interactions that have been sent to the host application will be cleared from the database when Delete Sent Interactions is used.

❗ ***Delete Sent Interactions MUST be performed on a regular basis. If not, the SD card could become too full and cause the terminal to discontinue receiving user punches. You will start to see warnings when the card is 30% full. At 45% full, the terminal will no longer accept punches.***

Default: None

Range: None

Dependencies: None

Who: A terminal administrator can use Delete Sent Interactions to remove old information that is no longer necessary in order to create room on the SD card for new information.

1. Log into the terminal as an administrator.

   ➡ ***See "Administrator Authentication" on page 47 for more information.***

2. Press ⬭ Maintenance Menu.
3. Press ⬭ Delete Sent Interactions.
4. Enter the number of days to retain sent interactions. A value of 0 deletes all sent interactions.
5. Press ⬭ Enter.

Shutdown

Shutdown is used to properly shut down the terminal. The terminal screen will indicate that the terminal is shutting down. Wait until the LED bar is no longer illuminated before removing power.

Default: None

Range: None

Dependencies: None

Who: A terminal administrator must use the shutdown operation before removing power from the terminal.

1. Log into the terminal as an administrator.

   ➡ ***See "Administrator Authentication" on page 47 for more information.***

2. Press ⬭ Maintenance Menu.
3. Press ⬭ Shutdown.
4. Press ⬭ Yes to shutdown (or ⬭ No to discontinue the shutdown request).
5. Wait until the LED bar is no longer lit.
6. You can now safely remove power from the terminal if needed.

Last Punch

Last Punch

Last Punch shows the last punch into the terminal. The user's last name, status (IN or OUT) and date and time of punch is displayed.

➡ ***This information is only accurate to within the last host synchronization.***

Default: None

Range: None

Dependencies: None

Who: A terminal administrator can view the last punch into the terminal at any time.

1. Log into the terminal as an administrator.

   ➡ ***See "Administrator Authentication" on page 47 for more information.***

2. Press ⬭ Last Punch.

FKScript List Menu

➡ ***This menu is available only when you are in Demo Mode.***

Activating the Function Key Script

The FKScript List menu uses an example script that was designed to show you some of the types of application you may want to implement at your own site. The sample applications access the Demo mode database which has been preloaded with a list of users and user messages.

➡ ***For more information about Demo Mode and the preloaded user database it uses, see the GT-Series Integration Package Quick Start Guide.***

FKScript List

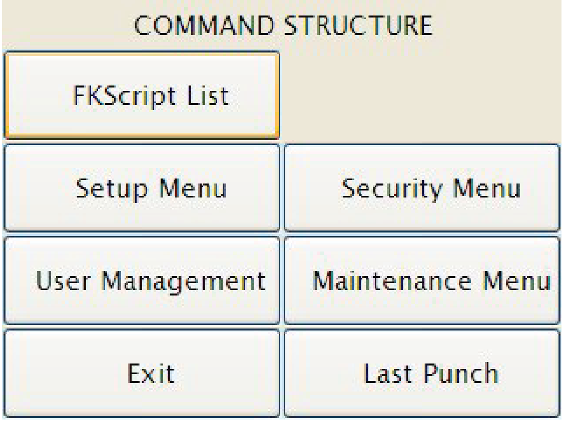
Activating the Function Key Script (FKScript List option)	
After you log in as an Administrator and go to Demo Mode, you can use the FKScript List option to activate the Function Key script.	**Default:** None **Range:** None **Dependencies:** None **Who:** A terminal administrator can activate this option any time from Demo Mode only.

1. From Demo Mode, log into the terminal as an administrator.

   ➡ ***See “Administrator Authentication” on page 47 for more information.***

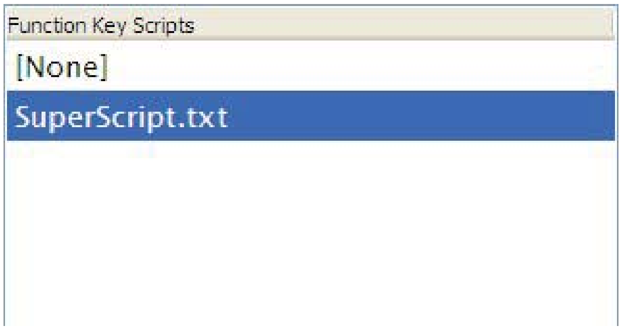
2. Figure shows the COMMAND STRUCTURE menu in Demo Mode.:

   Figure 6-1 Function Key Script List Option Accessible in Demo Mode



3. Press FKScript List. The script selection list displays as shown in Figure 6-2.

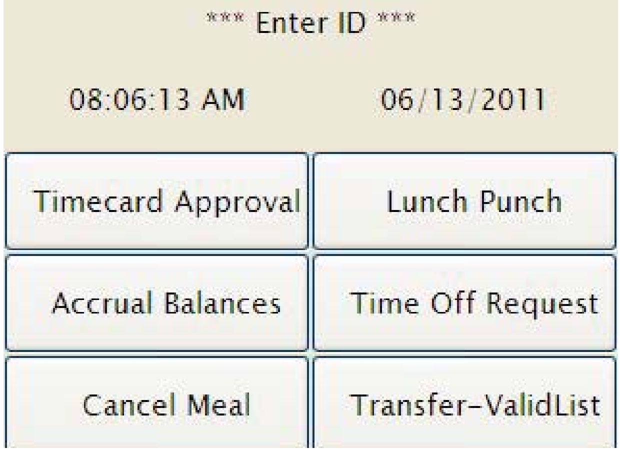
   Figure 6-2 Selecting the Function Key script



4. Scroll to the SuperScript option using . Press the middle key to select the Function Key script.

   The list of available Function Key script options displays. See Figure 6-3.

   Figure 6-3 Function Key Script Options


*** Enter ID ***

08:06:13 AM 06/13/2011

Timecard Approval

Timecard Approval

After the Function Key script has been activated in Demo Mode, you can log in and select the Timecard Approval option to view any unapproved timecards you may have.

Default: None

Range: None

Dependencies: None

Who: Any user can use this option any time after logging into the Terminal in Demo Mode

1. Press ⬭ Timecard Approval.
2. When prompted, log into the terminal.
3. If you have any unread messages (such as any new unapproved timecards) you will be prompted whether you want to read them. If so, press ⬭ YES.
4. After reviewing the timecard, press ⬭ Approve to approve the timecard, or press ⬭ Back to disapprove (or defer approving) the timecard.

Accrual Balances

Accrual Balances

After the Function Key script has been activated in Demo Mode, you can log in and select the Accrual Balance option to view any used and available vacation and sick leave you may have.

Default: None

Range: None

Dependencies: None

Who: Any user can use this option any time after logging into the Terminal in Demo Mode

1. Press ⬭ Accrual Balances.
2. When prompted, log into the terminal.
3. Your accrued and available vacation and sick leave time displays.

Cancel Meal

<table>
<tr><th colspan="2">Cancel Meal</th></tr>
<tr><td>After the Function Key script has been activated in Demo Mode, you can log in and select the Cancel Meal option to cancel a meal deduction.</td><td><b>Default:</b> None
<b>Range:</b> None
<b>Dependencies:</b> None
<b>Who:</b> Any user can use this option any time after logging into the Terminal in Demo Mode</td></tr>
<tr><td colspan="2">1. Press ⬭ Cancel Meal.
2. When prompted, log into the terminal.
3. You will receive a meal cancellation notification.</td></tr>
</table>

Lunch Punch (Meal Compliance)

<table>
<tr><th colspan="2">Lunch Punch (Meal Compliance)</th></tr>
<tr><td>Lunch Punch is typically used to enforce break/meal law regulations. You must be an Administrator to set Lunch punch lockout values. A user can then use the Function Key script's Lunch Punch option to punch back in from a meal break.
If the user punches in earlier than the specified Lunch Punch lockout setting, the user will receive a message indicating that he/she has attempted to log in earlier than the specific lockout session. The number of minutes/seconds the user must wait to punch back in is also specified.</td><td><b>Default:</b> None
<b>Range:</b> None
<b>Dependencies:</b> A lunch punch lockout setting must be activated by the Administrator prior to using this option.
<b>Who:</b> Any user can use this option any time after logging into the Terminal in Demo Mode.</td></tr>
<tr><td colspan="2">1. Press ⬭ Lunch Punch.
2. When prompted, log into the terminal.
3. If successful, the user will receive a message indicating successful lunch punch.</td></tr>
</table>

Time Off Request

<table>
<tr><th colspan="2">Time Off Request</th></tr>
<tr><td>After the Function Key script has been activated in Demo Mode, you can log in and select the Time Off Request option to request to take vacation or sick leave time.</td><td><b>Default:</b> None
<b>Range:</b> None
<b>Dependencies:</b> None
<b>Who:</b> Any user can use this option any time after logging into the Terminal in Demo Mode</td></tr>
<tr><td colspan="2">1. Press ⬭ Time Off Request.
2. When prompted, log into the terminal.
3. Scroll to the desired option in the list (AvailableVacation or AvailableSickHours) using ⊕. Press the middle key to select the desired option.
4. Enter the start date, using the format mm dd yyyy. (Example: 12 22 2011) and press ⬭ Enter.
5. Enter the total number of hours you want to take off. Press ⬭ Enter. If the number of hours you enter exceeds the total number of available hours, you will receive an error message.
6. After the request is accepted, you will see updated balances reflecting the requested time off.</td></tr>
</table>

Transfer-ValidList

<table>
<tr><th colspan="2">Transfer-ValidList</th></tr>
<tr><td>After the Function Key script has been activated in Demo Mode, you can log in and select the Transfer-ValidList option to transfer a user from one department and job to another (based on a predefined list of valid departments and jobs that have already been set up for that user).</td><td><b>Default:</b> None
<b>Range:</b> None
<b>Dependencies:</b> The administrator must first set up the list of valid departments for a given user to transfer. In Demo Mode, a list of valid departments has already been set up.
<b>Who:</b> Any user can use this option any time after logging into the Terminal in Demo Mode</td></tr>
<tr><td colspan="2">1. Press ⬭ Transfer-ValidList.
2. When prompted, log into the terminal.
3. Scroll to the desired department to which you want to transfer ◎. Press the middle key to select the department.
4. Scroll to the desired job to which you want to transfer ◎. Press the middle key to select the job.
5. You will see a transfer confirmation which displays the department and job to which you are to transfer.</td></tr>
</table>

Understanding GT-Series Biometric Terminals 7

Reviewing Hand Geometry Basics

This chapter will provide some basic information for those users who have never used a biometric terminal.

Hand Geometry Considerations

The terminal reads the shape of the hand, not the fingerprints or palm prints. Also note the following:

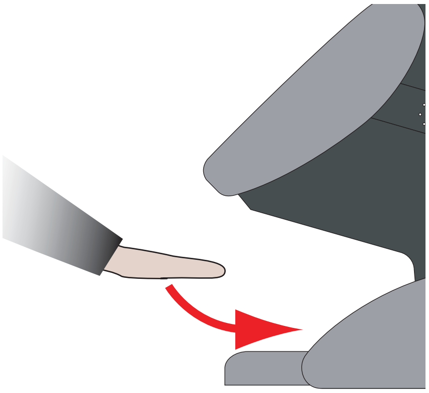
- It does not identify people. It verifies people's identity.
- It scans with an invisible light of the type used in TV remote controls.
- It does not transfer germs any more than a doorknob or money.
- It does not invade privacy; it guarantees it.
- The enrollment process requires three or more reads to collect enough information to create a template.

NOTE: For users with special needs that require a no hand enrollment, see "No Hand Enroll" on page 95.

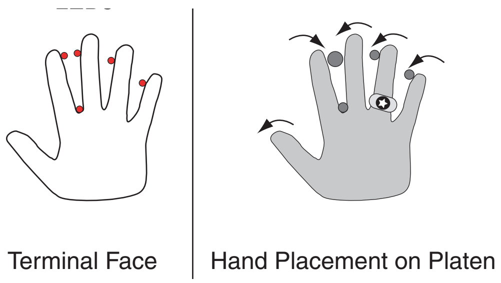
Proper Hand Placement

For correct, consistent hand reads it is very important that your hand is placed on the platen in the same manner every time. The following rules apply for proper hand placement on the platen.

1. If you are wearing a ring, rotate the ring so the stone faces up in its normal position.
2. Slide your right hand onto the platen rather like an airplane landing at the airport.
3. Slide your hand forward until the web between your index and middle finger stops against the web pin.
4. Keep your hand flat. You should feel the surface of the platen on your palm and the underside of your fingers.



5. Close your fingers together until they touch the finger pins and watch the hand diagram on the terminal display. There are small LEDs on the hand diagram that correspond with the finger pins. Your thumb should be held wide to the side.
6. The LEDs turn off when you have properly placed your fingers. If an LED remains on, a finger is not in proper contact with a finger pin.



Terminal Face

Hand Placement on Platen

Understanding Hand Read Scores

When a user verifies his/her hand, a score of the verification quality is generated. The score is displayed on the terminal's display after a successful verification.

The score can be found in the interaction data for the verification. This information is viewable in the Host Application.

The score number on the display reflects how accurately the user's hand is placed on the platen. Scores that vary greatly between low and high numbers are indicative of inconsistent hand placement. Scores above 50 are indicative of improper hand placement or of a drastic change in the physical appearance of the hand.

When this occurs, emphasize the importance of sliding the hand onto the platen and keeping the hand flat. Re-training and practice should lower a user's score. It might be necessary to assign an individual user reject threshold if the user has a mild disability. Re-enrollment might be necessary to create a new user template.

Understanding Verification Messages

Various messages can appear on the terminal's display during hand verification, as listed in Table 7-1.

NOTE: If you enter your ID number, but do not place your hand on the platen, the terminal will time-out in approximately 25 seconds. You can immediately end this timeout by pressing (ENTER) **.**

Table 7-1: Messages Displayed During Verification

Message	**Definition**
PLACE HAND	The platen is ready to receive your hand for verification.
OK <user name>	You are verified, proceed.

Table 7-1: Messages Displayed During Verification (Continued)

Message	Definition
REMOVE HAND	Remove your hand and place it on the platen again. Follow proper hand placement rules.
TRY AGAIN	Your attempt was rejected. Repeat verification following proper hand placement rules.
TIME RESTRICTION	You are not authorized to punch in at this time. If this seems to be in error, contact your supervisor about time restrictions.
ID INVALID	Your rejections exceeded the maximum number of tries allowed. Wait until a supervisor has verified and try again or call your supervisor.
ENTER ID	You entered your ID number incorrectly or your access time is restricted.
MOVE THUMB	Your thumb is interfering with the read attempt. Slide your thumb to the side of the terminal.
LIFT UP SLEEVE	Your sleeve is interfering with the read attempt. Slide your sleeve away from the body of the terminal.

Reviewing LED Bar Indications

When Terminal is Idle

Table 7-1: LED Bar Indication When Terminal is Idle

Event	LED
Connected to the terminal	Blue
Not connected to the terminal	Amber
Not connected to host application	Red

During Verification

Table 7-2: LED Bar Indications During Verification

Operation	Event	Beeps*	LED
During Keypad Entry	Keystroke accepted	1 per keystroke	no change
After ID Entry	OK-place hand	1	Slow blinking amber
	ID number not in database User locked out Timezone violation	2	No change
After Hand Placement	Hand image captured	1	White/Purple
	ID verified	1	Green
	ID not verified - try again	2	Red
	ID refused	2	Red
* Beeper will only sound if beeper is enabled. See "Set Beeper" on page 67 for more information.			

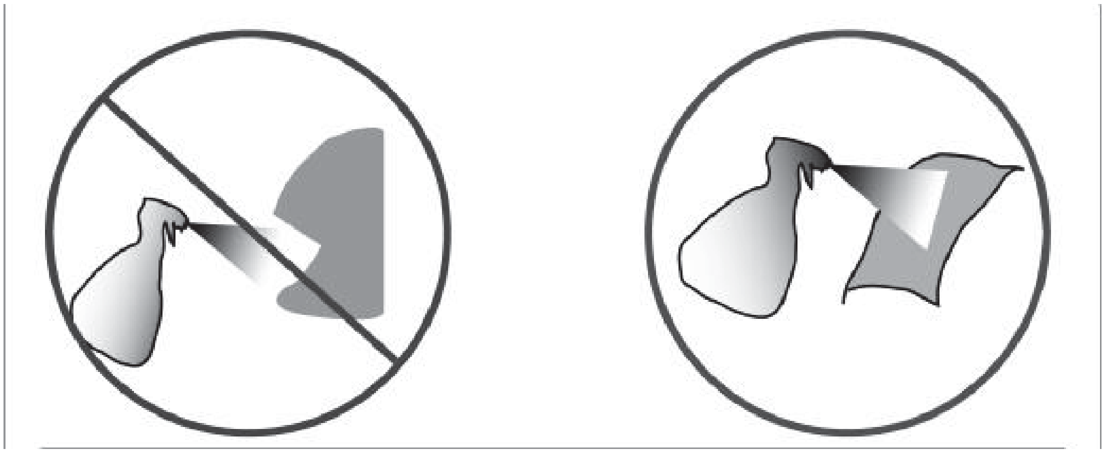
During Enrollment

Table 7-3: LED Bar Indications During Enrollment

Event	Beeps*	LED
OK - place hand	1	Slow blinking amber
Hand image captured	1	White/Purple
Bad hand placement, try again	1	Blinking red
* Beeper will only sound if beeper is enabled. See "Set Beeper" on page 67 for more information.		

Cleaning the Terminal and Platen

Inspect and clean the terminal regularly to maintain optimum performance. Clean the platen, side mirror, reflector, and the window above the platen using a clean cloth dampened with ordinary, nonabrasive window cleaner. Start at the rear corners of the platen and work your way forward.



❗ ***DO NOT SPRAY CLEANING FLUID DIRECTLY INTO OR ON THE TERMINAL.***

❗ ***There are NO user-serviceable parts inside the terminal.***

Troubleshooting 8

Viewing Terminal Status

Using the Terminal

The easiest step to take for any problem is to view the terminal status. It is useful to see the last network activity in which the terminal was involved. If you call technical support you will be asked to provide this information, since it lists all of the software versions running in the terminal. Terminal status lists such information as software versions, user database information, network information, and sync status.

To access the terminal status screen, see “Terminal Status” on page 110.

Using a Web Browser

➡ ***The administrator must have an EPIN assigned to him/her in their user record in order to use the terminal's web browser.***

1. From a computer on the same network as the terminal, open a web browser.
2. Enter the IP address of the terminal in the address bar of the web browser, and press Enter or click Go. The welcome screen should appear.
3. Log in with the ID and EPIN of an administrator.
4. Click the Terminal Status button. The same information that appears in the Terminal Status command menu is listed here.

Using Telnet

Telnet will likely be the single most useful maintenance and diagnostic tool you will use with GT-Series terminals. It provides a command line-style interface to the actual terminal, identical to the DOS prompt in Windows. "Run a telnet session and check the log file" is the most commonly used phrase when troubleshooting a terminal.

Choosing a Telnet Client

➡ ***The DOS prompt cannot be used as a telnet client to connect to your terminal.***

HyperTerminal comes with Windows, and can be used to create a telnet connection to your terminal. However it is not recommended because it has limited viewing and saving capabilities.

It is strongly recommended that you use the telnet client PuTTY (pronounced "PUH-tee"). It has robust saving capabilities and configuration options. It can be downloaded (for free) at the following address:

http://www.versiontracker.com/dyn/moreinfo/win/16985

The PuTTY developer's site is located at the following address:
http://www.chiark.greenend.org.uk/~sgtatham/putty/

Logging In and Out of Telnet

1. Enter the IP address of your terminal into your telnet client.
2. Click OK. A window will appear that displays the prompt
   `accord1 login:`
3. Enter the login name, which is root (it is case-sensitive).
4. Enter the password, which is 1520rsi by default (it is also case-sensitive).

❗ ***All directories, commands and files in Linux are case-sensitive. Pay very close attention to case when entering text because the difference between checking the status and deleting the entire file system can be a matter of using the wrong casing for a letter. Also, bear in mind that Linux is not as forgiving as other operating systems when it comes to making certain changes; if you delete a file, it is deleted forever; there is no undo or Recycle Bin. However, as long as you have a host connection, you need only reboot, and the host server will give back everything you deleted after it synchronizes.***

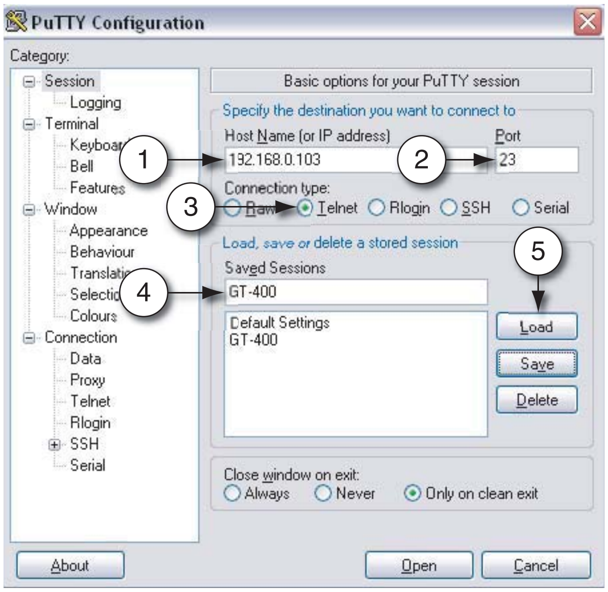
5. If the login is successful, the following prompt displays: ~#
   This is the Linux shell prompt.
6. To logout of the telnet session, type exit and press enter from anywhere in the shell.

Using a Telnet (PuTTY) Session

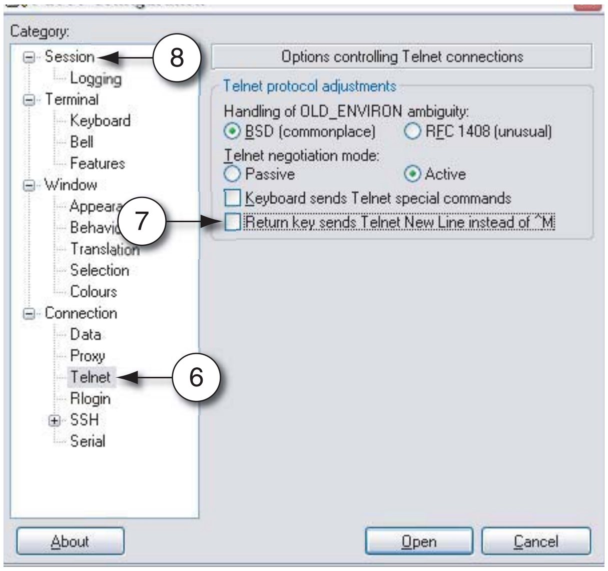
1. Enter the IP address for the terminal.

   ➡ ***See “Terminal Status” on page 110 for information on obtaining the terminal's IP address.***

2. Enter the telnet port number: 23.
3. Click the Telnet radio button.
4. Enter a title for the new profile.
5. Click Save to save the profile. If you have created a profile for this terminal in the past, you can select the profile from the list and click Load.
6. Click Telnet.
7. Uncheck the box labeled Return key sends Telnet New Line instead of ^M.
8. Click Session.
9. Save the profile again by clicking Save before opening the telnet session by clicking Open.
10. Once the telnet session is open, you can enter commands into the telnet window as described in other sections of this guide.
11. If you want to log your telnet session, click Logging.



Host Name (or IP address): 192.168.0.103
Port: 23
Connection type: ○ Raw ● Telnet ○ Rlogin ○ SSH ○ Serial
Saved Sessions: GT-400
Default Settings
GT-400
Close window on exit: ○ Always ○ Never ● Only on clean exit



Handling of OLD_ENVIRON ambiguity: ● BSD (commonplace) ○ RFC 1408 (unusual)
Telnet negotiation mode: ○ Passive ● Active
□ Keyboard sends Telnet special commands
□ Return key sends Telnet New Line instead of ^M

Changing the Telnet Password

Since all terminals come with a default telnet password (1520rsi), you will want to change it for security reasons.

1. At the prompt, type `passwd root`. This tells the shell you wish to change the password for the user root. The change password dialog will appear.
2. Enter the new password. Be sure to conform to the naming requirements.
3. Enter the password again. The password is now changed.

Navigating the File System

Once you are at the prompt, you are communicating with the terminal at a command-line level, similar to a DOS prompt in Windows. With DOS you can navigate the hard drive of your computer. With telnet you can navigate the SD card of the GT-Series Terminal. There are commands you can use to navigate the directories, view files and start or stop programs. Some of the most useful commands (such as cd, tail, cat, and ps) are described in this chapter; they are safe to experiment with as often as you want (as long as you keep in mind that commands are case sensitive).

Changing Directories Using the cd Command

The cd command is used to navigate from directory to directory. For example, if you type cd RecogSys at the first prompt, you will be moved to the RecogSys directory.

➡ ***The main directory is called root, so if you are ever asked to "cd to root", simply type cd anywhere and you will be taken to the main directory.***

One of the most useful features in Linux is filename/directory auto-fill, which enables you to type in only a portion of a directory name. For example, to change directories to RecogSys, you need only type a portion of the directory name (the portion that makes it unique from other existing directory names) and then press the tab key to “fill in” the rest of the directory name.

For example, if you want to change directories to RecogSys/Src/Python/RSITerm, you can do the following:

1. Type `cd R` and press the Tab key on the keyboard. The remainder of the directory name “RecogSys” will display, since, in this example, the “R” is unique enough in the list of available directory names to distinguish it from other directory names.
2. Continuing on, you can type `S` (plus Tab key), `P` (plus Tab key), `RSIT` (plus Tab key). Just keep in mind that if there are multiple directories that start with the same letter, you'll need to fill in enough letters to uniquely identify to the shell what directory is it is that you want to auto-fill.

Viewing Terminal Processes Using the ps Command

The ps command is used to view a list of all the processes running in the terminal. If have ever used the Task Manager in Windows, viewing the Processes tab is similar. If you execute the ps command on an active terminal, you will see a number of "python RSITerm.pyc" listings. These are all of the active processes (or threads) of the terminal application. If you do not see any "*python RSITerm.pyc*..." processes running, it means your terminal application has stopped.

To use the command, type `ps` at the prompt and press Enter.

Rebooting the Terminal Via Telnet

When you are having trouble with your PC, often the first thing to do to resolve the issue is to reboot it - the same is mostly true for the GT-Series Terminal. And just as you would not yank the power cable out of your PC to restart it, you should not power cycle the GT-Series Terminal before trying to reboot it gracefully. If you are unable to reboot through the command menus or the host server command, you can reboot it through the telnet session.

The command is `reboot` (and press Enter).

NOTE: After you have entered this command (and press Enter), the terminal may take up to a minute to shut itself down.

Shutting Down the Terminal Via Telnet

If you would rather shutdown the terminal as opposed to rebooting it, the command is `shutdown` (and press Enter).

Shutting Down The Application Via Telnet

If you shutdown the terminal with the poweroff argument (`shutdown poweroff`), you are telling the terminal to power down completely. However, if you run that same script, but give it the `nop` argument (`shutdown nop`), you are telling the terminal to shutdown only the application, but leave Linux running.

The command is `shutdown closeapp` (and press Enter).

This will shutdown the application and return you to the Linux shell prompt.

Starting the Application in Verbose Mode

After you have run the shutdown script with the `nop` argument, you can start the application again. If you start it in verbose mode, you will see a lot of messages during the start-up that should help you diagnose what is going on.

➡***When you're ready to take the terminal live again, you should reboot it. Avoid leaving a terminal on your live site running in verbose mode, because will put unnecessary strain on your terminal.***

The command is `vstartapp` (and press Enter).

Accessing a Terminal in Demo Mode Through Telnet

➡***These instructions ONLY apply to a terminal that has never been connected to a network.***

1. Using a cross-over cable, connect a computer to the terminal.
2. Access the Internet Protocol (TCP/IP) settings for your computer.

   ➡***See the documentation for your operating system for more information, or contact your system administrator for help.***

3. Set the IP address to 192.168.1.112.

   ➡***Your computer will not communicate with a network after changing this setting.You will need to write down your computer's TCP/IP settings and change them back when you are finished working with the terminal if you need to connect to a network.***

4. Open a telnet session to 192.168.1.110, or the IP address of your terminal, using a telnet client of your choice (a command prompt will not work properly).

   ➡***If the terminal has never been on a network, the IP address will be 192.168.1.110. If the terminal has been on a network, the IP address may be different. If you cannot determine your terminal's IP address, see “Returning the Terminal to Its Factory Settings” on page 132 to reset your terminal.***

5. At the `accord1 Login:` prompt, type `root`.
   At the `password:` prompt, type `1520rsi`.

You are now accessing the root directory of the terminal.

Using the Terminal Log File

The terminal log file resides in the terminal and provides a clear picture as to what is going on in the terminal. If you are experiencing any kind of issue, your first step should be to check the terminal's log file. This can often point out the last task the terminal was working on before it encountered the problem.

You can view the log file from your telnet session.

1. cd to RecogSys/ZODB:

   ```
   cd RecogSys/ZODB
   ```

2. Type `ls` (and press Enter) to see the list of files in this directory. The log file is named RSITerm.log.

Viewing the Log File Using the cat Command

There are a different ways to view the log file depending on your needs and circumstances. If the log file is small, the quickest way may be to use the `cat` command from the directory where the log file is located:

```
cat <log filename>
Example: cat RSITerm.log
```

At the prompt, type `entirelog` and press Enter.

This command provides the entire log file, which may exceed your window or buffer setting. However, the last line or last few lines are usually the most important. If you see a sync that did not complete, or an exception error message, you have likely found the source or your problem.

Viewing the Last Few Lines of the Log File Using the tail Command

The `tail` command can be used to look at just the last few lines of the log file.

The command is `recentlog`.

This will show the last 50 lines of the log file by default.

Saving the Log File to Your Computer

If you want to see the entire log file, or if your technical support representative requests it, you can easily save it to a file using PuTTY.

1. Before you start the telnet session, go to the Logging menu in the PuTTY setup window.

2. Select the radio button Log all output to a file and in the text field box, enter the name you want the log file to save. Click Browse to select the desired save location.

   ➡ ***It is recommended as a best practice to name the saved log file by the terminal's name and the date and time that the log file was saved. Save the log file to your desktop.***

3. Go back to the Session category, and click Save.

   ➡ ***This will create a log file for every telnet session you make to this terminal. Be careful not to over-write the log file (meaning if you close the session and create a new one, the log file from the previous session will be over-written). Before you start another telnet session, either move the log file or turn off logging in that session.***

Returning the Terminal to Its Factory Settings

If you have been using a terminal in Demo mode and want to convert it to network mode, you must first delete the database and log files on the terminal. This can be done either through telnet or through the terminal interface.

Through Telnet

1. Access the terminal through telnet.

   ➡ ***See "Accessing a Terminal in Demo Mode Through Telnet" on page 130 on page 99 for more information.***

2. Type `cd RecogSys/ZODB` and press Enter.
3. Type `rm *` and press Enter. This removes all files (using the wildcard *) in this directory.

Through the Terminal Interface

1. Clear the terminal setup.

   ➡ ***See "Clear Setup" on page 101 for more information.***

2. Clear the user database.

   ➡ ***See "Clear UserDB" on page 105 for more information.***

3. Reboot the terminal.

   ➡ ***See "Reboot" on page 109 for more information.***

Using the Terminal Command Line Interface (CLI)

The command line interface (CLI) is a program that runs within a telnet session. It allows you to explore the actual database of users, interactions, and so forth. If your log is not giving you very much information, you could choose to explore the terminal through the CLI for troubleshooting purposes.

There is integrated help within the CLI, which you can access by typing `h` at the prompt. The most useful basic activities are viewing interactions that have been sent to the host server, and viewing the total interaction list. If, for example, you are looking for a user's punch record, and there is no record of it in the host, you should be able to see if it actually happened by checking the interaction records through the CLI.

❗ ***As with all telnet operations, the CLI is a place where care must be taken when entering commands.***

Logging in and out

❗ ***Be sure to exit this client properly at all times. If you do not exit properly, it will still be running when you leave telnet, and you will not be able to get into it again without rebooting the terminal.***

Starting the CLI

1. cd to RecogSys/Src/Python/RSITerm
2. Type `python RSICLIClient.pyc` and press Enter. The login prompt will appear.
3. At the prompt, enter `Schlage538` (this is the default CLI password). The CLI prompt will then display.

Exiting the CLI

Type `close` at the prompt. Wait to be returned to the telnet prompt.

Viewing Help

The CLI comes with contextual help, which you can view by entering `h` at the prompt.

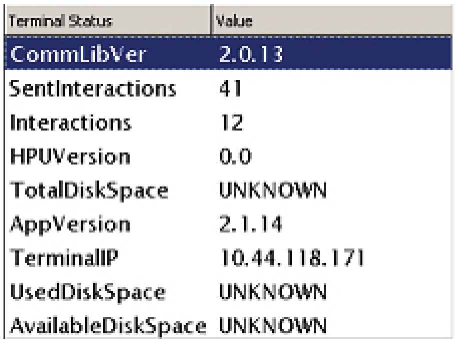
Saving the Output to a Text File On Your Computer

You can save output from the CLI session the same way you would save output from the telnet session; in fact, using the CLI is part of the same telnet session, so you need only enable logging for the telnet session and all CLI output will be saved there.

Retrieving Sent/Unsent Interactions From Terminal

When a host terminal connection is present, all interactions performed at terminal will be pushed to host and saved in host database. If host terminal connection is not present, interactions generated in terminal will be saved in the terminal and pushed to host whenever host terminal connection is resumed.

Figure 8-3 Terminal Status view that shows Sent/Unsent Interactions



Terminal Status	Value
CommLibVer	2.0.13
SentInteractions	41
Interactions	12
HPUVersion	0.0
TotalDiskSpace	UNKNOWN
AppVersion	2.1.14
TerminalIP	10.44.118.171
UsedDiskSpace	UNKNOWN
AvailableDiskSpace	UNKNOWN

In most cases, terminal interactions will make their way to host and be saved in host database. In case for some reason you are not able to retrieve interactions from host, you can retrieve them from terminal using the RSICLIClient.

To retrieve sent and/or unsent interactions from terminal, you can start an RSICLIClient by using the following steps:

1. Open a telnet session to terminal.

   ➡ ***See "Logging In and Out of Telnet" on page 126 for more information.***

2. Change the working directory to `/RecogSys/Src/Python/RSITerm`
3. Start the RSICLIClient by typing the following command at the prompt:
   ```
   Python RSICLIClient.pyc 127.0.0.1 8090
   ```
4. When prompted for password, enter Schlage538 (the default password).
5. You will see the `Ready >` prompt if you successfully started the CLI Client.
6. At the ready prompt, enter the following to list the sent interactions in the terminal, in XML format:
   ```
   Ready >sia
   ```
7. At the ready prompt, enter the following command to list the unsent interactions in the terminal, in XML format:
   ```
   Ready >ia
   ```
8. Save the output from executing steps 6 and 7 into a file and write an XML parser to parse the interactions and retrieve the information as necessary.

Troubleshooting Summary

The most common steps used to troubleshoot a terminal are:

- Using Telnet (to view the terminal's log file and check processes).
- Reviewing Terminal Status (either through the command menus or the terminal's web server)
- Using the CLI (to view specific database information records on the terminal)

Lastly, keep in mind that rebooting the terminal is a perfectly acceptable way of troubleshooting a problem. Just be sure to do it through the terminal command menus, or telnet - *do not power cycle the terminal to reboot the terminal*. Also, keep in mind that rebooting may only offer a temporary solution; if the problem continues to arise, accessing at the log file and trying to understand what the terminal is doing at the time of failure will be critical in resolving the problem.

INDEX

Ingersoll Rand
Security Technologies

Ingersoll Rand's Security Technologies Sector is a leading global provider of products and services that make environments safe, secure and productive. The Sector's market-leading products include electronic and biometric access control systems; time and attendance and personnel scheduling systems; mechanical locks and portable security, door closers and exit devices, steel doors and frames, architectural hardware and technologies and services for global security markets.

www.securitytechnologies.ingersollrand.com

SCHLAGE

GT-Series

Terminal User's Guide

Ingersoll Rand

Contents

Introduction

The Least You Should Know

before installing and setting up the terminal, you should read and understand ***Important Information for Installers and Terminal Administrators*** on page 5

Using the GT-Series Terminal

The GT-Series Terminal is the first member of the Schlage G-Series biometric hand geometry time and attendance terminals. The GT-Series Terminal records and stores the three dimensional shape of the human hand for comparison and identity verification. Upon verification, the terminal records the time, date, user ID number, and collected time and attendance data and makes this information available for collection by a host computer. The terminal can produce an output to operate an auxiliary device, such as an electronic door lock or signal bell, and can communicate with a host computer. The terminal also has auxiliary inputs that can be used to control other systems.

A third-party/custom host application communicates with GT-Series Terminals across a TCP/IP network, maintaining and storing data collected by the terminals, analyzing and updating data, maintaining security, and initiating alarms as necessary. Access to this data is achieved through a web browser or custom application. The GT-Series Terminal provides employee identification verification and includes the sophisticated operating features one expects in a time and attendance terminal. Because of this unique combination of capabilities, the GT-Series Terminal provides the most accurate and flexible time and attendance data collection terminal available.

Biometrics

Schlage offers hand geometry terminals, one of the most widely used biometric technologies, for time and attendance applications. Hand geometry technology uses the size and shape of the person's hand to verify the user's identity. Schlage biometric solutions also offer multi-authentication options. Smart card, proximity and magnetic stripe readers can be integrated into the terminals to provide an extra layer of security customized to the application requirements. Some of the world's largest providers of time and attendance systems recommend Schlage's HandPunch terminals as part of their total solution. By using biometric technology, corporations reduce payroll costs and eliminate "buddypunching" fraud.

Principles of Operation

The GT-400 terminal uses low-level infrared light, optics and a CMOS (IC chip) camera to capture a threedimensional image of the hand. Using advanced microprocessor technology, the terminal converts the image to an encrypted electronic template. It stores the template in a database with the user's ID number. To gain access, the user enters his or her ID number using the terminal keypad or uses an optional, built-in card reader. The terminal prompts the user to place his or her hand on the terminal's platen. The terminal compares the hand on the platen with the user's unique template. If the templates match, the terminal records the transaction for processing.

Database Synchronization

Synchronization, when used in this guide, refers to the process by which the database is updated on both the terminal and the host application. Synchronization only occurs on networked terminals. When synchronization occurs, the terminal and the host application compare their databases and make sure they both have the most current data. Every synchronization results in the host and terminal databases being identical.

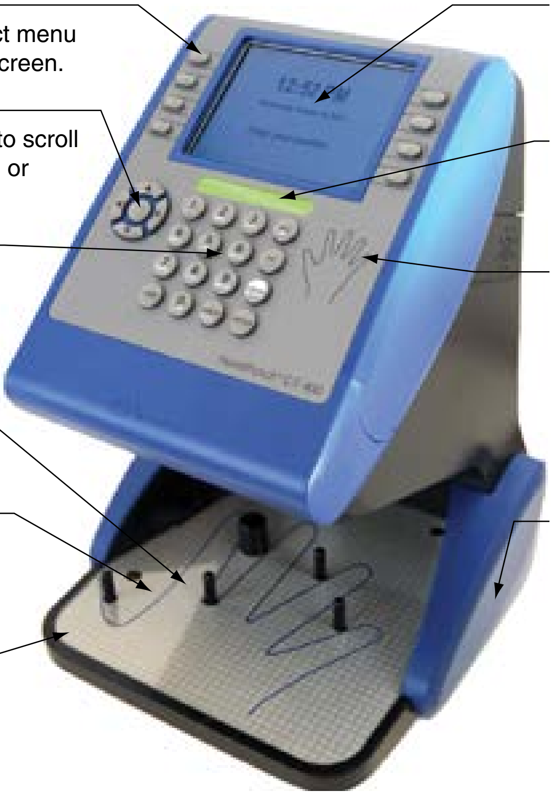
Command Menus

Command menus are the menus in the terminal that are used to configure the terminal. The command menus can be accessed by pressing ESC ← ESC and then ENTER ENTER from the ready screen. If the terminal is a new terminal and has no users, the command menus will immediately appear. After the administrator has been created and enrolled, verification will be required to access the command menus.

Verification

Verification refers to the process of placing the hand on the terminal platen as a part of the authentication process. Authentication consists of entering a user identification number on the terminal's alpha-numeric keypad and verification of the hand.

Features



Function Keys
Function keys are used to select menu options displayed on the LCD screen.

Navigation Keypad
The navigation keypad is used to scroll through lists or to move forward or backward in text fields.

Alpha-Numeric Keypad
The alpha-numeric keypad is used to enter text or numbers into the terminal.

Finger Pins
Finger pins are used to position the hand on the terminal platen.

Hand Placement Outline
The hand placement outline is a visual guide for hand placement on the terminal platen.

Platen
The platen is the surface upon which the hand is placed for verificaton.

LCD Screen
The LCD screen shows menus and messages on the terminal.

LED Bar
The LED bar gives a visual indication of terminal status.

Hand Placement Guide
The hand placement guide gives a visual indication of hand placement on the platen. Red LED indicators light when fingers are not in the correct position in relation to the finger pins.

Side Cover
The side covers are removable to access screw holes for mounting the terminal to the wall plate.

Specifications

Size:	8 inches (20.32 cm) wide by 11.18 inches (28.40 cm) high by 7.52 inches (19.10 cm) deep
Weight:	5.60 lbs (2.54 kg) – 6.90 lbs (3.13 kg) with optional backup
Power:	12 VDC nominal (10.8 to 13.5 VDC), 4.5 Watts max. Linear power supply recommended
Transient Protection:	8,000 volts – all terminals
Reverse Voltage:	On power input
Environment:	Operating: 32°F to 113°F (0°C to 45°C) Relative humidity: 5% to 95%, non-condensing non-operating (storage): -40°F to 185°F (-40°C to 85°C)
Verification Time:	Less than one second
Date Retention:	3 years using a standard internal lithium battery
Transaction Buffer:	Memory card-dependant
Baud Rate:	9600 to 115200 bps
Communications:	TCP/IP over ethernet – 10/100 Base T
Function Keys:	8 programmable soft keys
Alarm Monitoring:	Unit tamper
Relay Output:	1 – 250 VAC @ 10A
Battery Backup (optional):	2 hour minimum run time

Table 3.1: Terminal Specifications

Using the GT Series Terminal Keypad

Types of Keys

There are three types of keys used to make entries into the terminal. Each will be indicated in this guide as shown below.

Type of Key	Location and Purpose	Symbol
Function Key	These keys are located on both sides of the terminal screen. They are used to navigate through the command menus.	⬭
Alpha-Numeric Key	These keys are located in the terminal keypad. They are used to enter letters and numbers into the terminal.	1 .-+
Navigation Pad	These keys are located to the left of the terminal keypad. They are used to navigate through lists displayed on the terminal screen. The middle key can be used as an "Enter" or "Select" key.	▲◀○▶▼

Table 3.2: Types of Terminal Keys and Corresponding Symbols

Important Information for Installers and Terminal Administrators

➔ *Field installers and terminal administrators should read this section thoroughly before attempting to install or configure a GT-Series Terminal site. It explains important concepts and lists required administrative terminal operations.*

Network Setup and Ethernet Switches

For best performance, it is recommended that you use ethernet switches to connect the terminal(s) to the host, rather than ethernet hubs. Using ethernet hubs to connect the terminal(s) to the host may lead to terminal instability. If instability is encountered while using ethernet hubs, you may need to reboot the terminal(s).

Power-on and Shutdown Precautions

- If your terminal is equipped with a backup battery, it should be connected after power has been applied to the terminal.

➔ *See **Making Back Board Connections** on page 13 for more information.*

- The network (ethernet) cable must be connected to the terminal before applying power. The terminal establishes itself on the network during start-up. You will not be able to communicate with the terminal if the cable is not connected before applying power. Other connections, including optional USB, or serial or auxiliary relay connections, should also be made before applying power.

  ! ***The terminal must not be disconnected from its power source without shutting down the application first.***

Terminal Placement

The recommended height for the terminal's platen is between 40 and 48 inches (102 - 122 cm) from the finished floor. This height conforms to the Americans with Disabilities Act (ADA) standards (40 inches is recommended for ADA standards). All terminals within a site should be placed at the same height.

The terminal should be out of the path of pedestrian and vehicular traffic.

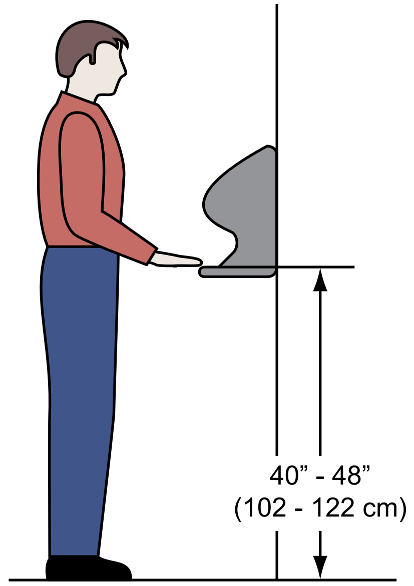


Figure 5.1: Terminal Installation Height

Make sure that the terminal is not exposed to excessive airborne dust, direct sunlight, water, or chemicals.

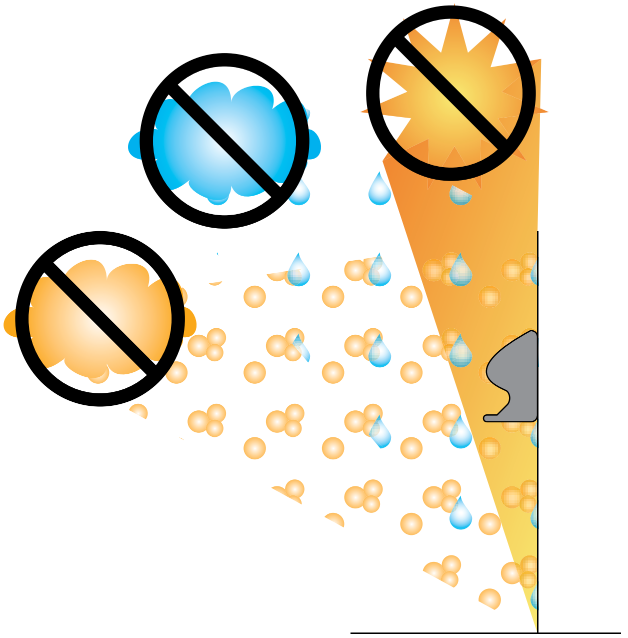


Figure 5.2: Terminal Installation Location

Removing the Terminal from the Box

1. Remove any accessories from the box.
2. Remove the packing materials from the top of the terminal.
3. Lift the terminal from the box. Do not touch the underside of the terminal face.

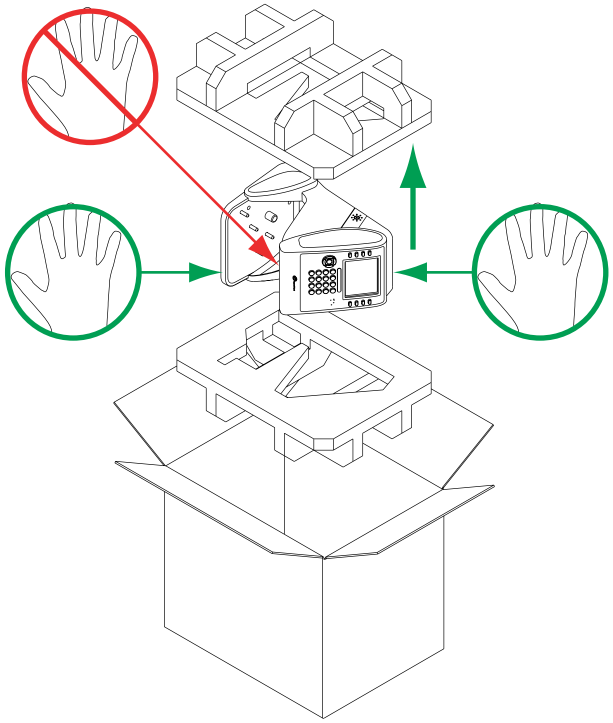


Figure 5.3: Removing the Terminal from the Box

Wall Preparation

❗ ***These directions and provided hardware are for installation on a hollow wall only. For installation on a solid wall, other means should be used.***

1. Measure and mark a point 49 inches (124.5 cm) from the surface of the finished floor.

   ➔ *This point is used by the leveling hole where the top-center point of the terminal should be mounted. At 49 inches, the unit's platen will be 40 inches from the floor.*

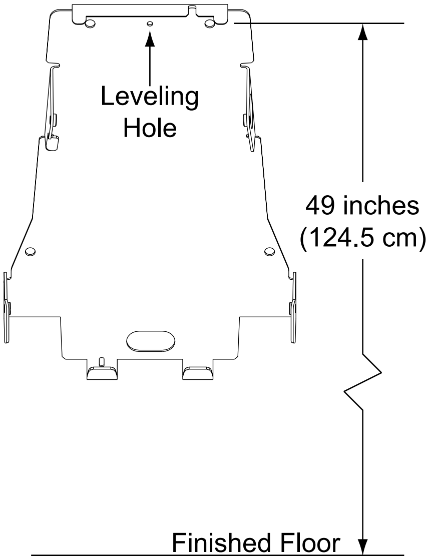


Figure 5.4: Measurements for Terminal Installation

2. Drive a small nail into the wall at the mark.

   ➔ *For a solid wall, pre-drill a ⅛" hole. Insert nail into the hole.*

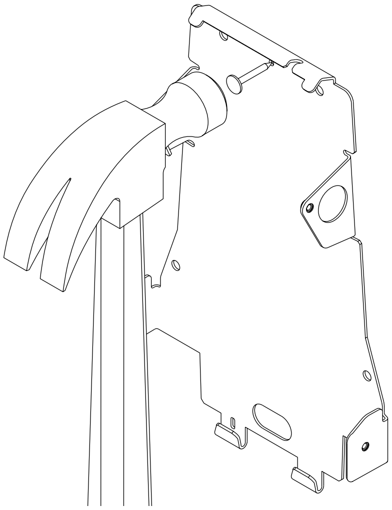


Figure 5.5: Leveling the Terminal, Step 2

3. Hang the wall plate from the leveling hole located near the top of the wall plate.
4. Use a bubble level to ensure that the wall plate is level.

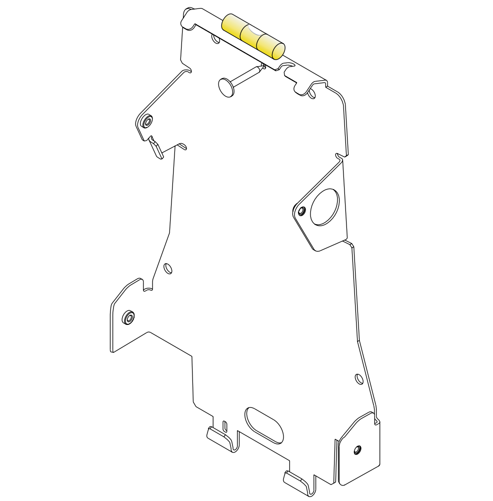


Figure 5.6: Leveling the Terminal, Step 4

5. Mark the locations of the two upper mounting holes and the two lower mounting holes.

   ➔ *For a concealed wiring connection through the wall, mark the rear cable entry hole on the wall plate.*

6. Remove the wall plate and nail.

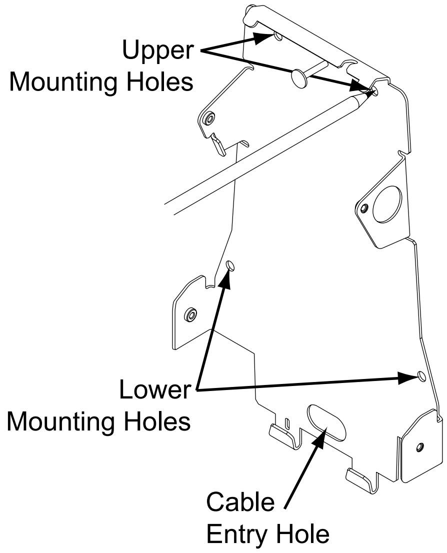


Figure 5.7: Leveling the Terminal, Step 5

7. Drill upper and lower mounting holes.
   - ➔ *For a concealed wiring connection, drill a ½” hole in the center of the outlined rear cable entry hole.*
   - ➔ *Additional holes may be drilled to enlarge hole for concealed wiring connection if necessary.*
8. Clear all dust and debris away from the

   terminal mounting location.

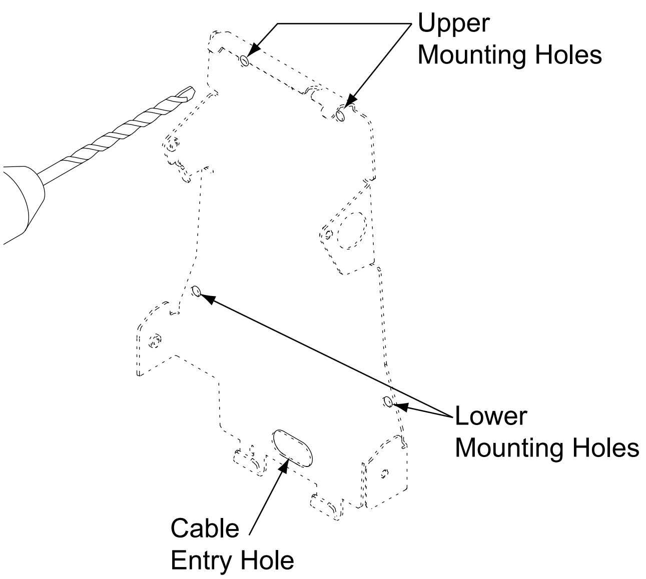


Figure 5.8: Drill Holes

Attaching the Wall Plate

These directions and provided hardware are for installation on a hollow wall only. For installation on a solid wall, other means should be used.

1. Pull all wires through holes in wall (if necessary) and make sure wires are clear of wall plate.
2. Install the four provided fasteners into the mounting hole locations. Then use the four provided screws to attach the plate to the wall.

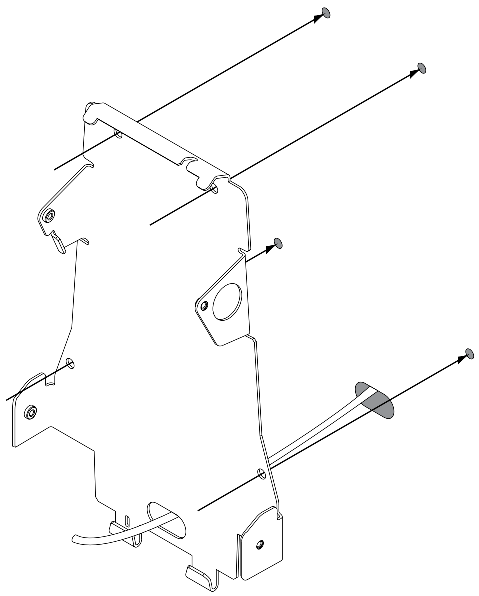


Figure 5.9: Attaching the Wall Plate

Hanging Terminal and Running Wires

1. If the side covers are attached to the terminal, they must be removed before hanging the terminal on the wall plate.

   ➔ *See **Removing Side Covers** on page 15 for more information*

2. Slide slots in terminal over hooks on wall plate. Allow terminal to rest against the wall while performing the following steps.

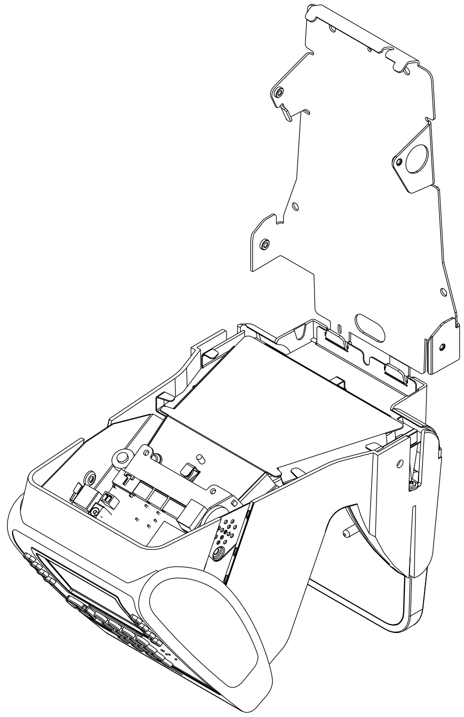


Figure 5.10: Hang the Terminal from the Wall Plate

3. There are several options for running the wiring to the terminal.

   a. Run wiring through hole in wall plate.

   b. Run wiring through slot in terminal.

   c. Run wiring through battery cover (material removal required).

   ➔ *If using option c, locate indentation in battery cover, drill ¼” hole in battery cover indentation and use utility knife to remove excess material.*

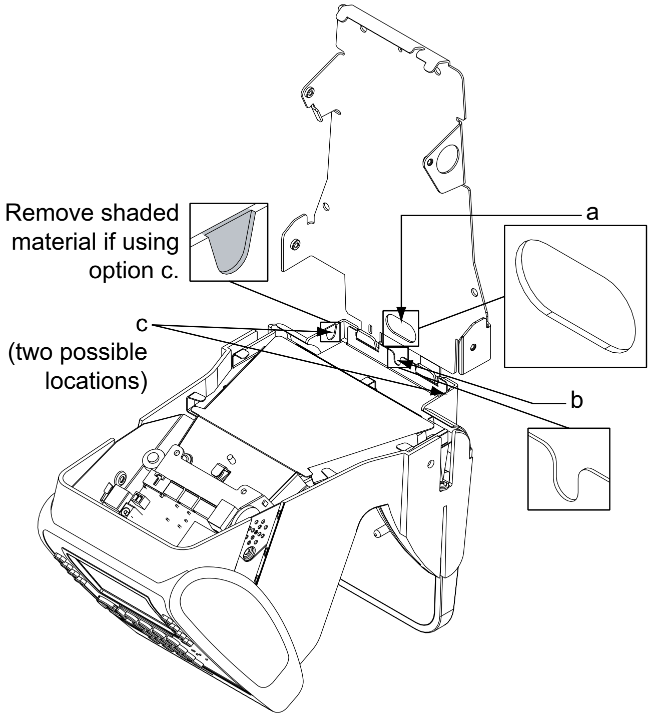


Figure 5.11: Terminal Wiring Options

4. Tuck wires under tabs on terminal to minimize risk of crimping wires.
5. Follow all local electrical codes when routing wire and making the terminal connections.
   - ➔ *For concealed wiring, pull the terminal wiring through the ½" cable entry hole.*
   - ➔ *Ensure there is at least twelve inches of extra cable beyond what is needed to make the required connections to the back board.*
   - ➔ *For conduit wiring, pull an extra twelve inches of cable through the conduit beyond what is needed to make the required connections to the back board.*
   - ➔ *You may need to run the cable and then attach the connectors in order to fit cables through necessary holes and/or slots.*

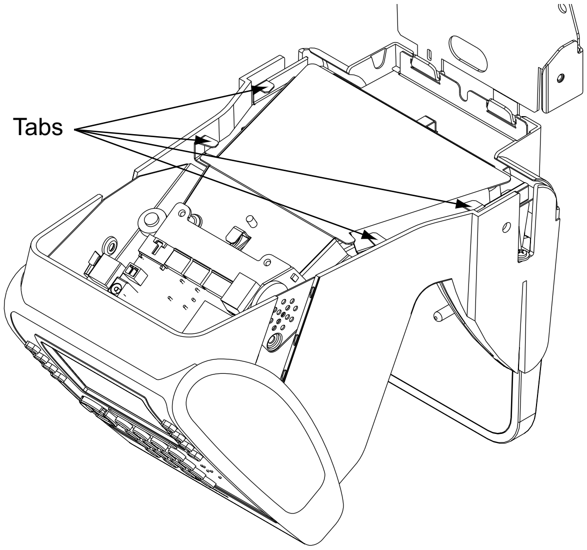


Figure 5.12: Wire Tabs

Making Back Board Connections

Use caution when making connections to the back board to avoid damage. Be aware of possible damage due to electrostatic discharge (ESD). ESD is of particular concern when working on carpeted surfaces and in dry environments. Use a ground strap to minimize ESD concerns.

DO NOT apply power until you are ready to configure the terminal!

DO NOT connect backup battery (if using) until after main power has been supplied!

1. Connect the earth ground. The earth ground connection is made to the ground pin on the terminal. Bundle all ground connections into one crimp lug and attach the lug to the ground pin with a 8-32 nut.
2. Connect the ethernet cable to the ethernet connection socket inside the terminal casing.
3. DO NOT apply power until you are ready to configure the terminal. Connect the P1 plug to the twisted pair per the following: Pin 1: Ground, Pin 2: Power.

   ➔ *See **Important Information for Installers and Terminal Administrators** on page 5 for more information.*

4. If using the optional backup battery, locate the backup battery relay, but DO NOT connect backup battery until after the main power has been connected.
5. Make other back board connections as necessary. Use the diagram below as a reference.

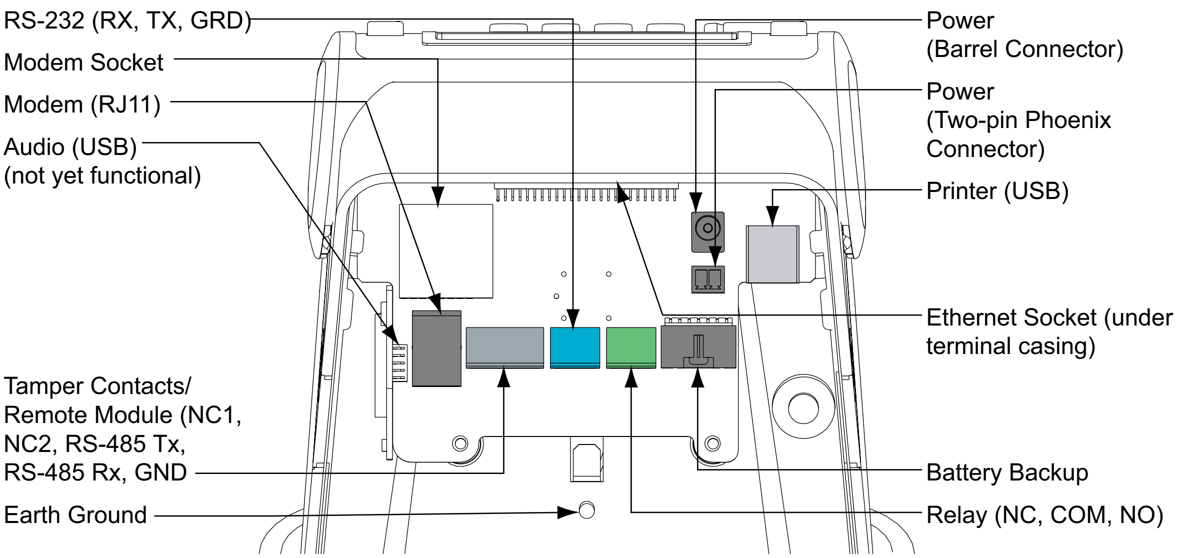


Figure 5.13: Back Board Connections

Attaching the Ferrite Clip

The ferrite clip must be attached to the terminal's power cord in order to be FCC compliant.

1. Make a loop in the power cord approximately six (6) inches from the power supply.
   The loop will keep the clip from sliding on the power cord.
2. Clamp the ferrite clip over the loop. Make sure the tabs fully engage.

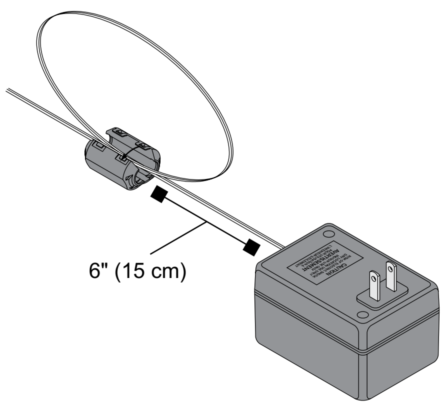


Figure 5.14: Attaching the Ferrite Clip

Configuring the Terminal

❗ ***You must configure the terminal before completing installation***

Go to

Removing and Installing Side Covers

The side covers must be removed in order to attach the terminal to the wall plate.

The terminal may be shipped without the side covers attached.

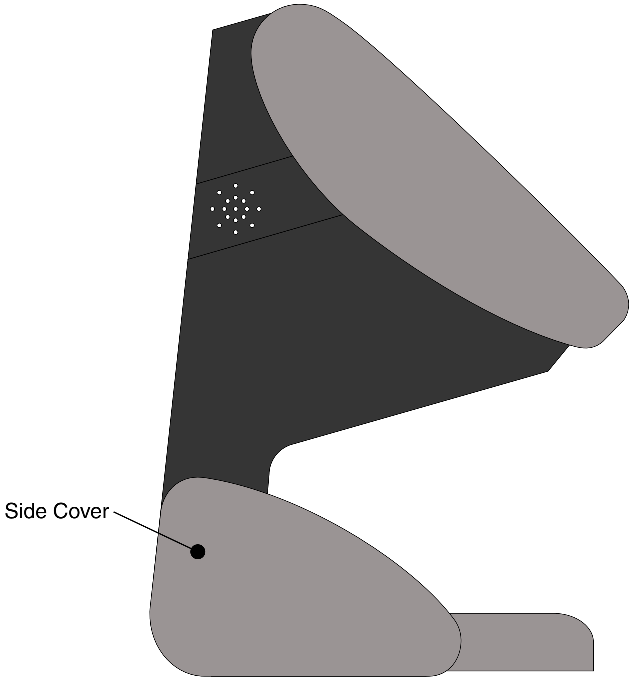


Figure 5.15: Terminal Covers

Removing Side Covers

1. Locate slot on bottom of side cover. Insert a small screwdriver into slot.
2. Rotate screwdriver gently. Side cover will pop off.

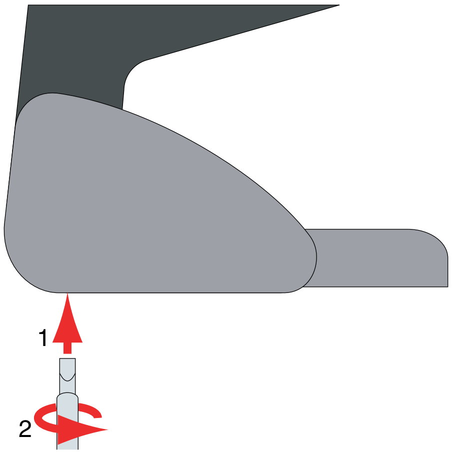


Figure 5.16: Removing the Side Covers

Installing Side Covers

1. Place outside ridge of side cover under edge of terminal body.
2. Rotate side cover toward terminal body and snap into place.

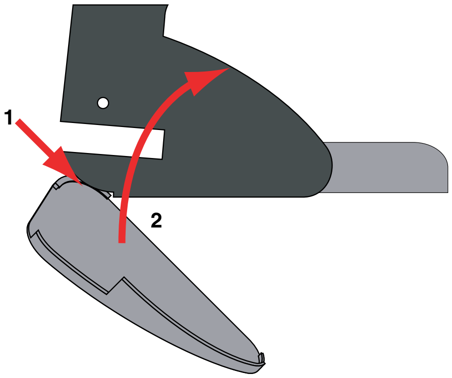


Figure 5.17: Installing the Side Covers

Attaching the Terminal to the Wall Plate

Remove any dust and debris from the mounting site before attaching the terminal. Dust and debris can seriously affect the performance of the terminal.

1. Choose the standard Phillips head screws or the security head screws for installation.

➔ *A special tool is required to install and remove a security head screw*

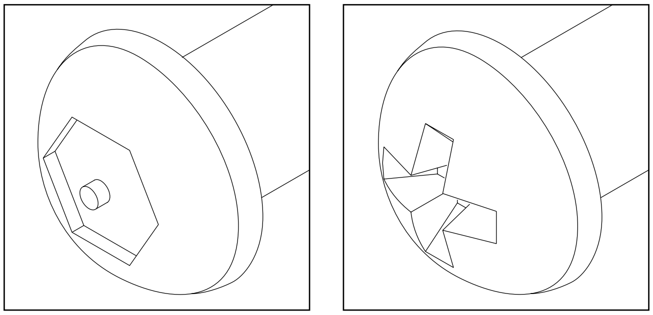


Figure 5.18: Installation Screw Choices

2. Terminal should already be hanging from wall plate.
3. Rotate terminal toward the wall plate. Make sure not to pinch or damage any wiring.
4. Make sure that the screw holes in the body of the terminal are aligned with the screw holes in the wall plate.
5. Install two (2) screws into the lower screw holes.
6. Attach side caps.

   ➔ *See **Installing Side Covers on page 15** for more information.*

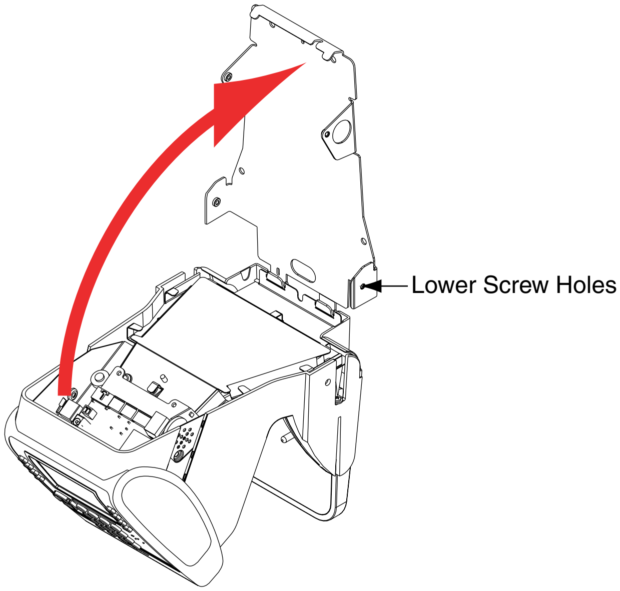


Figure 5.19: Rotate Terminal Towards Wall Plate

Index

Ingersoll Rand
Security Technologies

Ingersoll Rand's Security Technologies Sector is a leading global provider of products and services that make environments safe, secure and productive. The Sector's market-leading products include electronic and biometric access control systems; time and attendance and personnel scheduling systems; mechanical locks and portable security, door closers and exit devices, steel doors and frames, architectural hardware and technologies and services for global security markets.

1-877-671-7011 www.schlage.com www.ingersollrand.com