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

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.*

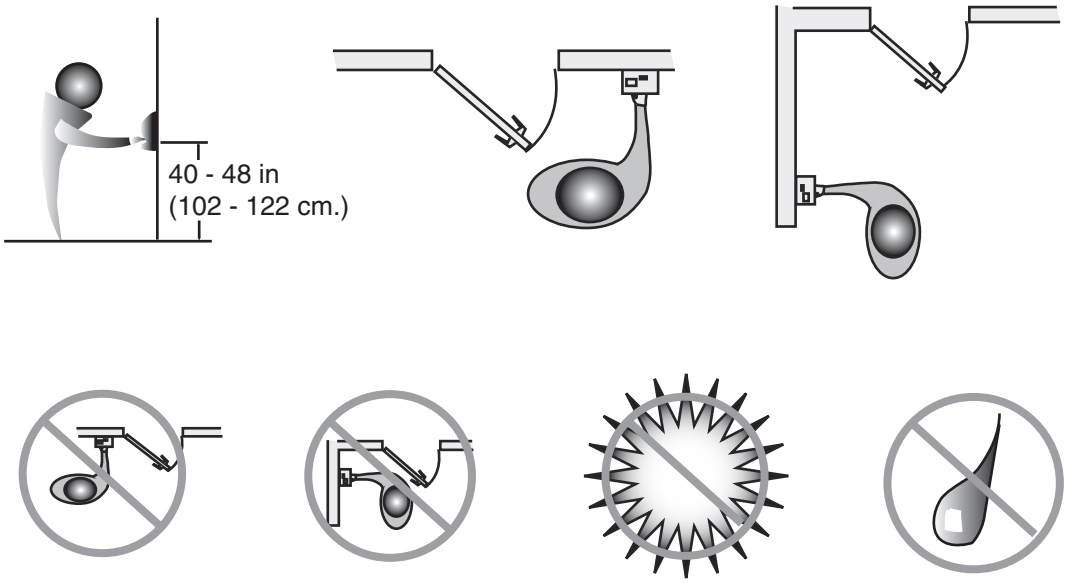


Figure 3-1: Reader Placement Rules

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.

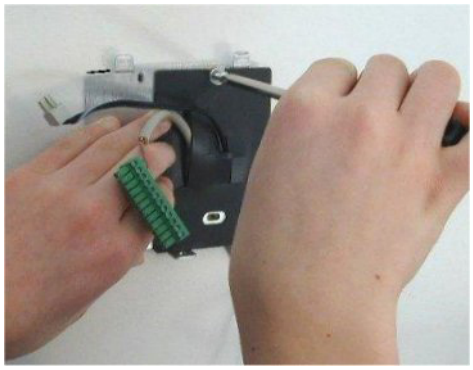
Mount All Readers at the Same Height

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.

   - 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

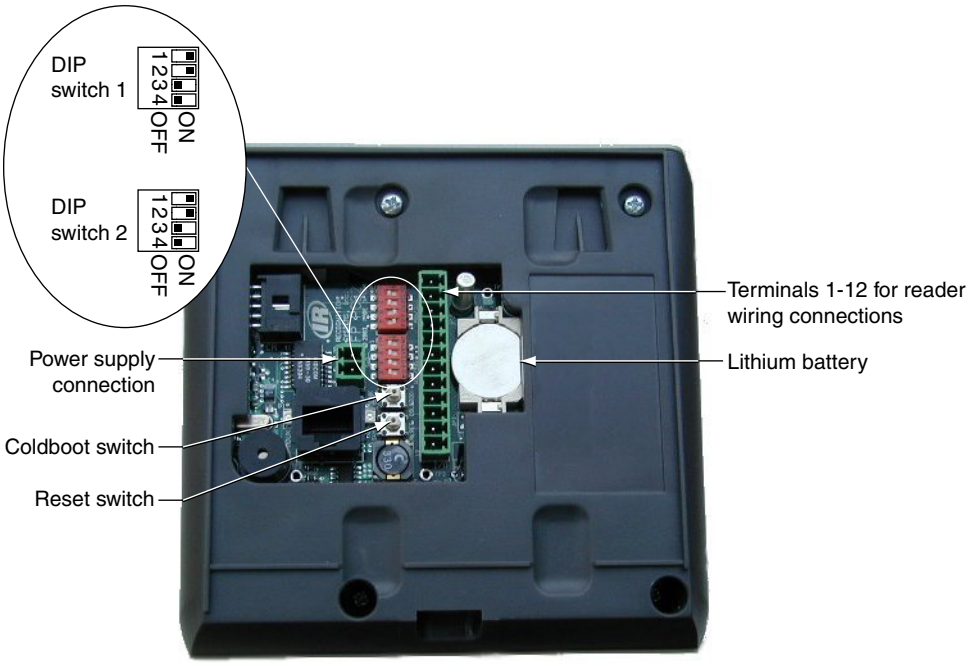
Schlage Biometrics is not responsible for readers damaged by improper wiring.

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

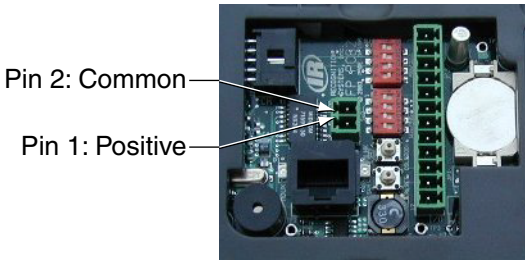
Terminal	Connection	Notes
1	Card Reader: Wiegand D0 or Magnetic Stripe Data Input	Use these terminals to connect to an external card reader to supply user IDs instead of having users enter their IDs using the reader keypad. (These terminals aren't needed if your reader has a built-in card-reader.)
2	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.

   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.

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

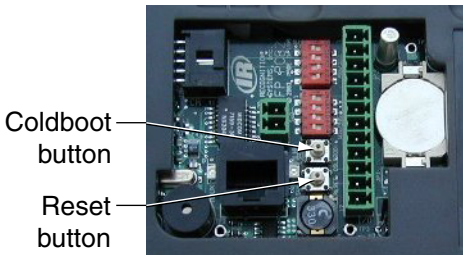
- If you've changed network related settings (address, master/remote status, etc.) through the reader menus: The reader automatically resets itself when you leave the menus. You'll see a message that tells you that the reader is resetting if this is needed.
- If you've changed DIP switches: You must 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

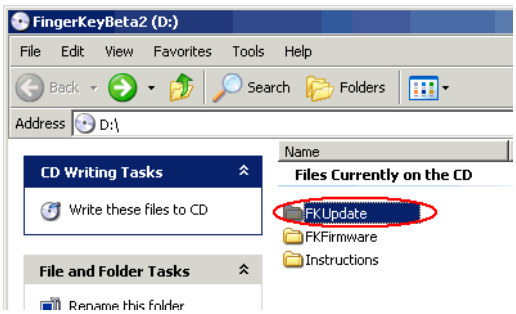
If you don't have the .NET Framework, you must install it.

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.

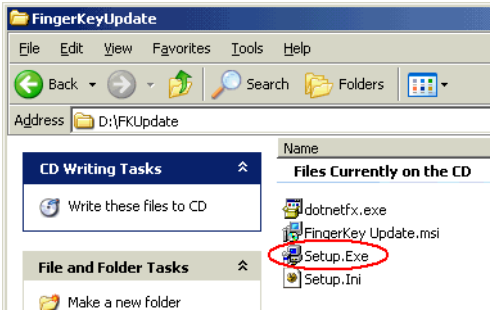
Once the .NET Framework is installed, you are ready to install the FingerKey Update Utility.

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.

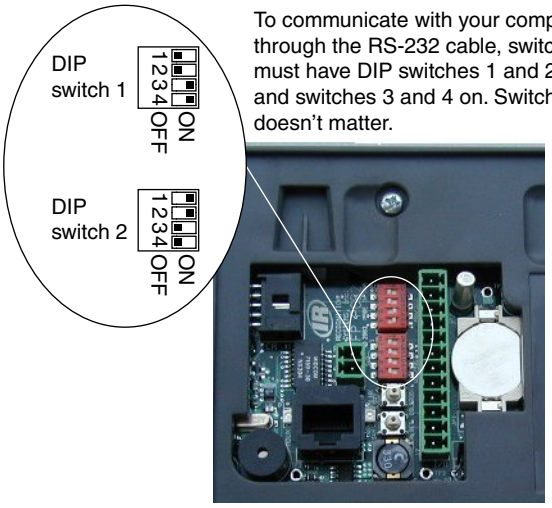
Upgrading the FingerKey or Sensor Firmware

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.

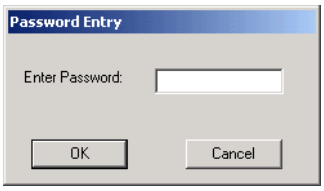
Establishing Communication Between the Reader and the Update Utility

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.



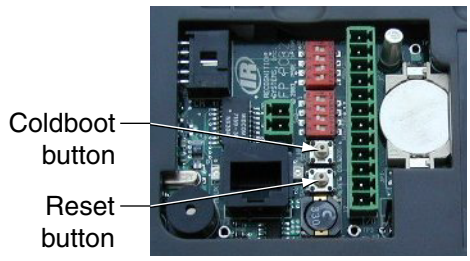
To communicate with your computer through the RS-232 cable, switch 1 must have DIP switches 1 and 2 off, and switches 3 and 4 on. Switch 2 doesn't matter.

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.



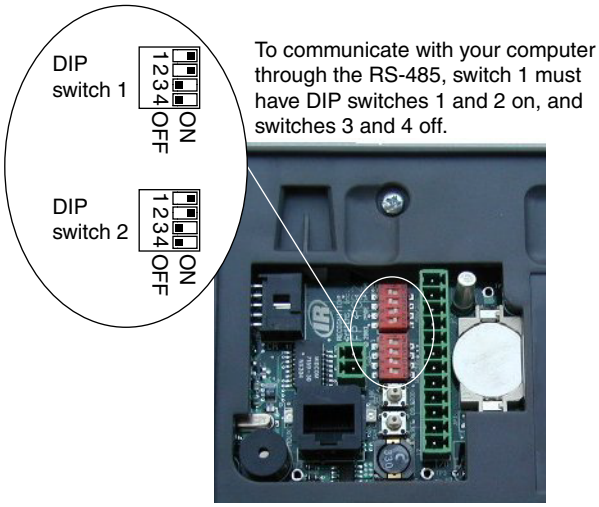
10. Confirm that the reader and update utility are communicating by looking at Bootloader Version, Firmware Version, and Program Checksum displayed in the lower-left corner of the utility.

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.



- 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:

   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:

   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.

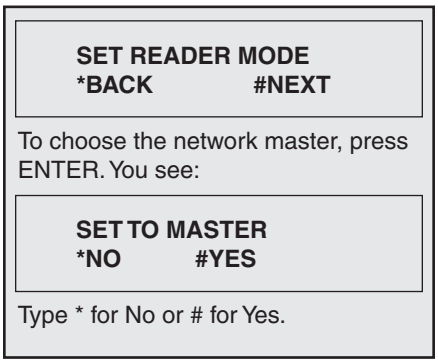
The commands are in the order listed above. To get to any command after you get to the menu, keep pressing # (Next) until you get to the command you want.

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.

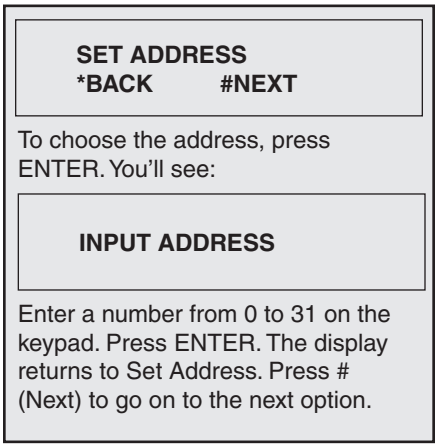


Setting the Reader's Address

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.



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

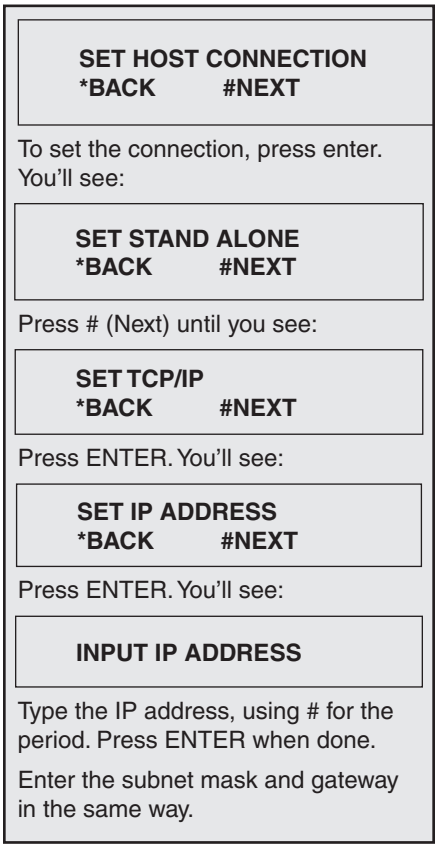
If the reader is connected to the host computer through a TCP/IP (Ethernet) connection, then you must first upgrade your reader using the Ethernet Upgrade option; see page 42.

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.



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.

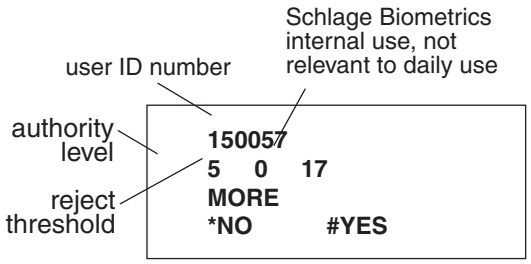
Getting to This Menu

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:



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.

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.

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.

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 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).

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.

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..... .....XXXXXXXXXXXXXXA
	3	WC03=34BIT:16BIT ID	Facility code: 16 bits, bit 2-17 ID: 16 bits, bit 18-33 1 2 3 12345678901234567890123456789012345 PFFFFFFFFFFFFFFFIIIIIIIIIIIIIIIIP EXXXXXXXXXXXXXXX..... .....XXXXXXXXXXXXXXXA
	4	WC04=26BIT:20BIT ID	Facility code: 12 bits, bit 2-13 ID: 20 bits, bit 14-33 1 2 3 12345678901234567890123456789012345 PFFFFFFFFFFFFIIIIIIIIIIIIIIIIIIIP EXXXXXXXXXXXXXXX..... .....XXXXXXXXXXXXXXXO
	5	WC05=34BIT:32BIT ID	ID: 32 bits, bit 2-33 1 2 3 12345678901234567890123456789012345 PIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIP EXXXXXXXXXXXXXXX..... .....XXXXXXXXXXXXXXXO
	6	WC06=35BIT:20BIT ID	Facility code: 12 bits, bit 3-14 ID: 20 bits, bit 15-34 1 2 3 12345678901234567890123546789012345 PPFFFFFFFFFFFFIIIIIIIIIIIIIIIIIIIP .EXX.XX.XX.XX.XX.XX.XX.XX.XX.XX. .XX.XX.XX.XX.XX.XX.XX.XX.XX.XX.O OXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
	7	WC07=37BIT:19BIT ID	Facility code: 16 bits, bit 2-17 ID: 19 bits, bit 18-36 1 2 3 123456789012345678901234567890123456789 PFFFFFFFFFFFFFFFIIIIIIIIIIIIIIIIIIIP EXXXXXXXXXXXXXXXXXX..... .....XXXXXXXXXXXXXXXXXO
	8	WC08=37BIT:35BIT ID	ID: 35 bits, bit 2-36 1 2 3 123456789012345678901234567890123456789 PIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIP EXXXXXXXXXXXXXXXXXX..... .....XXXXXXXXXXXXXXXXXO

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.

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.

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.

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.

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.

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.

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.

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.

You won't generally need to use this option if you set the reader to automatically update cards.

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

Symbols

A

B

C

D

E

F

H

I

L

M

N

O

P

R

S

T

U

W

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 70100-6200 Rev. 3.1 06/09