ALLEGION

SCHLAGE

HandNet-Lite

Terminal User's Guide

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and, if not installed and used in accordance with the Installation Manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at the user's own expense.

This Class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numerique de la classe A respecte toutes les exigences du Reglemente sure le materiel brouilleur du Canada.

Document Part Number: 70100-6210 – Revision 3.1 – 09/14

Contents

Getting Started

Introduction

What HandNet Lite Does

HandNet Lite lets you control and monitor many connected FingerKey and/or HandKey readers. In this one program, you can control who can use each reader and when. You can also monitor activity and alarms for all readers at once.

Figure 3.1: Starting HandNet Lite

HandNet Lite System Requirements

Operating Systems:

- Windows XP SP3
- Windows Vista
- Windows Server 2003 SP1 or greater
- Windows 2000 Professional or Server Editions SP4
- Windows 95 & 98
- Windows 7 32bit & 64bit
- Windows 8 32 bit & 64bit.

Screen Resolution: Screen resolution must be set to at least 1024 x 768; the HandNet Lite window won't fit on your screen if you use a lower resolution. The actual screen size is 1020 x 720, so if your screen resolution is 1024 x 768, your task bar must be on the top or bottom of the screen, and the task bar must be no more than two lines high; if the task bar is three lines or higher or if it is on the side of your screen, part of the HandNet Lite window will run off the screen.

Starting HandNet Lite

To start HandNet Lite, either double-click the HandNet Lite icon on your Windows desktop or click the Start menu on your Windows taskbar, highlight Programs, highlight Schlage Biometrics, highlight the HandNet Lite folder, and click HandNet Lite. The main window opens.

Logging into HandNet Lite

HandNet Lite requires you to log in before you can make any changes; this prevents unauthorized people from changing information. If you aren't logged in, you can look at the current status of readers and get on-line help, but you can't change any information or use any other options.

1. **Click Login on the Main window. See Figure 3.2: Logging into HandNet Lite.**
2. **Type your Login name and Password and click Accept.**

Figure 3.2: Logging into HandNet Lite

If this is a new system: Use a Login name of "1234" and a Password of "new." (After logging in for the first time, you should add one or more new operators. See **Managing Operators** on page **20** for more information.)

After initial setup: If you forget your Login name or Password, see your supervisor or security administrator.

The login name and password are case sensitive. For example, the passwords new, New, and NEW are all different.

After you are done using HandNet Lite, log out so unauthorized people won't be able to use the program.

Select Language

After HandNet-lite version 2.3 is installed, the first time it is run the following screen will be presented so that the displayed language can be selected. If you do not see the special characters on your computer, use Control Panel, Regional and Language Settings, Advanced tab and select the desired character sets.

This is the “Select Language” screen. Current language choices are English, French, Dutch, Simplified Chinese, Traditional Chinese, and Bahasa Indonesian.

Figure 3.3: Select Language

Getting Help in HandNet Lite

The on-line help has the same information as this manual. To get help in HandNet Lite, click the Help button. Use the contents, index, or search tabs at the left of the help window to find any topic.

For Basic Topics

Click the Contents tab at the top of the left pane, click a book to open, and then click a topic. Not every topic is in the Contents though, so if you don’t find what you need, try the Index or Search tabs.

For Groups of Topics on a Single Theme

In addition to the contents you can also click on the pull-down list right under the Previous/Next buttons (in the bottom middle of the header). This list contains a number of important groups of topics. Once you are on one of these topics, the Next and Previous buttons work as well.

Marking a Topic to Return To

In the on-line help, to mark a topic that you want to come back to:

1. Go to the topic that you want to mark.
2. Click the Favorites tab at the top of the left pane.
3. Click the Add button at the bottom of the pane. This adds the topic to your favorites list.

To get back to any marked topic later:

1. Click the Favorites tab at the top of the left pane of the help window.
2. Double-click the topic.

Main HandNet Lite Window

After you log into HandNet Lite, a number of additional tabs appear that let you get to the different parts of the program. Which tabs you see depends on which operator login you used. The screen below shows all of the options.

Figure 3.4: Main HandNet Lite Window

What You Can Do On Each Tab

Each of the tabs are explained in further detail later in the following chapters.

Status: The Status tab lists every reader in HandNet Lite and the network (group of readers) the reader is connected to. It gives information about each reader and the state of its connection. See **Status Tab** on page **5** for more information.

Users: The Users tab lists every user that has been added to HandNet Lite, including the user's name, ID, access profile (the group of readers the user has access to), authority level (which reader menus the user can program), and whether the user is enrolled. See **Users Tab** on page **7** for more information. You can add, change, or delete users through the buttons in this tab.

Log: The Log window lists significant events at any connected reader. It doesn't list user accesses, but it lists user additions and enrollment, alarm conditions, and so on. It also lists significant changes made in HandNet Lite. For each event you see the date and time, network and reader, user name and IDs, a brief description of what happened, and an icon showing the type of activity. See **Log Tab** on page **13** for more information.

Reports: The Reports tab lets you generate reports on all of your users and all of your readers. See **Reports Tab** on page **15** for more information.

Alarms: The Alarms tab shows a subset of what you see on the Log tab; this tab lists only those events that are classified as alarm conditions. These generally require immediate attention. See **Alarms Tab** on page **19** for more information.

Settings: The Settings tab lets you change HandNet Lite's login name and passwords. It also lets you choose the default Access Profile for users added at a reader, that is, which readers the user has access to. See **Settings Tab** on page **19** for more information.

Configuration: You may add, change, or delete networks and readers. The Configuration tab also allows you to create Wiegand output configurations which can be used for setting FingerKey output. See **Configuration Tab** on page **21** for more information.

Smart card: The Smart Card tab is used to manage iCLASS, DESFire and MiFare cards. See **Smart Card Tab** on page **35** for more information.

Access: The Access tab lets you define access profiles. Access profiles control which readers different groups of people have access through. See **Access Tab** on page **45** for more information.

Database: The Database Tab is used to backup, restore, delete, detach and attach the database. See **Database Tab** on page **47** for more information.

Getting Around with the Keyboard

To move from tab to tab: Press ctrl tab.

To move from entry to entry with a tab: Press tab to move to the next entry, and shift tab to move to the previous entry.

This page intentionally blank.

Status Tab

The *Status* tab lists every network and reader that has been configured in HandNet Lite. Click the heading of any row to sort the list by that heading. Click the heading again to reverse the sort order.

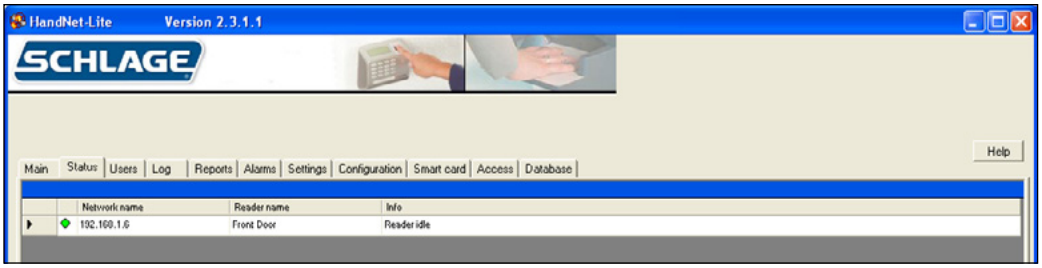


Figure 4.1: Status Tab

Table 4.1: Reader Status	
Column	**Description**
Status Indicator (untitled)	Indicates the current status of the reader
Network name	Name of the reader's network
Reader name	Name of the reader
Info	Details about the status of the reader's connection

Table 4.2: Reader Status Indicators		
Icon	**Description**	**Additional Information**
	Reader is communicating	• Click the green icon to display download and conditionally upload user choices. • If the reader is a FingerKey you will have a Download (Download from PC to the reader) choice. • If the reader is a HandKey you will have both a Download (from the PC to the reader) and Upload (from the reader to the PC) choices.
	Reader is not enabled	• Readers must be first created (see create new reader) and then enabled (see enable reader).
	Reader is not communicating.	• The reader is not configured correctly, or is disconnected. • Click the red icon for further details.

This page intentionally blank.

Users Tab

The *Users* tab lists every user and is used to add or change users. Users are individuals who are enrolled in readers. Click the heading of any row to sort the list by that heading. Click the heading again to reverse the sort order. Clicking on a user row will display actions that can be performed for that user.

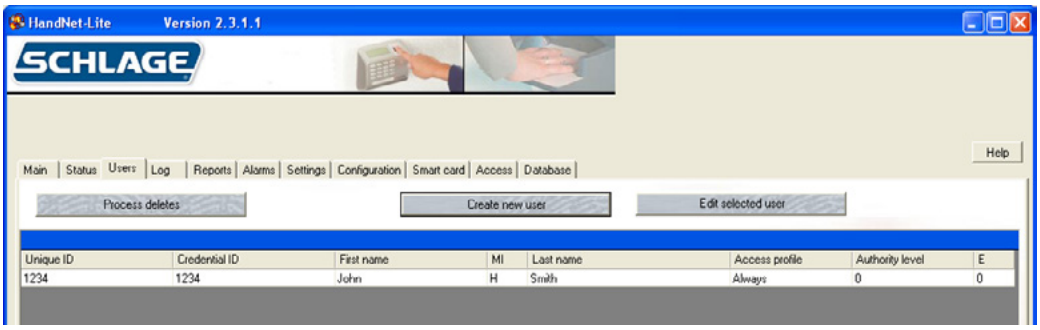


Figure 5.1: Users Tab

Table 5.1: List of Users

Column	Description
Unique ID	ID by which the user is identified in the database
Credential ID	ID the user enters at the reader in order to gain access
First Name	User's first name
MI	User's middle initial
Last Name	User's last name
Access profile	Access profile that is associated with the user. See **Add an Access Profile** on page **45** for more information.
Authority Level	Authority level for the user. Zero (0) for most users, meaning the user can gain access through the reader, but not use the command menus in the reader to change settings. See **Table 5.3: Authority Levels** on page **11** for more information.
E	Indicates enrollment status Zero (0) indicates that the user is not enrolled. One (1) indicates that a HandKey template has been captured for the user Two (2) indicates that a FingerKey template has been captured for the user Three(3) indicates that HandKey and FingerKey templates have been captured for the user.

Enroll Users

Users must be enrolled on a reader. For help enrolling users, see the reader's manual.

A user may be added to HandNet Lite in one of two ways:

- **Enroll the user at a reader before entering the user in HandNet Lite.** If the reader is connected, the user is automatically added to HandNet Lite. If users are enrolled in readers before they are connected to HandNet Lite, when the reader is initially connected to HandNet Lite, all users are imported then.

  If a user is enrolled first, the user ID in the reader (the Credential ID) is used in HandNet Lite for the user's First name, Last name, and Unique ID (an identifier used only by HandNet Lite to help distinguish users with similar names). Edit these entries by selecting the user in the Users window and clicking the Edit selected user button; see Edit Fingerprint Settings page 41.
- **Enter the user in HandNet Lite before enrolling the user in a connected reader.** Enter the user in the User edit window. See **Add a User** on page **9** for more information. The user will be listed as unenrolled in the Users window (denoted by a zero (0) in column E). See **Table 5.2: User Fields** on page **10** for more information. When you enroll the user at a reader, HandNet Lite will import the finer template.

➔ When enrolling users at the reader, you must completely leave the reader's command menus before HandNet Lite will detect the enrollments.

Problems with User Enrollment

Since bypassing finger or hand recognition gives you reduced security, it should only be used as a last resort. Try these options first:

- The user might have placed the finger or hand badly during the initial enrollment.
  1. Remove the user from the reader.
  2. Instruct the user on correct finger or hand placement. Make sure the user is placing the right finger.
  3. Add the user again. This creates a new template for the user.
- If using a FingerKey, Remove the user, and enroll the user again using different fingers. Try the thumb if other fingers don't work
- If the user has a mild disability that prevents consistent finger or hand placement, change the user's reject level. See **Biometric Threshold** on page **10** for more information. See the reader manual for instructions on how to set the appropriate reject setting for the user.

If these options aren't possible, or if you try them and they don't work, then check the Verify on ID only (no biometric verification) box on the User edit screen. See **Verify on ID only (no biometric verification)** on page **10** for more information.

Adding a Special User

When using a FingerKey, if a user's fingerprint cannot be scanned (for any reason), the user can be added as a special user. Special users are still required to place a finger on the scanner, but the scanner does not try to match a finger template.

If a user has unrecognizable fingerprints, severe arthritis, or other conditions that keep the user's finger from being recognized, you can give the user access without finger recognition. If you choose this, the reader still asks the user to place a finger on the reader so it won't be apparent to others that finger recognition isn't required, but the reader doesn't check the finger template; it gives access regardless of whose finger is placed there.

Add a User

1. Click the *Users* tab.
2. Click the *Create new user* button.
3. Complete the fields on the screen. See **Table 5.2: User Fields** on page **10** for more information.
4. Click the *Accept Settings* button.
5. If the user has not been enrolled on a reader, do so now. See **Enroll Users** on page **8** for more information.

Edit a User

1. Click the *Users* tab.
2. Click to select the name of the user you want to edit.
3. Click the *Edit selected user* button.
4. Complete the fields on the screen. See **Table 5.2: User Fields** on page **10** for more information.
5. Click the *Accept Settings* button..

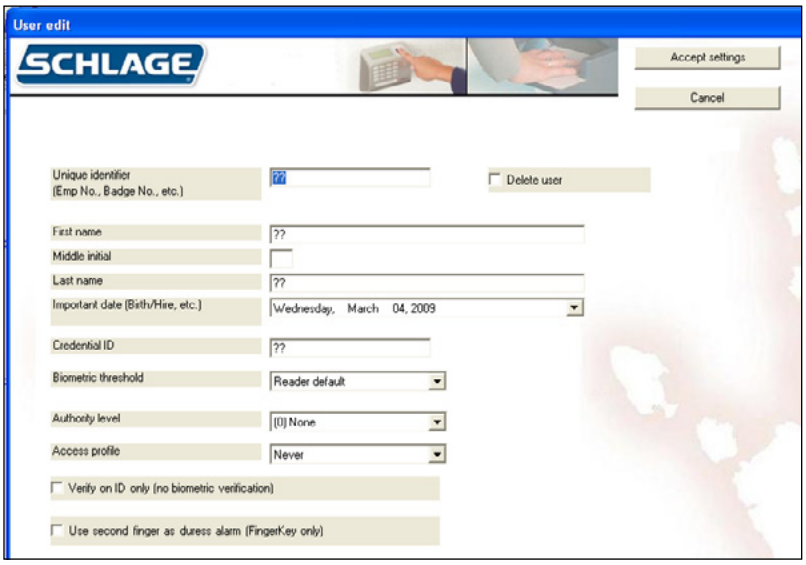


Figure 5.2: User Edit Screen

Delete a User

1. Click the *Users* tab.
2. Click to select the name of the user you want to delete.
3. Click the *Edit selected user* button.
4. Click the *Delete user* check box.
5. Click the *Accept Settings* button.

➔ Note: You can also edit, delete, and enroll an existing user by clicking on that user listed on the User's tab and selecting the desired action from the pop-up menu.

Table 5.2: User Fields		
Field	**Req'd?**	**Description**
Unique Identifier	Yes	• Up to 30 characters (any combination of letters, numbers, spaces, or special characters) • If user was added from the reader, will initially match credential ID in the reader but can be changed.
First Name	Yes	• User's first name • If user was added at the reader, will initially match the credential ID
Middle Initial	No	• User's middle initial
Last Name	Yes	• User's last name • If user was added at the reader, will initially match the credential ID
Important Date	No	• Used to distinguish between users with similar names • Type a date directly into the entry box using the format Thursday, January 01, 2009 • Click the drop-down button to select the date from a calendar.
Credential ID	Yes	• User's credential ID • ID number from user's card (when card readers are used) or the number a user enters manually at the reader. See the reader's manual for help with designing an ID numbering system.
Biometric Threshold	Yes	• Controls how closely user's finger or hand must match the stored template in order for access to be granted. • Reader default uses the Reject Threshold from the reader's setup. See **Reject threshold** on page **26** for more information. In most cases, Reader default is the appropriate choice. • To override the reader's reject threshold, choose from values of 30-250 in the drop down list (common values of 250, 150, 75, 50, and 30 are singled out at the top). • Use a lower number for higher security. • Use a higher number if a user has trouble gaining access. See the reader's manual for more information.
Authority Level	Yes	• Determines what menus the user can access at the reader. • Each level gives access to all the lower levels. • See **Table 5.3: Authority Levels** on page **11** for more information.
Access Profile	Yes	• Controls which readers the user can use. • Always allows access to all readers. • Never blocks access to all readers. • Additional choices correspond to the profiles configured in the Access tab. See **Access Tab** on page **45** for more information.
Verify on ID only (no biometric verification)	No	• Check for users who fingerprints or hand cannot be scanned • Since bypassing finger or hand recognition gives you reduced security, only use this as a last resort. See **Adding a Special User** on page **8** for more information.
Use Second Finger as Duress Alarm (FingerKey only)	No	• When checked, user's second finger will be used as a duress indicator.
Delete User	No	• Check to delete user from HandNet Lite. • User will be deleted from HandNet Lite and from all connected readers when you click the *Accept* button.

Table 5.3: Authority Levels	
Authority Level	**Description**
(0) None:	• Allows user to gain access through the reader, but not use the command menus in the reader to change the reader's settings. • This choice is appropriate for most users.
(1) Service:	• Allows the master reader to display the status of all readers on the network. • Not relevant on readers that are not configured as a master.
(2) Setup:	• Allows user to control reader setup • See reader's manual for more information.
(3) Management:	• Allows user to list all of the users in the reader • Allows master reader to send/acquire user databases to/from readers in a network.
(4) Enrollment:	• Allows user to add or remove users.
(5) Security:	• Allows user to modify security settings • See reader's manual for more information.

See the reader's manual for information on directly changing settings through the reader.

Process Deletes Button

When the Process Deletes button is pressed, HandNet-Lite looks for a RemoveUserXML.Xml file in the root directory of the C: Drive. If this file is found, any users listed in that file will be removed from Handnet-lite. Figure 3.1 provides a sample C:\RemoveUserXML. Xml file which would remove users with UserIDs of 1000, 1001, 1002, 1003, and 1004 when the Process Deletes button is pressed.

```
<?xml version="1.0" standalone="yes"?>
<RemoveUser xmlns="http://tempuri.org/RemoveUser.xsd">
  <CRsiRemoveUser>
    <UserID>1000</UserID>
  </CRsiRemoveUser>
  <CRsiRemoveUser>
    <UserID>1001</UserID>
  </CRsiRemoveUser>
  <CRsiRemoveUser>
    <UserID>1002</UserID>
  </CRsiRemoveUser>
  <CRsiRemoveUser>
    <UserID>1003</UserID>
  </CRsiRemoveUser>
  <CRsiRemoveUser>
    <UserID>1004</UserID>
  </CRsiRemoveUser>
  <CRsiRemoveUser>
    <UserID>1005</UserID>
  </CRsiRemoveUser>
</RemoveUser>
```

Figure 5.3: Example of RemoveUserXML.xml

This page intentionally blank.

Log Tab

The *Log* tab lists events that occur in any connected reader. It also lists any changes made in HandNet Lite.

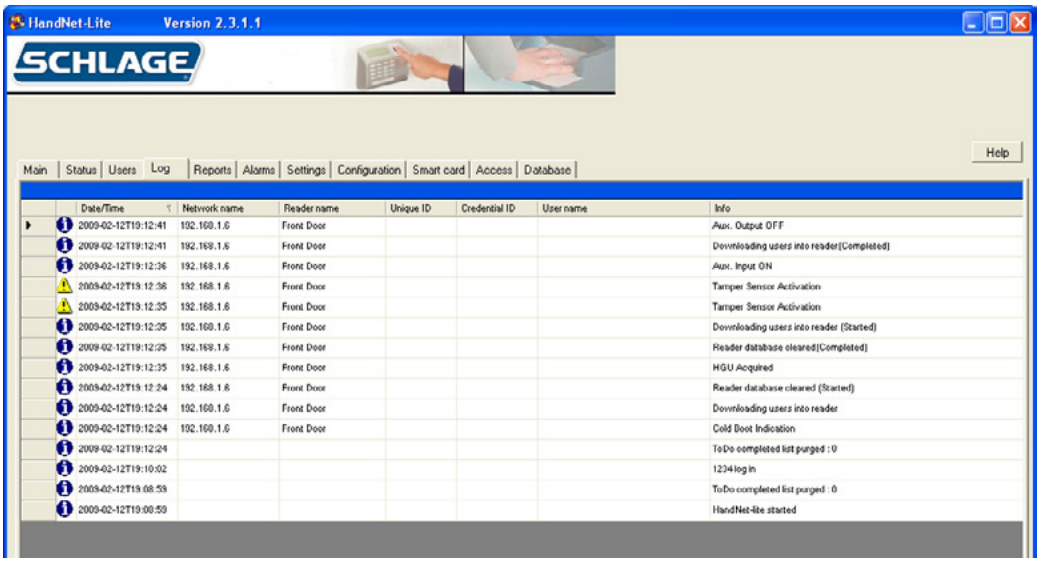


Figure 6.1: Log Tab

Table 6.1: Log Tab Fields

Column	Description
Event type (untitled)	One of the following icons: : Indicates a standard informational message. : Indicates that the condition is important and warrants further investigation. These conditions are also listed on the Alarms tab.
Date/Time	Shows the date and time when the event occurred. The date is listed in year-month-day order, and the time lists hours:minutes:seconds
Network name	Network name if activity occurred at a reader
Reader name	Reader name if activity occurred at a reader
Unique ID	User's unique ID if event is associated with a particular user
Credential ID	User's credential ID if event is associated with a particular user
User name	User's name if message is event with a particular user
Info	Explanation of event

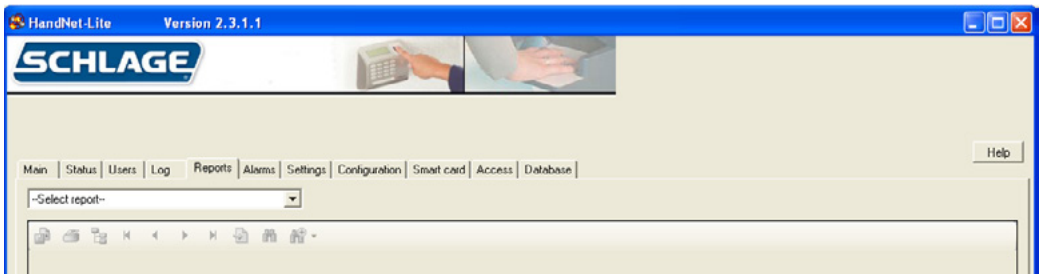
Click the heading of any row to sort the list by that heading. Click the heading again to reverse the sort order.

This page intentionally blank.

Reports Tab

The Reports tab is used to generate and view reports on users and readers.

Figure 7.1: Reports Tab



Generate a Report

1. Click the *Reports* tab.
2. Click the drop-down list at the top of the reports tab and choose the report you want to generate.
3. To print or move around in the report, click the corresponding icon in the bar above the report window.

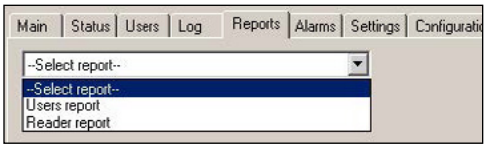


Figure 7.2: Generate a Report

Table 7.1: Report Types

Report Type	Description
Users Report	Lists key information about every user in the system
Readers Report	Lists key information about every reader in the system

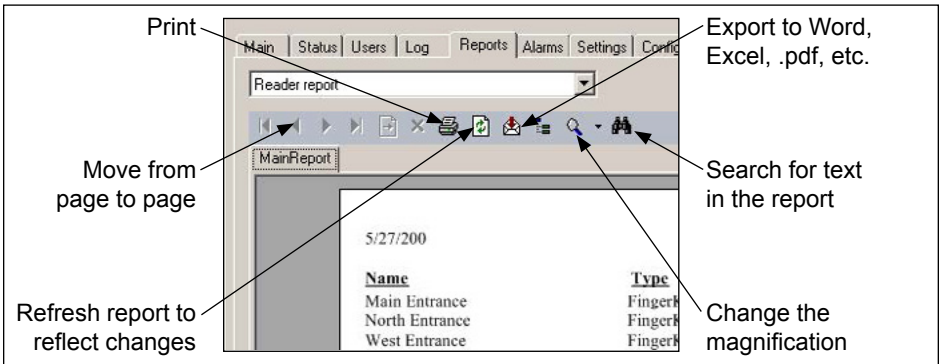


Figure 7.3: Report Window Icons

Users Report

The Users report lists the information for each user in the program.

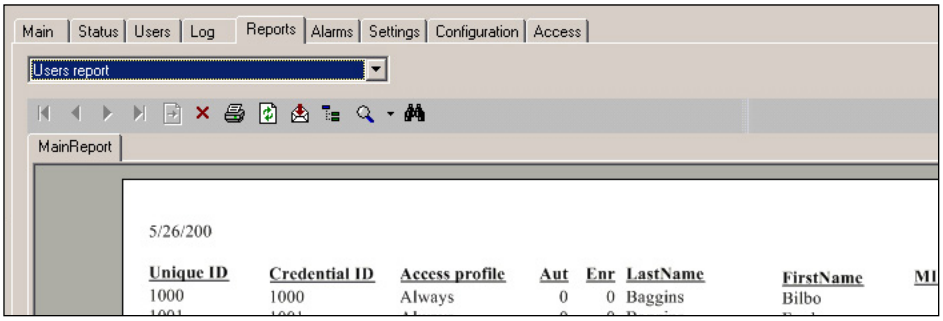


Figure 7.4: Users Report

Table 7.2: Users Report	
Column	**Description**
Unique ID	• User's Unique identifier
Credential ID	• User's credential ID (card or manual ID)
Access Profile	• Access profile associated with the user
Aut	• User's authority level
LastName	• User's last name • If you added the user at the reader and have not changed the name, user ID is listed
FirstName	• User's first name • If you added the user at the reader and have not changed the name, user ID is listed
MI	• User's middle initial.

Reader Report

The Reader report lists information for each reader in the program.

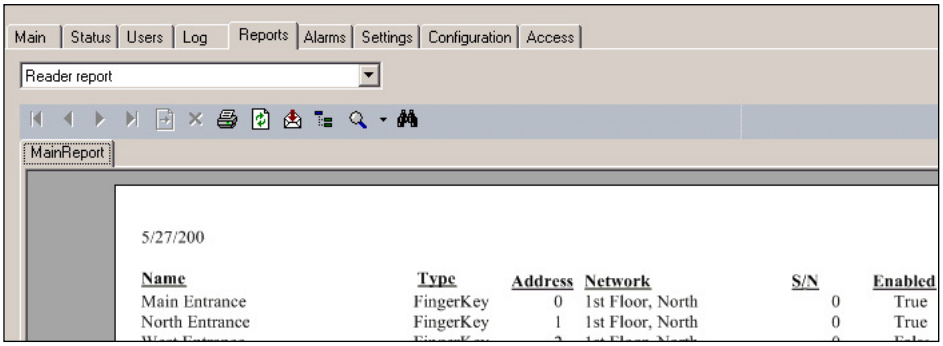


Figure 7.5: Reader Report

Table 7.3: Reader Report	
Column	**Description**
Name	Reader's name
Type	Indicates whether the reader is a hand or fingerprint reader
Address	Reader's address
Network	Network to which reader is connected
S/N	Reader's internal serial number
Enabled	• true: program attempts to communicate with the reader • false: program does not attempt to communicate with the reader

Alarms Tab

The *Alarms* tab shows all alarms that have been recorded in the system. Alarms are also listed with the rest of the activity in the *Log* tab.

Click the heading of any row to sort the list by that heading. Click the heading again to reverse the sort order.

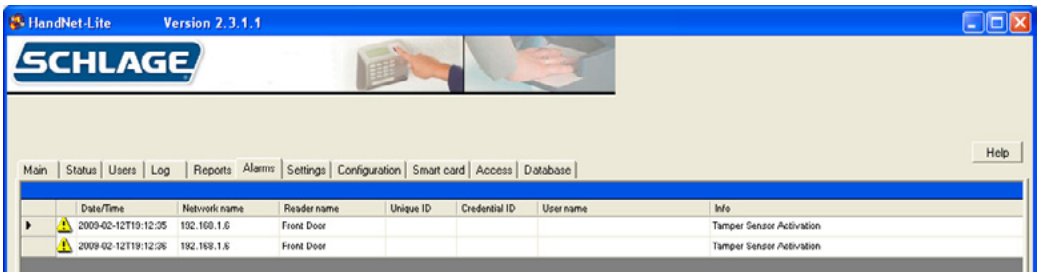


Figure 8.1: Alarms Tab

Table 8.1: Alarms Fields

Column	Description
Date/Time	Date and time when the alarm occurred. The date is listed in year-month-day order, and the time lists hours:minutes:seconds
Network name	Network name if alarm is associated with a particular reader
Reader name	Reader name if alarm is associated with a particular reader
Unique ID	User's unique ID if alarm is associated with a particular user
Credential ID	User's credential ID if alarm is associated with a particular user
User name	User's name if alarm is associated with a particular user
Info	Description of alarm

This page intentionally blank.

Settings Tab

The *Settings* tab allows you to set default settings and add operators to the system.

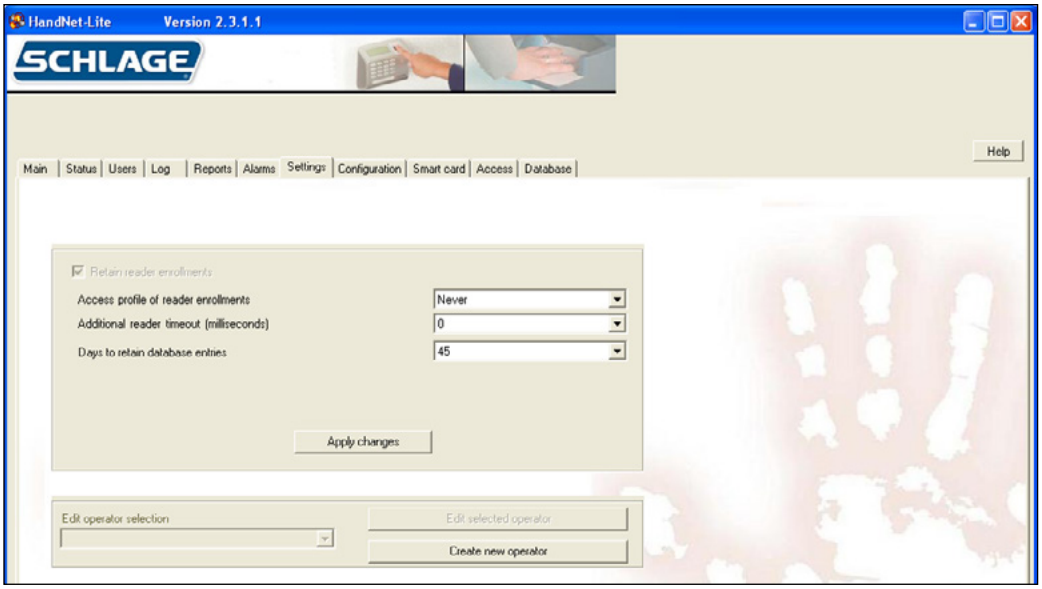


Figure 9.1: Settings Tab

Table 9.1: Settings Fields

Setting	Description
Retain reader enrollments	• This box is always checked and cannot be changed.
Access profile of reader enrollments	• Access profile assigned to users by default when users are added at a reader before being added in the system. • Choices are Always, Never or any custom profiles created by an operator. See **Access Tab** on page **45** for more information.
Additional reader timeout	• Additional time that is added globally to the command timeout. • Select additional time if command timeout errors are generated on the network. These errors would be displayed on the Alarms tab. See **Alarms Tab** on page **17** for more information.
Days to retain expired database entries	• Number of days expired database entries are retained • Choose default of 45 days initially. If database becomes too large, make this number smaller.

Managing Operators

Operators are individuals who can control the system. The level of control can be set individually for each operator.

Add a New Operator

1. Click the *Settings* tab.
2. Click the *Create new operator* button. The Operator edit screen will appear:
3. Click the *Define automatic Windows login for this operator* box to use Windows login information for this operator. See **Enable Automatic Windows Login** on page **20** for more information.
4. Enter a login name in the operator login name box. This name is case sensitive.
5. Enter the password and confirmation in the enter and confirm boxes. The password is case sensitive.
6. Choose the operator allowed actions by clicking the corresponding check box(es).
7. Choose the tabs to which the operator has access by clicking the corresponding check box(es).
8. Click the *Accept Settings* button.

Figure 9.2: Add a New Operator

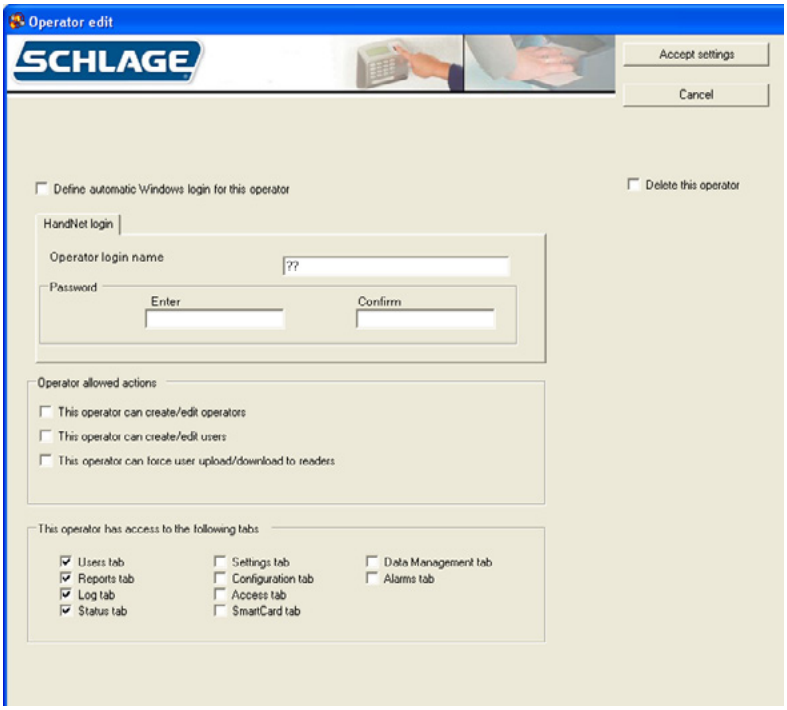


Figure 9.3: Operator Edit Screen

Edit an Operator

1. Click the *Settings* tab.
2. Select the operator you want to edit from the *Edit operator selection* drop-down box.
3. Click *Edit selected operator* button.
4. Edit the necessary settings. See **Add a New Operator** on page **20** for more information.
5. Click the *Accept Settings* button.

Delete an Operator

1. Click the *Settings* tab.
2. Select the operator you want to delete from the *Edit operator selection* drop-down box.
3. Click the *Delete this operator* check box.
4. Click the *Accept Settings* button.

Enable Automatic Windows Login

If you wish to allow automatic Windows login for HandNet Lite:

1. Click the *Main* tab.
2. Log off.
3. Click to un-check the *Force login prompt* checkbox.
4. Shut down HandNet Lite. The next time you start HandNet Lite, you will be automatically logged in.

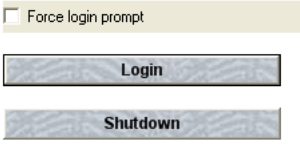


Figure 9.4: Force Login Prompt Checkbox

Disable Automatic Windows Login

1. Click the *Main* tab
2. Log off.
3. Click to check the *Force login prompt* checkbox.
4. Shut down HandNet Lite. The next time you start HandNet Lite, you will be prompted for login name and password.

Configuration Tab

The *Configuration* tab is used to add or edit networks, readers and card formats.

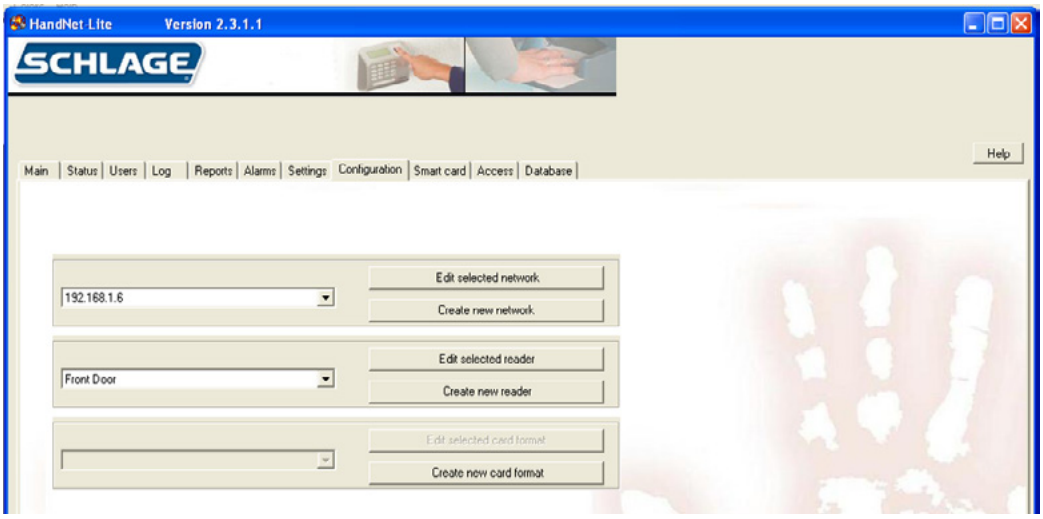


Figure 10.1: Configuration Tab

Managing Networks

A network is a group of up to 32 daisy-chained readers connected though a single serial port using 2 wire RS485, a single reader connected to a computer with RS232, or a single TCP/IP (ethernet) reader. (See the reader manual for wiring and connection detail.)

You control access to each reader separately using HandNet Lite, so having readers with unrelated purposes in one network is fine.

There are two parts to setting up a network and readers: you must physically set the readers up and connect them to each other and to the computer, and you must add the network and readers in HandNet Lite. This manual only explains how to set up the network and readers in HandNet Lite. For help setting up and connecting the readers, see the manual that came with the readers.

Add a Network

1. Click the *Configuration* tab.
2. Click the *Create new network* button
3. Choose the Network type from the drop-down box. The remaining fields displayed will be determined by this selection.
4. Complete the fields on the screen. See **Connecting through a TCP/IP network** on page 22 and **Connecting through a serial port** on page 23.
5. Click *Accept settings*.

Edit a Network

1. Click the *Configuration* tab.
2. Select the network you want to edit from the drop-down box.
3. Click the *Edit selected network* button
4. Complete the fields on the screen. See **Connecting through a TCP/IP network** on page 22 and **Connecting through a serial port** on page 23.
5. Click *Accept settings*.

Delete a Network

Only networks with no readers can be deleted.

1. Click the *Configuration* tab.
2. Select the network you want to delete from the drop-down box.
3. Click the *Edit selected network* button
4. Click the *Delete this network* check box.
5. Click *Accept settings*.

Connecting through a TCP/IP network

To connect to a site through the network, you must have a TCP/IP network with static IP addresses. Your computer must have a network card and be connected to the network. If the network is faster than 10baseT, you must have a switching hub. To use TCP/IP, you must have either ordered readers with the Ethernet option enabled or purchased an Ethernet upgrade.

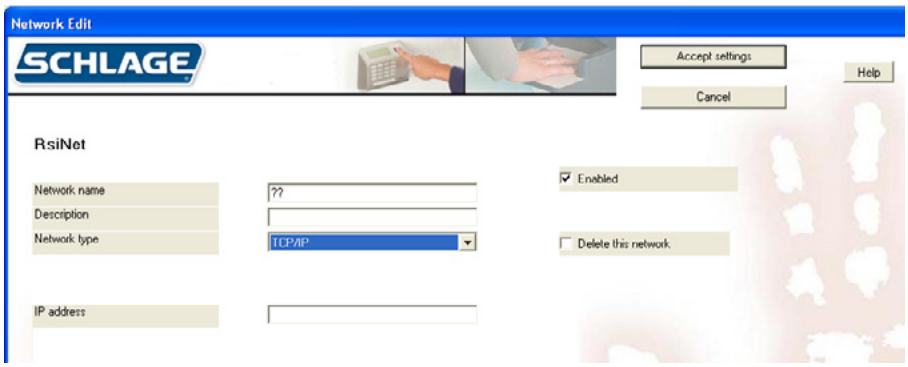


Figure 10.2: Edit a TCP/IP Network

Table 10.1: TCP/IP Network Fields

Field	Req'd?	Description
Network Name	Yes	• Name of the network • Any combination of letters, numbers, spaces, and special characters, up to 30 characters long
Description	No	• Brief description of the network
Enabled	No	• Must be checked for HandNet Lite to communicate with the network and monitor any readers connected to it. • Generally you would only uncheck this if you were in the process of setting up or reconfiguring the network and didn't want the program to try to communicate • Having the Enabled box checked if the network isn't really connected to HandNet Lite causes the program to slow down significantly. Make sure that this is only checked if the network is actually set up and connected
Delete This Network	No	• Check to delete this network and remove it from the Schlage Biometrics network selection list. If there are no readers in the network, it will be deleted when you click Accept settings. • You can't delete a network with readers on it
Network Type	Yes	• Choose Serial port or TCP/IP • The remaining fields will be determined by this selection.
IP address	Yes	• Only available if TCP/IP was chosen in the Network type field. • The IP address (xxx.xxx.xxx.xxx) of the reader • Must match the IP address set in the reader. See the reader manual for more information • Ask your network administrator for an appropriate address

Connecting through a serial port

To connect to a site by running a cable from your computer to the reader, you must have a free serial port on your computer. See the reader manual for more on the requirements for the cable.

Figure 10.3: Edit a TCP/IP Network

Table 10.2: Serial Network Fields

Field	Req'd?	Description
Network Name	Yes	• Name of the network • Any combination of letters, numbers, spaces, and special characters, up to 30 characters long
Description	No	• Brief description of the network
Enabled	No	• Must be checked for the system to communicate with the network and monitor any readers connected to it. • Uncheck when in the process of setting up or reconfiguring the network to keep the program from trying to communicate • If checked when the network is not really connected, the system will slow down significantly.
Delete This Network	No	• Check to delete this network and remove it from the network selection list. • You cannot delete a network with readers in it
Network Type	Yes	• Choose Serial port or TCP/IP • The remaining fields will be determined by this selection.
Comm Port	Yes	• Only available if Serial port was chosen in the Network type field. • Must match the serial port to which the reader is connected • Only the ports that are currently available on your computer are listed.
Baud Rate	Yes	• Only available if Serial port was chosen in the Network type filed. • Choose from values of 4800, 9600, 19200, 28800, 38400, or 57600. • Choose 9600 initially. Increase the rate after a working connection has been established. Longer wire distances require lower rates. • Must match the rate set in all readers on the network. See the reader manual for more information.

Managing Readers

There are two parts to setting up readers: physically setting up the readers and connecting them to each other and to the computer, and adding the network and readers in HandNet Lite. This manual only explains adding the network and readers in HandNet Lite. For help setting up and wiring readers, see the manual that came with the readers.

Before you add readers, you must set up the network to which they are connected. See **Add a Network** on page **21** for more information.

If You've Been Using Readers Already

If you've been using readers without HandNet Lite, when you add the network and readers to the system, HandNet Lite automatically gets the users from the readers and adds them to the system. See **Enroll Users** on page **8** for more information.

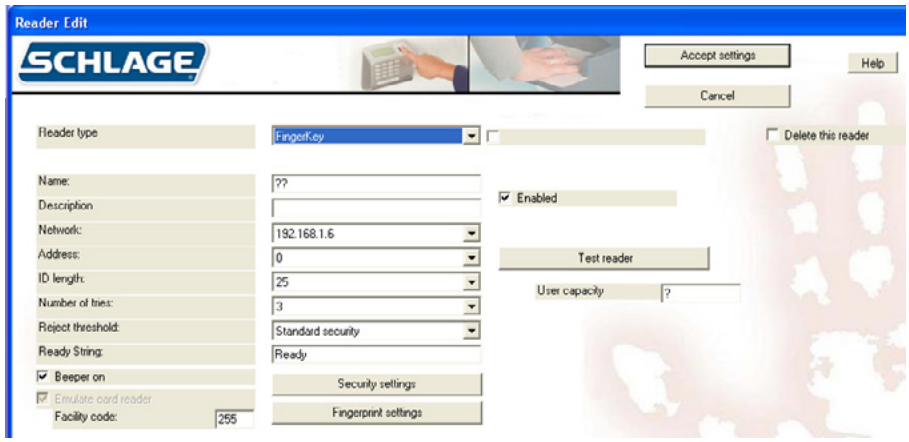


Figure 10.4: FingerKey Reader Edit Screen

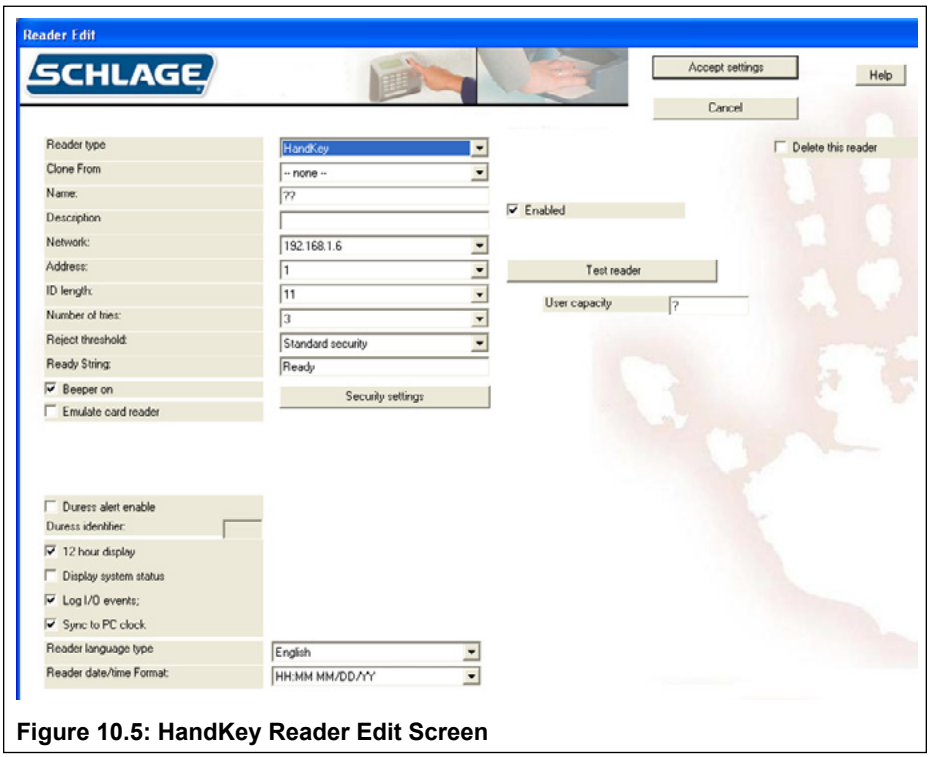


Figure 10.5: HandKey Reader Edit Screen

Add a Reader

1. Click the *Configuration* tab.
2. Select the network in which the new reader will exist from the network drop-down box.
3. Click the *Create new reader* button.
4. Choose the *Reader type* from the drop-down box. The entries on the screen will differ depending on the reader type chosen.
5. Fill in the entries on the Reader Edit screen. See **Figure 10.4: FingerKey Reader Edit Screen** and **Figure 10.5: HandKey Reader Edit Screen**.
6. Click the *Test reader* button. If the reader is properly configured, the reader will be able to communicate.
7. To change the security settings for the reader, click the *Security settings* button. See **Figure 10.6: Security Settings Screen** on page **28** for more information.
8. If you are editing a FingerKey and want to edit the fingerprint settings, click the *Fingerprint settings* button. See **Figure 10.7: Fingerprint Settings Screen** on page **29** for more information.
9. Click the *Accept settings* button.

Edit a Reader

1. Click the *Configuration* tab.
2. Select the network in which the reader you want to edit exists in the network drop-down box.
3. Click the *Edit selected reader* button.
4. The entries on the screen will differ depending on the reader type chosen.
5. Fill in the entries on the Reader Edit screen. See **Figure 10.4: FingerKey Reader Edit Screen** on page **24** and **Figure 10.5: HandKey Reader Edit Screen** on page **24**.
6. Click the *Test reader* button. If the reader is properly configured, the reader will be able to communicate.
7. To change the security settings for the reader, click the *Security settings* button. See **Figure 10.6: Security Settings Screen** on page **28** for more information.
8. If you are editing a FingerKey and want to edit the fingerprint settings, click the *Fingerprint settings* button. See **Figure 10.7: Fingerprint Settings Screen** on page **29** for more information.
9. Click the *Accept settings* button.

Delete a Reader

1. Click the *Configuration* tab.
2. Select the network in which the reader you want to delete exists in the network drop-down box.
3. Click the *Edit reader* button.
4. Click the *Delete this reader* check box.
5. Click the *Accept settings* button.

Table 10.3: FingerKey Reader Fields		
Field	**Req'd?**	**Description**
Clone From	No	• Appears only after at least one reader has been configured. • Allows you copy the settings from another reader, including the underlying Fingerprint and Security Settings. • If this option is chosen, all of the following fields will be populated automatically.
Name	Yes	• Any combination of letters, numbers, spaces, and special characters, up to 30 characters.
Description	No	• Briefly describe the reader.
Network	Yes	• Select the network in which the reader exists. • Network must be set up before you can add the reader. See **Add a Network** on page **21** for more information.
Address	Yes	• Must match the address set in the reader. See the reader's manual for information on setting the address in the reader. • Field will be automatically populated with the first available address that hasn't been used. Choose another number from the pull-down list if desired. • Changing the address on this screen does NOT change the address in the physical reader. If you change an address here, you must also change the address in the reader.
ID Length	No	• If all user IDs are the same length, choose the number of digits here (any value from 1-25) so users don't have to press enter after typing the ID at the reader. • If user IDs are different lengths, choose the longest number of digits. Users with the longest IDs will not have to press ENTER after typing the ID at the reader. • Entry does not affect the length of IDs on cards. It only affects IDs entered at the keypad.
Number of Tries	Yes	• Controls how many times the user can try to get access before the reader will block the user's ID and not allow further tries. • Prevents someone from making repeated tries to gain access with someone else's ID. • Normally 3 is a good setting.
Reject threshold	Yes	• The lower this number is, the more closely the user's finger must match the template of the finger stored in the FingerKey. • 30 (the lowest possible number) requires the fingerprint to match very closely; 250 (the highest possible number) will grant access if the finger match is close but not exactly the same. • 75 is good for most contexts. Choose a lower number if you have an especially high security situation. • If particular users have trouble placing their fingers consistently, you can override the reader's setting for an individual user on the User edit screen in the Users window. See **Edit a User** on page **9** for more information.
Ready String	Yes	• This text appears in the reader display when the reader is ready and waiting for the user to enter an ID. • Any combination of letters, numbers, spaces, and special characters, up to 20 characters
Beeper On	No	• When checked, the reader beeps each time you press a button • In a high security setting, you might want the beeps off to make it harder for a casual observer to figure out how many digits are in the ID number.
Emulate Card Reader	Yes	• FingerKey readers always emulate a card reader, so you can't uncheck this box
Facility Code	Yes	• Facility code that should be passed to the access control panel. • Numeric value from 0 (zero) to 65535
Enabled	No	• Check if the reader is physically set up and ready to be used. • Checking the Enabled box if the reader is not really connected slows the program down significantly. Make sure this is only checked if the reader is actually set up and connected
User capacity	Yes	• Will be filled in automatically by the reader.
Delete This Reader	No	• Check ONLY to delete reader and remove it from the reader selection list.

Table 10.4: HandKey Reader Fields		
Field	**Req'd?**	**Description**
Clone From	No	• Appears only after at least one reader has been configured. • Allows you copy the settings from another reader, including the underlying Fingerprint and Security Settings. • If this option is chosen, all of the following fields will be populated automatically.
Name	Yes	• Any combination of letters, numbers, spaces, and special characters, up to 30 characters.
Description	No	• Briefly describe the reader. You may leave this blank if you wish
Network	Yes	• Select the network in which the reader exists. • Network must be set up before you can add the reader. See **Add a Network** on page **21** for more information.
Address	Yes	• Must match the address set in the reader. See the reader's manual for information on setting the address in the reader. • Field will be automatically populated with the first available address that hasn't been used. • Choose another number from the pull-down list if desired. • Changing the address on this screen does NOT change the address in the physical reader. If you change an address here, you must set the reader to the same address or the program won't be able to communicate with the reader
ID Length	No	• If all user IDs are the same length, choose the number of digits here (any value from 1-25) so users don't have to press enter after typing the ID at the reader. • If user IDs are different lengths, choose the longest number of digits. Users with the longest IDs will not have to press ENTER after typing the ID at the reader. • Entry does not affect the length of IDs on cards. It only affects IDs entered at the keypad.
Number of Tries	Yes	• Controls how many times the user can try to get access before the reader will block the user's ID and not allow further tries. • Prevents someone from making repeated tries to gain access with someone else's ID. • Normally 3 is a good setting.
Reject threshold	Yes	• The lower this number is, the more closely the user's finger must match the template of the finger stored in the FingerKey. • 30 (the lowest possible number) requires the fingerprint to match very closely; 250 (the highest possible number) will grant access if the finger match is close but not exactly the same. • 75 is good for most contexts. Choose a lower number if you have an especially high security situation. • If particular users have trouble placing their fingers consistently, you can override the reader's setting for an individual user on the User edit screen in the Users window. See **Edit a User** on page **9** for more information.
Ready String	Yes	• This text appears in the reader display when the reader is ready and waiting for the user to enter an ID. • Any combination of letters, numbers, spaces, and special characters, up to 20 characters
Beeper On	No	• When checked, the reader beeps each time you press a button • In a high security setting, you might want the beeps off to make it harder for a casual observer to figure out how many digits are in the ID number.
Emulate Card Reader	Yes	• Controls the Output Mode of teh reader (Lock Output mode if unchecked, Card Reader Emulation Output if checked).
Enabled	No	• Check if the reader is physically set up and ready to be used. • Checking the Enabled box if the reader is not really connected slows the program down significantly. Make sure this is only checked if the reader is actually set up and connected
User capacity	Yes	• Contains the number of users the reader is capable of storing (this field is filled in after the Test Reader button is pressed)
Delete This Reader	No	• Check ONLY to delete reader and remove it from the reader selection list.
Duress alert enable	No	• If checked, duress activates AUX output
Duress identifier	No	• This is the key which, when pressed, will generate the DURESS event. • Must be a digit 0 through 9. Other values will disable the duress feature.
12 hour display	No	• If checked, displays terminal time in 12 hour format, otherwise 24 hour time format.
Display system status	No	• If checked, the reader's LCD will display system status on line 2. If unchecked, line 2 of the LCD will display the unit's date and time.
Log I/O events	No	• Currently ignored by HandKey units, I/O Events will always generate a DataLog
Sync to PC clock	No	• The reader's clock will be synchronized to this PC's system time.
Reader language type	No	• Selects the language used on the reader for LCD prompts.
Reader date/time Format	No	• Selects the format that the reader will display date & time on the LCD display.

Security Settings Screen

The Security Settings Screen controls the passwords needed to access the menus in the reader.

Generally the default passwords shown above are adequate since a user must be set up with the appropriate Authority level on the User edit screen in the Users window (see **Edit a User** on page **9**), and the user must know how to get to these menus in the reader before the passwords below would do any good.

Figure 10.6: Security Settings Screen

Edit Security Settings

1. Click the *Configuration* tab.
2. Select the network in which the reader you want to edit exists in the network drop-down box.
3. Select the reader you want to edit from the reader drop-down box.
4. Click the *Edit selected reader* button.
5. Click the *Security settings* button.
6. Edit the passwords. See **Table 10.5: Security Settings Fields**.
7. Click the *Accept settings* button.

Table 10.5: Security Settings Fields

Field	Req'd	Description
Service	Yes	Allows the master reader display the status of all readers on the network
Setup	Yes	Controls reader setup including the reader's address, ID length, auxiliary output settings, facility codes, network configuration, the duress indicator, etc. It also contains an option to upgrade the maximum number of users
Management	Yes	Allows display of a list all of the users in the reader and lets the master reader send/acquire user databases to/from readers in a network
Enrollment	Yes	Allows you to add or remove users
Security	Yes	Allows you to customize user settings, control how closely user fingerprints must match templates, set the menu passwords, clear all the users from reader, etc

For more detail on the reader menus, see the reader manual.

Fingerprint Settings Screen

The Fingerprint Settings screen controls a number of the reader's internal settings.

Edit Fingerprint Settings

1. Click the *Configuration* tab.
2. Select the network in which the reader you want to edit exists in the network drop-down box.
3. Select the reader you want to edit from the reader drop-down box.
4. Click the *Edit selected reader* button.
5. Click the *Fingerprint settings* button.
6. Edit the necessary fields. See **Table 10.6: Fingerprint Settings Fields**.
7. Click the *Accept settings* button.

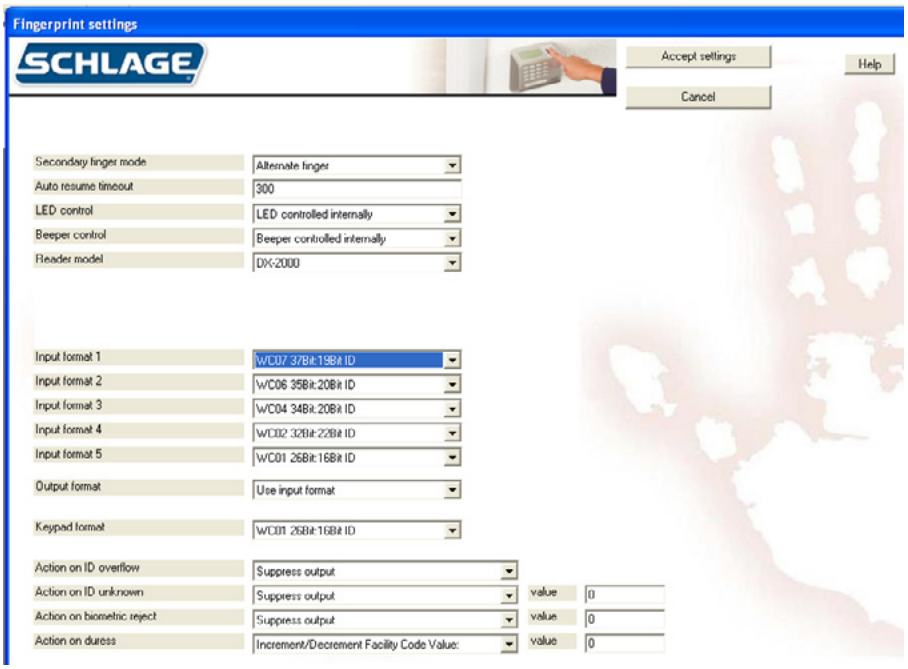


Figure 10.7: Fingerprint Settings Screen

Table 10.6: Fingerprint Settings Fields

Field	Req'd?	Description
Secondary Finger Mode	Yes	• Disabled: reader collects only one finger for each user. • Alternate finger: Scan of second finger grants access exactly as the first does. If user cannot verify with one finger, the other enrolled finger can be used. • Duress finger: Scan of second finger grants access and triggers a duress alarm. (Accomplished by either sending an alternate facility code or with reverse parity, depending on how your access control panel is set up.)
Auto Resume Timeout	Yes	• Number of seconds that reader stays in idle mode after being set into idle mode by a host command. • Number between 60 and 65535 • Default value is 300. • DO NOT change this setting unless advised to by technical support
LED Control	Yes	• Determines what controls the reader's LED display. • LED controlled internally: reader controls the LED display • LED controlled externally: access control panel control the LED display • For more information on setting up the LED control, see the reader's manual.
Beeper Control	Yes	• Determines what controls the reader's beeper. • Beeper controlled internally: reader controls beeper • Beeper controlled externally: access control panel controls beeper • For more information on setting up the beeper control, see the manual that came with the readers.
Reader Model	Yes	• Select the FingerKey model type from the drop down choices which are: • DX-2000 - Select this if you are using a DX-2000 model FingerKey. • DX-2100 HID Prox - Select this if you are using a DX-2100 model FingerKey using HID Prox cards. • DX-2200 HID iClass - Select this if you are using a DX-2200 model FingerKey with HID iClass cards. • DX-2400 Philips Mifare Standard - Select this if you are using a DX-2400 model FingerKey with Mifare Standard cards and settings. • DX-2400 Philips Mifare DESFire - Select this if you are using a DX-2400 model FingerKey with Mifare DESFire cards and settings.

Table 10.6: Fingerprint Settings Fields

Field	Req'd?	Description
iCLASS Configuration	Yes	• Choose None unless you are using iCLASS readers and cards. • If using iCLASS readers and cards, choose any iCLASS configuration that you've defined. • See **Add an iCLASS Definition** on page **35** for more information.
Mifare standard Configuration	Yes	• Choose None unless you are using Mifare Standard readers and cards. • If using Mifare Standard readers and cards, choose any Mifare Standard definition that you've defined. • See Add a Mifare Standard Definition on page 57 for more information.
DESFire Configuration	Yes	• Choose None unless you are using Mifare DESFire readers and cards. • If using Mifare DESFire readers and cards, choose any Mifare DESFire definition that you've defined. • See **Add a DESFire Definition** on page **39** for more information.
Input Format 1-5	Yes	• Card formats reader will accept from an internal or external card reader. • Choose either Wiegand or Magstripe formats but not both. Most companies use only one format. See **Table 10.7: Card Format Fields** on page **32** for more information. • If you change from Wiegand to Magstripe format, or from Magstripe to Wiegand, you must reboot the reader. See the reader manual for further detail
Output Format	Yes	• Format reader sends to the access control panel if you use an internal or external card reader. • Use Input Format: Passes through whatever format is received • None: Reader sends no output when the ID is entered with a card. • Formats 1-11: Choose one of the formats from **Table 10.7: Card Format Fields** on page **32**.
Keypad Format	Yes	• Format the reader sends to the access control panel when a user enters his ID on the keypad instead of using a card. • None: Reader sends no output when the ID is entered with the keypad. • Formats 1-11: Choose one of the formats from **Table 10.7: Card Format Fields** on page **32**.
Action on ID Overflow	Yes	• Indicates what reader sends to access panel when card ID is longer than maximum length permitted by selected formats. • Suppress Output: Reader sends no output • Substitute all 1 bits: All 1 (one) bits are sent instead of the ID that was entered • Substitute all 0 bits: All 0 (zero) bits are sent instead of the ID that was entered
Action on ID Unknown	Yes	• Controls what the reader sends the access panel when ID is not recognized • Suppress Output: reader sends no output • Alternate Facility Code Value: reader sends facility code entered in the value entry, instead of the normal facility code • Increment/Decrement Facility Code Value: Reader sends facility code increased or decreased by the amount in the Value entry. • Toggle All Parity Bits: reader toggles the output parity bits.
Action on Biometric Reject	Yes	• Controls what the reader sends the access panel when a valid ID is entered but the finger doesn't match the template. • Same four options here as for Action on ID Unknown
Action on Duress	Yes	• Controls what the reader sends the access panel when a user places a duress finger • Same four options here as for Action on ID Unknown
Value	Yes	• Number between 0 and 32767 • Used when either Alternate Facility Code Value, Increment/Decrement Facility Code Value is chosen in the previous three fields • Enter a minus (-) sign before the number if you want to decrement the value.

Enabling a Secondary Finger Later

If users are enrolled with Seconday finger mode disabled, only one finger will be collected. If Secondary finger mode is later changed, all users need to be removed and re-enrolled in order to obtain a template for the second finger. The first finger will still function normally, but the second finger functionality will not be available until the user is re-enolled.

Interpreting the Format Detail

In the explanation of the format detail, you'll see an elaboration on the format that looks like **Figure 10.8: Format Detail**.

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.

```
          1         2
12345678901234567890123456
PFFFFFFFFIIIIIIIIIIIIIIIIP
EXXXXXXXXXXXX.............
.............XXXXXXXXXXXXO
```

Figure 10.8: Format Detail

P/E/O/X/.: P indicates a parity bit; the E under the first parity bit here indicates that this parity is even. The X's following indicate which bits are used to determine that parity bit; the periods following indicate that those bits are not used in determining that parity bit; in this example, bits 2-13 are used to determine parity bit 1, and bits 14-26 do not affect this parity bit. The O under the second parity bit (bit 26) indicates this parity bit is odd; the preceding X's indicate that bits 14-25 are used to determine this parity bit.

For a list of available card formats, see **Table 10.7: Card Format Fields** on page **32**.

Managing FingerKey Card Formats

Most users don't need to define additional formats; the predefined formats that we initially provide cover almost all situations. However, if you need some other Wiegand format, you can define any format that you want.

We don't recommend changing or deleting any of our standard card formats. If you need a format that is similar to one of our existing formats, choose to add a new format; there's an option on the screen that lets you clone (copy) an existing format; you can then change the copy rather than changing the original.

Add a Card Format

1. Click the *Configuration* tab.
2. Click the *Create new card format* button.
3. Complete the fields on the screen. See **Table 10.7: Card Format Fields** on page **32** for more information.
4. Click the *Accept settings* button.

Edit a Card Format

1. Click the *Configuration* tab.
2. Select the card format you want to edit from the drop-down box.
3. Click the *Edit selected card* format button.
4. Make changes to the fields on the screen. See **Table 10.7: Card Format Fields** on page **32** for more information.
5. Click the *Accept settings* button.

Delete a Card Format

1. Click the *Configuration* tab.
2. Select the card format you want to edit from the drop-down box.
3. Click the *Edit selected card format* button.
4. Click the *delete* check box.
5. Click the *Accept settings* button.

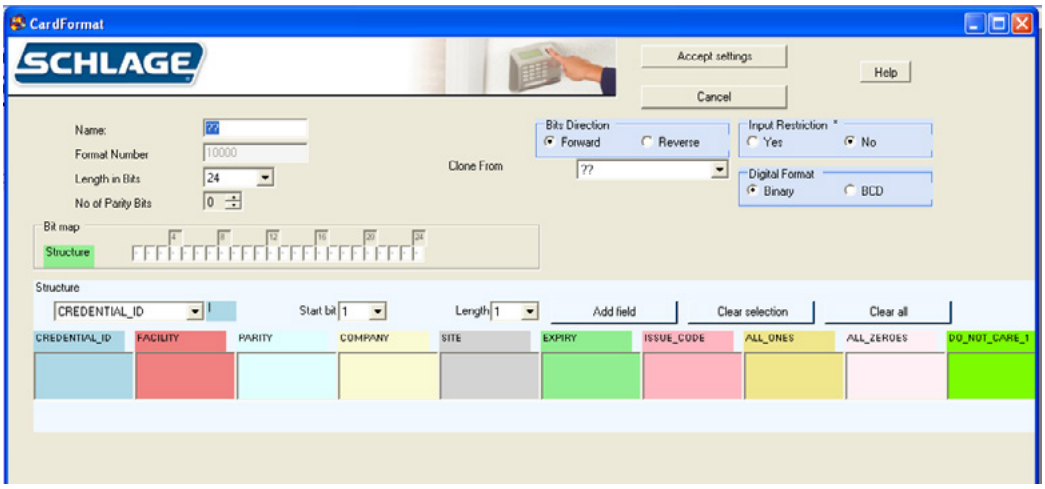


Figure 10.9: The Card Format Screen

The appearance of this screen varies depending on what you choose. The width of the Bit Map section changes based on the length you define for the ID. The Parity sections at the bottom only appear if you indicate that there are parity bits

Table 10.7: Card Format Fields

Field	Req'd?	Description
Name	Yes	• Name that clearly identifies the format
Format Number	Yes	• Internally generated number to identify the format. Cannot be changed.
Length in Bits	Yes	• Number of bits in the format. This is the total number of bits, not just the number of bits in the ID
No of Parity Bits	No	• If there are any parity bits, enter the number (1-4) here. • For each parity bit specified here, a Parity section appears below
Bit Map	Yes	• Structure of the format and how each bit is used. • To change how different bits are used, see **Card Format Structure** on page **33** and **Figure 10.10: Bit Map Example** on page **33** for more information.
Delete	No	• Deletes the current format.
Bits Direction	Yes	• Forward: bits will be read in from left to right • Reverse: bits will be read in from right to left
Clone From	No	• Only appears if you are creating a new format. • Allows you to make a copy of an existing format. • Entries on the screen will be set to match the settings for the format you choose.
Input Restriction	Yes	• Yes: only an exact format match will be accepted. Gives higher security since cards that are not issued by you will not be accepted. • No: any input and parses will be accepted
Digital Format	Yes	• Leave this set to Binary unless you understand what BCD is and have a specific reason for choosing it

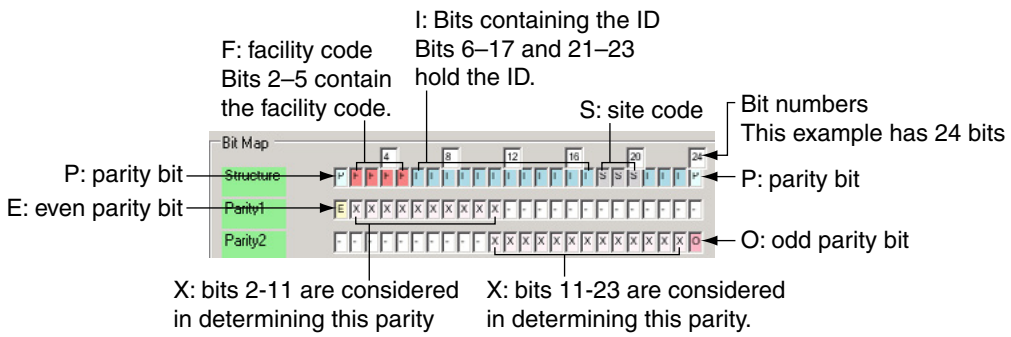


Figure 10.10: Bit Map Example

Card Format Structure

1. Under Structure, choose the type of bit you want to add from the drop-down box.
   - Credential ID
   - Site
   - All Zeros
   - Facility
   - Expiry
   - Do Not Care 1
   - Parity
   - Issue Code
   - Do Not Care 0
   - Company
   - All Ones

   To add parity bits, see **Set Up the Parity Bits** on page **34**.
2. Choose the first bit you want to use for the structure from the *Start bit* drop-down box.
3. Choose the number of sequential bits from the *Length* drop-down box.
   - For example, if bits 2-11 should contain the ID, select 2 from the Start Bit drop-down box, and 10 from the Length drop-down box.
   - If a particular structure is broken up, the structure will be added in multiple steps. For example, if you have a 15 bit ID, but that ID is contained in bits 2–6, 8–12, and 14–18, add the Credential ID three times: the first time with a Start Bit of 2 and a Length of 5, the second time with a Start Bit of 8 and a Length of 5, and the third time with a Start Bit of 14 and a Length of 5.
   - Similarly, suppose a particular structure is scrambled. For example, suppose bit 2-11 are used for the ID, but instead of being in order, bit 9 is the first bit of the ID, bit 3 is the second, etc. You would simply add this one bit at a time, starting with the first bit (bit 9), then the second, etc. Bits are considered in the order they appear in the structure list. (If you add bits in the wrong order, there's no way to rearrange them. You must delete the incorrect bits and then add them again in the correct order.)
   - If the Start Bit is disabled, then you have used all available bits; if you want to change the function of an existing bit, you must delete the incorrect bits before you can add them elsewhere.
4. Click *Add Field*.

   The bit numbers will be added in the corresponding columns in the structure table, and the bits will be reflected in the Bit Map representation above.
5. To remove an incorrect bit, check the box next to the bit and then click the *Clear Selection* button.
6. To clear (delete) the entire structure, click the *Clear All* button.

Set Up the Parity Bits

1. Add the Parity Bit to the Structure
   a. Under Structure, choose *Parity* from the drop-down box.
   b. Choose the first bit you want to use for the parity bit from the *Start bit* drop-down box.
   c. Choose the number of sequential bits (usually 1) from the *Length* drop-down box.
   d. Click the *Add Field* button.
2. Indicate whether that parity bit is even or odd
   a. Under *Parity 1*, choose *Even* or *Odd* from the drop-down box.
   b. Under Start Bit, choose the bit for which you want to identify parity from the drop-down box.
   c. Click *Add Field*.
3. Identify which bits are considered to determine that parity bit
   a. Under *Parity 1*, choose *Included*
   b. Under *Start Bit*, choose the first bit that is used to determine this parity
   c. Under *Length*, indicate the number of bits to consider
   d. Click *Add Field*.
   e. If the bits to consider are broken up (for example, if you want to consider bits 2–10 and bits 14–18), simply repeat this step to add the additional bits.

Smart Card Tab

The Smart Card tab is used only with FingerKeys. It is used to manage FingerKey iCLASS, DESFire and MiFare cards.

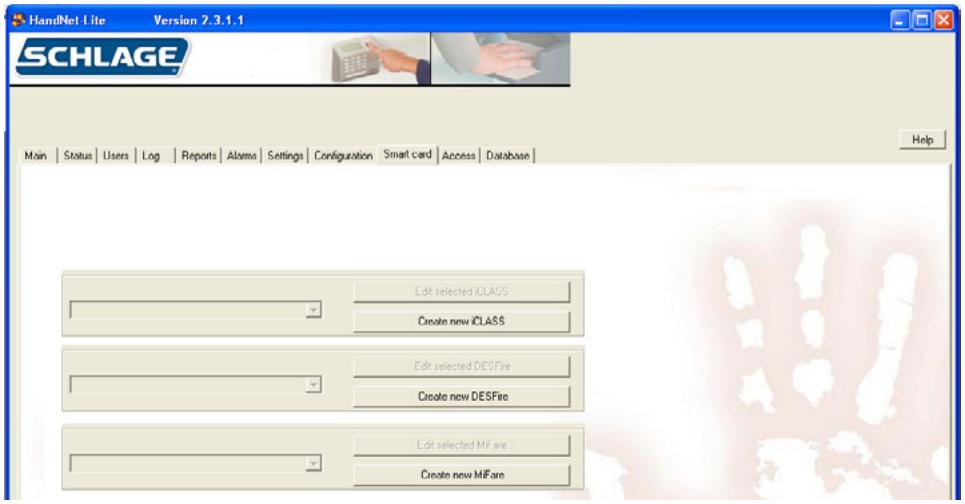


Figure 11.1: Smart Card Tab

Managing FingerKey iCLASS Definitions

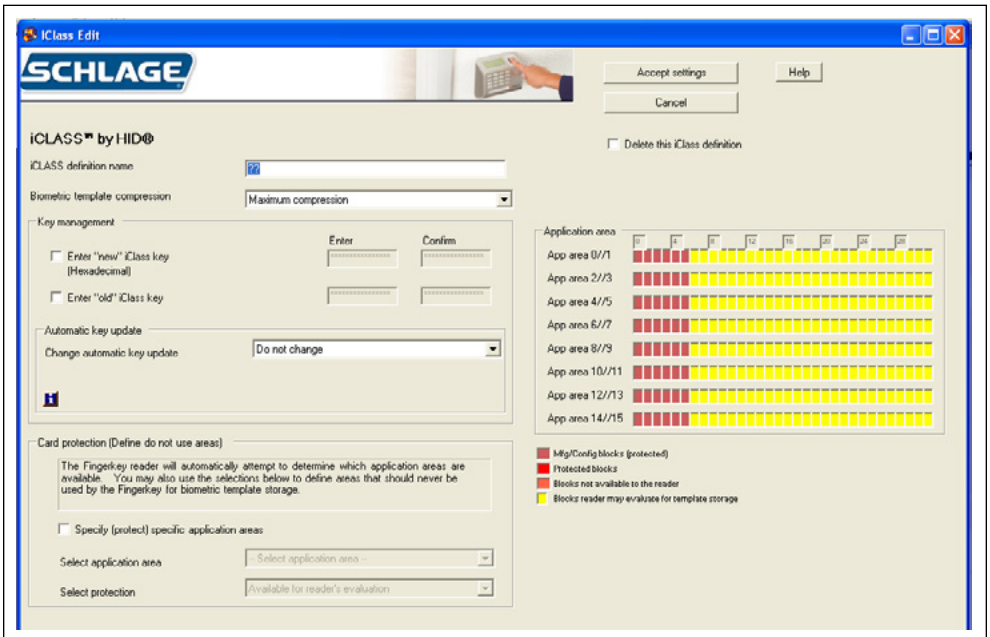


Figure 11.2: iCLASS Definition Screen

Add an iCLASS Definition

1. Click the *Smart Card* tab.
2. Click the *Create new iCLASS* button.
3. Complete the fields on the screen. See **Table 11.1: iCLASS Definition Fields** on page **36** for more information.
4. Click the Accept settings button.

Edit an iCLASS Definition

1. Click the *Smart Card* tab.
2. Choose the iCLASS definition you want to edit from the drop-down box.
3. Click the *Edit selected iCLASS* button.
4. Complete the fields on the screen. See **Table 11.1: iCLASS Definition Fields** on page **36** for more information.
5. Click the *Accept settings* button.

Delete an iCLASS Definition

1. Click the *Smart Card* tab.
2. Choose the iCLASS definition you want to delete from the drop-down box.
3. Click the *Edit selected iCLASS* button.
4. Click the *Delete this iCLASS definition* check box.
5. Click the *Accept settings* button.

Table 11.1: iCLASS Definition Fields		
Field	**Req'd?**	**Description**
iCLASS definition name	Yes	• Name of the iCLASS definition • Any name that distinguishes this definition from others
Biometric template compression		• Controls the amount of compression of the finger template before it is written to the iCLASS card • Maximum compression should be used initially • See **Table 11.2: iCLASS Card Compression** on page **36** for more information.
Enter "new" iClass key		• A password that encrypts the areas used by the readers on iCLASS cards • Protects the fingerprint data from being read if the same cards are used with other devices. • 16 hex digits (0–9 and A–F.) • A default key is used when a new iCLASS definition is defined. Can be used permanently if desired. • For increased security, change this key periodically.
Confirm "new" iClass key		• Confirmation of previous field
Enter "old" iClass key		• Old reader key, usually populated automatically. • Required for the reader to change the key. • All cards should be updated each time the key is changed, to ensure they key is always up-to-date. • **See Resetting Old Card Keys on page 37 for more information.**
Automatic Key Update		• Indicates whether readers using this definition can automatically change the key on a card. • Defaults to Do Not Change. Whatever setting was previously entered will continue to be used. If you're editing a previously created definition, click the H button to see what the current settings are. • Options: • Do Not Change: Use the previously entered setting. • Disable Auto Key Update: Prevents the reader from changing a key. • Start Unlimited Auto Key Update: Any card with the old key will be automatically updated when used at the reader. • Start Limited Auto Key Update: Any card with the old key will be automatically updated at the reader, until the number of cards and/or date specified is reached. • See **Automatic Key Update** on page **38** for more information.
Specify (protect) application areas		• Only check this box if you are sharing the iCLASS card with another iCLASS device that does not automatically determine the template location on the card. • See **iCLASS Card Protection** on page **37** for more information.

Table 11.2: iCLASS Card Compression		
	Number of Enrolled Fingers	
	1	**2**
No Compression	854 bytes	1654 bytes
Minimum Compression	566	1078
Medium Compression	454	854
Maximum Compression	310	566

iCLASS Card Protection

The grid on the right shows the protected blocks in red:

You can protect multiple areas simply by choosing new values for each of these entries. You can clear any protected area by choosing the application area and choosing Available for Reader's Evaluation in the Select Protection drop down menu.

When you protect blocks in even application areas (0, 2, 4, etc.), blocks are used from the left to the right, that is, starting at block 6 and working up; when you protect areas in odd application areas (1, 3, 5, etc.), blocks are used from right to left, that is, starting at 31 and working down.

If you protect both even and odd sections in any pair (for example, if you protect parts of both area 0 area 1), then the fingerprint reader can't use that pair at all so the entire area is marked as protected.

➔ Programmed iCLASS cards require application area 0 to be blocked off. To do this, click Select Application Area and pick Application Area 0 from the drop down menu. Then click Select Protection and choose Protect 26 blocks.

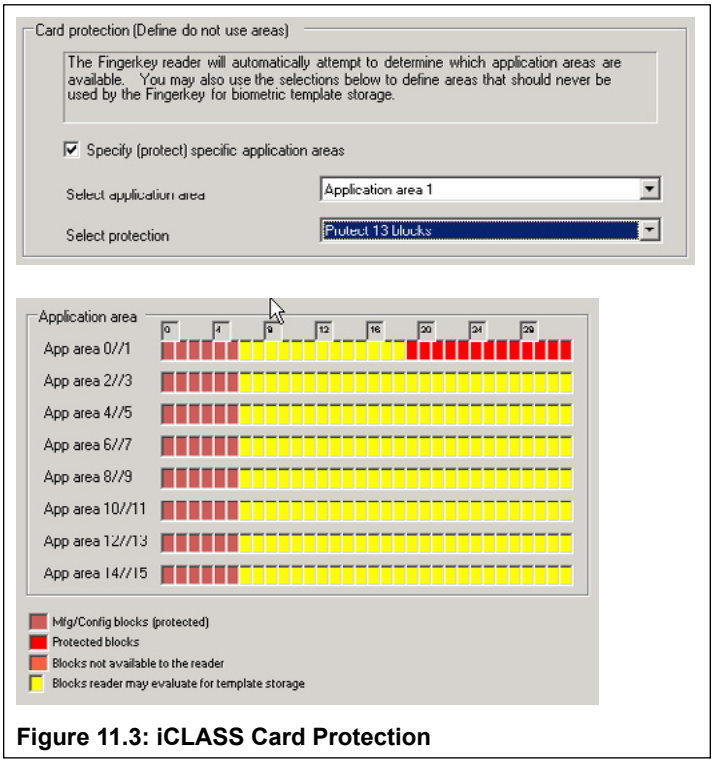


Figure 11.3: iCLASS Card Protection

Resetting Old Card Keys

To change the key for a previously used iCLASS card, the reader must know what the old key is—this prevents unauthorized people from converting other cards to work with your system. HandNet Lite keeps track of what the last key you used was, so most of the time, you don't need to change this entry.

For example, suppose you originally set the key to 1234123412341234 and then you entered a New Reader Key of 5678567856785678. HandNet Lite remembers the old key; it would automatically change cards to the new key if you set it to automatically update keys (see **Automatic Key Update** on page **38**).

However, suppose in January you set the key to 1234123412341234, in February change it to 5678567856785678, and in March change it again to 9ABC9ABC9ABC9ABC. Cards that got used during February would have been updated to 5678567856785678; cards that didn't get used during February would still have January's key of 1234123412341234. The reader can automatically update those cards with the most recent old key (5678567856785678), but it would no longer recognize the prior old key of 1234123412341234. If you have a situation like this, to update the older cards, you must manually indicate what old key to use by checking the Reset Old Key checkbox and then entering the appropriate value in the old key entries.

If you have an older card and know that one of several keys was used on it but aren't sure which one, enter the various old keys in turn here, trying to update the card each time.

You can avoid ever having to do this if you make sure that all cards get updated each time you change your key.

Automatic Key Update

Some administrators want any reader to update the key; other administrators prefer to only let selected readers update cards. For example, for top security, you might only let a non-networked reader in a security office update cards so that was the only place they could be updated. To do this, the administrator would create one iCLASS definition for the public readers (with Automatic Key Update unchecked), and another iClass definition (Automatic Key Update checked) for the administrative reader.

If you disable automatic updates here, you can still manually update keys using the reader command menus.

If you return to this screen, this entry defaults to Do Not Change; this means that whatever setting was previously entered will continue to be used. If you're editing a previously created definition, click the  button to see what the current settings are. (This button doesn't do anything when creating a new definition.)

Your choices are:

Do Not Change: Use the previously entered setting.

Disable Auto Key Update: This prevents the reader from ever changing a key. With this setting, to update cards, you would have to use a reader associated with another iCLASS definition that allowed updates, or you would have to manually update cards with the reader's command menus.

Start Unlimited Auto Key Update: If any card with the old key is used, this automatically updates the card to the new key. There's no limit to the number of cards that can be updated, and no limit on the date range.

Start Limited Auto Key Update: If any card is used that currently has this old key, this automatically updates the card to the new key until the number of cards and/or date specified in the following two entries is reached. For example, if you had 20 employees, you might set this to only automatically update 20 cards; once that was done, cards would not be automatically updated until you changed the key again. You could also specify a date; cards would then be automatically updated until that date, but would not be updated after that date.

Specify (protect) application areas

Only check this box if you are sharing the iCLASS card with another iCLASS device that doesn't automatically determine the template location on the card. If fingerprint readers are the only iCLASS device that you use with your cards, or if you use other device that also automatically choose an available space to store information, then you don't need to change this setting.

For example, Schlage Biometrics hand readers always store their templates in blocks 19–31 of area 1. If you were using the same iCLASS cards with both Schlage Biometrics hand readers and Schlage Biometrics fingerprint readers, you'd have to protect these blocks so a fingerprint template wouldn't get written in this area; if it did, the hand reader would write a template over it.

To protect these blocks, check the box by Specify (protect) application areas, click Select Application Area and pick Application Area 1 from the drop down menu, and click Select Protection and choose Protect 13 blocks from the menu.

Managing FingerKey DESFire Card Definitions

Add a DESFire Definition

1. Click the *Smart Card* tab.
2. Click the *Create new DESFire* button.
3. Complete the fields on the screen. See **Table 11.3: DESFire Definition Fields** on page **40** for more information.
4. Click the *Accept settings* button.

Edit a DESFire Definition

1. Click the *Smart Card* tab.
2. Choose the DESFire definition you want to edit from the drop-down box.
3. Click the *Edit selected DESFire* button.
4. Complete the fields on the screen. See **Table 11.3: DESFire Definition Fields** on page **40** for more information.
5. Click the *Accept settings* button.

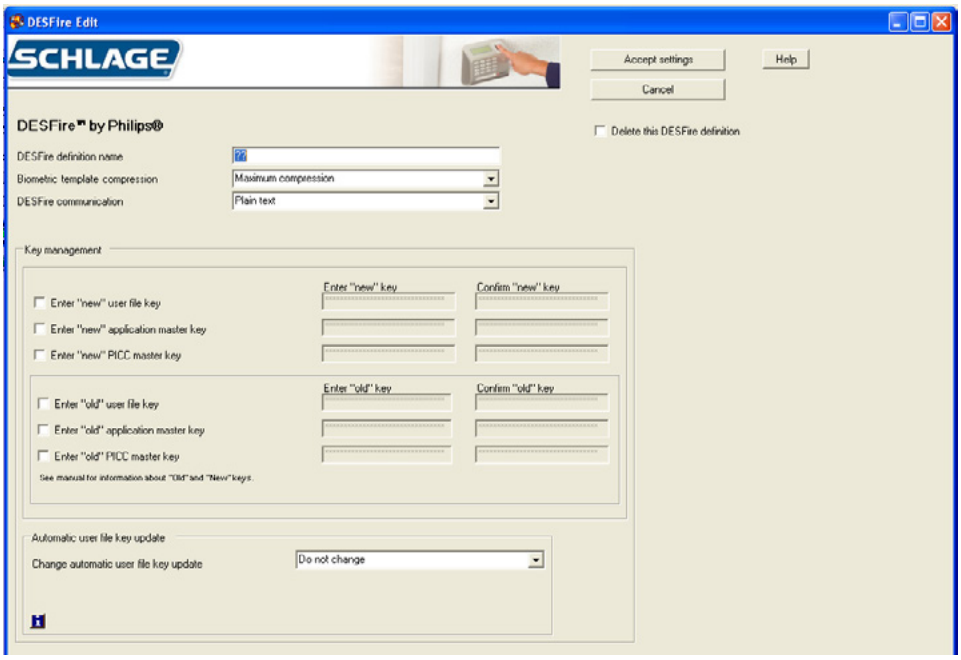


Figure 11.4: DESFire Definition Screen

Delete a DESFire Definition

1. Click the *Smart Card* tab.
2. Choose the DESFire definition you want to delete from the drop-down box.
3. Click the *Edit selected DESFire* button.
4. Click the *Delete this DESFire* definition check box.
5. Click the *Accept settings* button.

Table 11.3: DESFire Definition Fields		
Field	**Req'd?**	**Description**
DESFire definition name	Yes	• Name of the DESFire definition • Any name that distinguishes this definition from others
Biometric template compression	Yes	• Controls the amount of compression of the finger template before it is written to the DESFire card • Maximum compression should be used initially • See **Table 11.4: DESFire Card Compression** on page **40** for more information.
DESFire communication	Yes	• Select either *Plain Text* or *DESFire* ciphered
Enter "new" user file key	Yes	• Check the box to edit these fields. • Key entered must be exactly the same in both boxes.
Enter "new" application master key	Yes	• Check the box to edit these fields. • Key entered must be exactly the same in both boxes.
Enter "new" PICC master key	Yes	• Check the box to edit these fields. • Key entered must be exactly the same in both boxes.
Enter "old" user file key	Yes	• Check the box to edit these fields. • Key entered must be exactly the same in both boxes.
Enter "old" application master key	Yes	• Check the box to edit these fields. • Key entered must be exactly the same in both boxes.
Enter "old" PICC master key	Yes	• Check the box to edit these fields. • Key entered must be exactly the same in both boxes.
Change automatic user file key update	Yes	• The automatic user key update choices are: • Do not change • Disable auto key update • Start unlimited auto key update • Start limited auto key update (displays two additional fields) • With limited auto key update the operator can select the number of cards to be updated and/or the number of cards to automatically update.

Table 11.4: DESFire Card Compression		
	Number of Enrolled Fingers	
	1	**2**
No Compression	854 bytes	1654 bytes
Minimum Compression	566	1078
Medium Compression	454	854
Maximum Compression	310	566

Managing FingerKey Mifare Standard Card Formats

Add a Mifare Standard Definition

1. Click the *Smart Card* tab.
2. Click the *Create new Mifare* button.
3. Complete the fields on the screen. See **Table 11.5: Mifare Standard Definition Fields** on page **42** and **Table 11.6: Mifare Standard Sector Fields** on page **42** for more information.
4. Click the *Accept settings* button.

Edit a Mifare Standard Definition

1. Click the *Smart Card* tab.
2. Choose the Mifare definition you want to edit from the drop-down box.
3. Click the *Edit selected Mifare* button.
4. Complete the fields on the screen. See **Table 11.5: Mifare Standard Definition Fields** on page **42** and **Table 11.6: Mifare Standard Sector Fields** on page **42** for more information.
5. Click the *Accept settings* button.

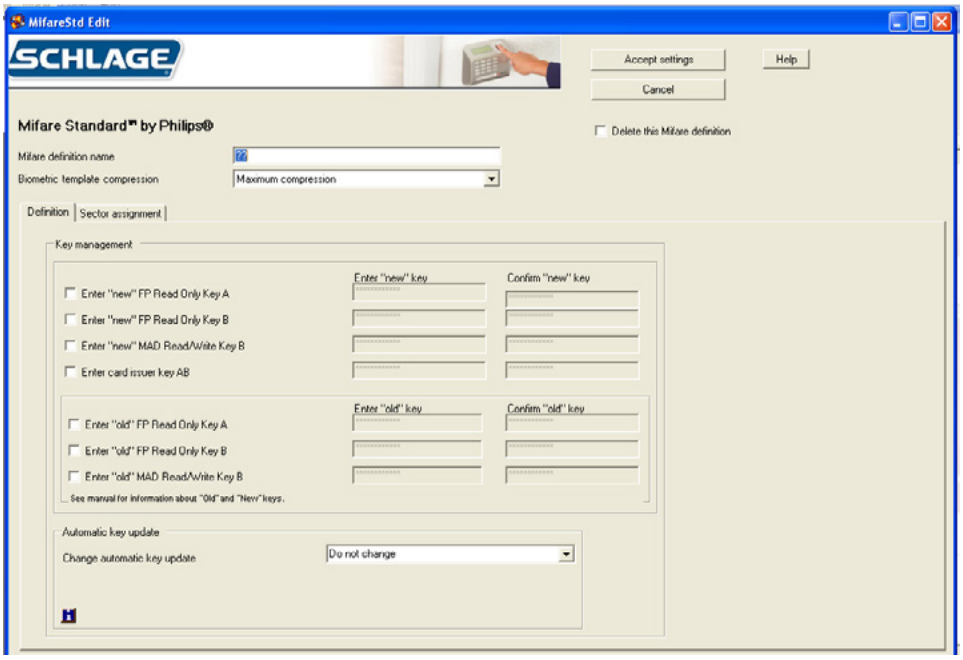


Figure 11.5: Mifare Standard Definition Screen

Delete a Mifare Standard Definition

1. Click the *Smart Card* tab.
2. Choose the Mifare definition you want to delete from the drop-down box.
3. Click the *Edit selected Mifare* button.
4. Click the *Delete this Mifare* definition check box.
5. Click the *Accept settings* button.

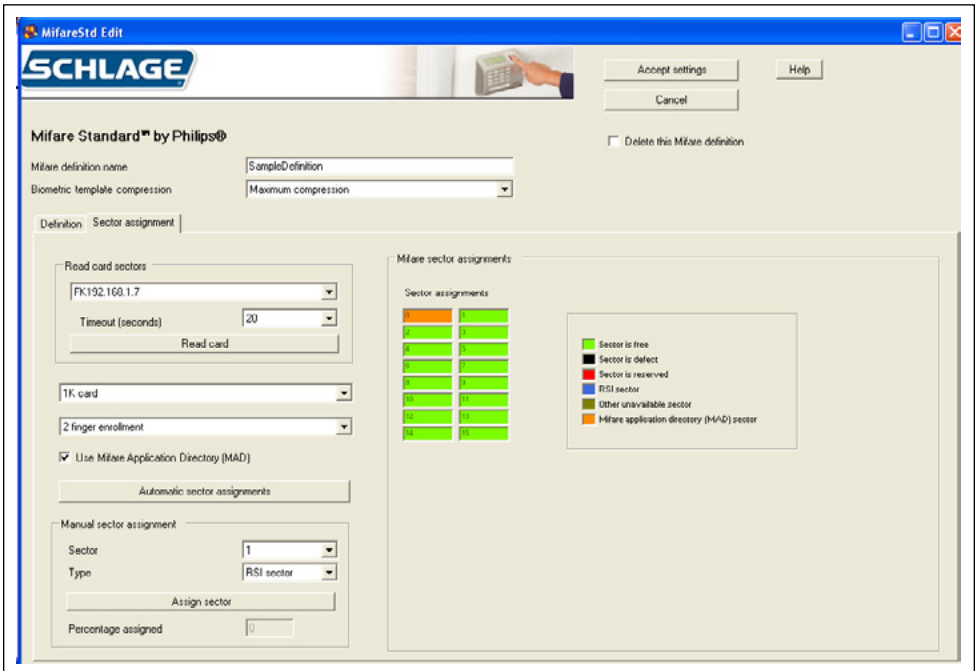


Figure 11.6: Mifare Standard Sector Assignment Screen

Table 11.5: Mifare Standard Definition Fields		
Field	**Req'd?**	**Description**
Mifare definition name	Yes	• Name of the Mifare definition • Any name that distinguishes this definition from others
Biometric template compression	Yes	• Controls the amount of compression of the finger template before it is written to the Mifare card • Maximum compression should be used initially • See **Table 11.7: Mifare Card Compression** on page **43** for more information.
Enter "new" FP Read Only Key A	Yes	• Check the box to edit these fields • Key entered must be the same in both boxes
Enter "new" FP Read Only Key B	Yes	• Check the box to edit these fields • Key entered must be the same in both boxes
Enter "new" MAD Read/Write Key B	Yes	• Check the box to edit these fields • Key entered must be the same in both boxes
Enter card issuer key AB	Yes	• Check the box to edit these fields • Key entered must be the same in both boxes
Enter "old" FP Read Only Key A	Yes	• Check the box to edit these fields • Key entered must be the same in both boxes
Enter "old" FP Read Only Key B	Yes	• Check the box to edit these fields • Key entered must be the same in both boxes
Enter "old" MAD Read/Write Key B	Yes	• Check the box to edit these fields • Key entered must be the same in both boxes
Change automatic key update	Yes	• The automatic key update choices are: • Diable auto key update • Start unlimited auto key update • Start limited auto key update (displays two additional fields) • With limited auto key update, the operator can select the number of cards to be updated and/or the number of cards to automatically update.

Table 11.6: Mifare Standard Sector Fields		
Field	**Req'd?**	**Description**
Read card sectors		• Select the desired FingerKey to use in reading an existing Mifare Standard card • Select a card read timeout in seconds • Click the *Read card* button and present the Mifare Standard card to the reader • The card characteristics will be displayed • Use either Automatic Sector Assignment or Manual Sector Assignment to determine where the FingerKey will place the biometric template.
1K Card or 4K Card	Yes	• Allows you to tell HandNet Lite if the Mifare Standard cards you will be using have 1K or 4K capacity. • If you have used the *Read card* button described above, this will be filled in automatically.
Two finger enrollment or One finger enrollment	Yes	• Allows for storage of either one or two fingerprint biometric templates on the card.
Use Mifare Application Directory (MAD)	Yes	• Allows for use of a MAD (Mifare Application Directory) on the card. A MAD is stored in sector 0 (and 16 if a 4K card) and tells devices how the sectors on the card are allocated. • If unchecked, then you can assign any card sectors to fingerprint template storage.
Automatic sector assignments		• If *Use Mifare Application Directory* is checked, then clicking this button will instruct HandNet Lite to automatically assign the sectors on the card to be used for biometric template assignment (Schlage Biometrics Sector).
Manual Sector Assignment		• Allows you to manually assign the sectors for either biometric template assignment (Schlage Biometrics sector) or a free/available sector. You will need to assign sectors as Schlage Biometrics sectors until the percentage assigned is 100%.

As you use either Automatic or Manual sector assignment the display in the Mifare sector assignments group will change showing you the current assignment.

If your installation is currently using Mifare Standard cards with another device and you wish to add FingerKey biometrics to your existing cards you will wish to:

a. Determine if your current cards are formatted to use a Mifare Application Directory. Contact your existing device manufacturer. You can attempt to use the “Read card sectors” button in HandNet lite to attempt to read an existing MAD on the card.

b. If your current cards are not formatted to use a MAD, then you will need to determine which sectors your current device manufacturer uses on your card. It is normal that sector 0 will be used, but your current cards may also contain data in additional sectors. Check with your existing device manufacturer to determine which sectors on your cards are available and begin the Schlage Biometrics sector assignment at the first free sector.

Once you are satisfied with the card definition, click the “Accept settings” button to record the definition. You will then need to go back to the “Configuration” tab, and for each FingerKey to use this Mifare Standard definition you will need to “Edit selected reader”, click “Fingerprint settings” and use the drop down for “Mifare standard configuration” and select the saved Mifare Standard Definition.

It is important that each FingerKey be assigned the correct Mifare standard configuration setting.

Table 11.7: Mifare Card Compression

	Number of Enrolled Fingers	
	1	**2**
No Compression	854 bytes	1654 bytes
Minimum Compression	566	1078
Medium Compression	454	854
Maximum Compression	310	566

This page intentionally blank.

Access Tab

The Access Tab is used to add or edit access profiles. Access profiles define which type of user can use each reader.

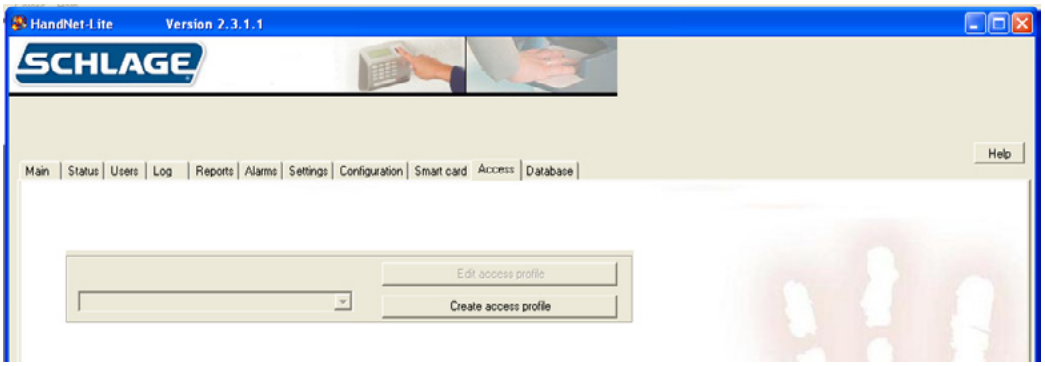


Figure 12.1: Access Tab

For example, suppose your maintenance staff should have access to the maintenance rooms, your office staff should have access to the office, and your supervisors should have access to everything. You would create three access profiles: one for supervisors, one for office staff, and one for maintenance personnel. These profiles would identify which readers each group could use. After creating these profiles, whenever you added a user, you would identify which group the user was a part of, and the access profile for that group would automatically give the appropriate access.

If you want all users to be able to use every reader, you don't need to set up access profiles. HandNet Lite comes set up with an Always profile that lets users use any reader in the system. (It also has a Never profile that doesn't let the user verify at any reader.) You can't change or delete the Always or Never profile.

Add an Access Profile

1. Click the *Access* tab.
2. Click the *Create access profile* button.
3. Enter the access profile name.
4. Check the boxes next to the readers you want users with this access profile to be able to access.
5. Click the *Accept settings* button.

Figure 12.2: Access Profile Edit Screen

Edit an Access Profile

1. Click the *Access* tab.
2. Select the name of the access profile you want to edit from the drop-down box.
3. Click the *Edit access profile* button.
4. Edit the access profile name, if necessary.
5. Check the boxes next to the readers you want users with this access profile to be able to access.
6. Click the *Accept settings* button.

Delete an Access Profile

1. Click the *Access* tab.
2. Select the name of the access profile you want to delete from the drop-down box.
3. Check the box next to *Delete this access profile*.
4. Click the *Accept settings* button.

Table 12.1: Access Profile Fields		
Field	Req'd?	Description
Access profile name	Yes	• Name of the access profile • Use a name that describes the group of users for which this access profile will be used. • Any combination of letters, numbers, spaces, and special characters up to 30 characters
Check readers to be included in this access profile	No	• Lists all the readers in the system • Check the box next to each reader you want users with this profile to be able to access. • Uncheck the box next to each reader you do not want users with this access profile to be able to access.
Delete this access profile	No	• Check to delete this access profile and remove it from the access profile list. • Access profiles that are assigned to users cannot be deleted. To remove an access profile from a user, see **Edit a User** on page **9**. • If you delete the profile that is the default profile for reader enrollments, the next profile in the list will be selected. To choose a different default profile, go to the Settings window and choose the correct profile. See **Table 9.1: Settings Fields** on page **19** for more information.

Database Tab

The Database Tab is used to backup, restore, delete, detach and attach the database.

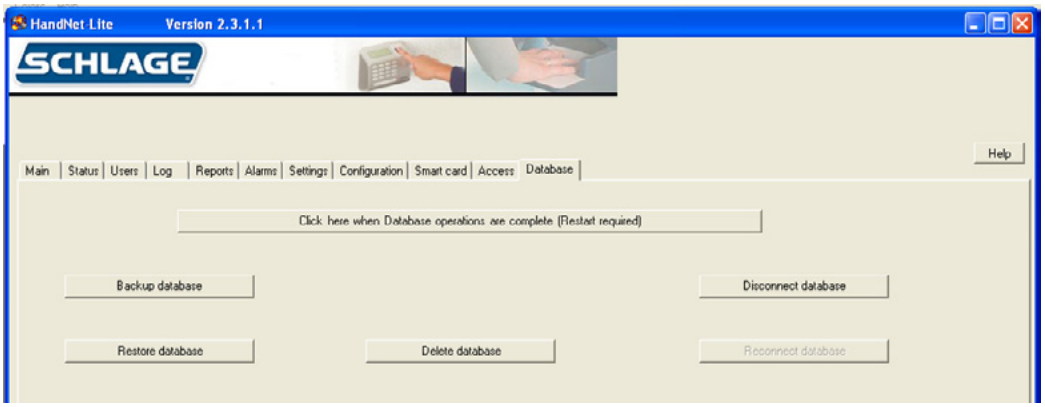


Figure 13.1: Database Tab

Back Up the Database

The Backup database button is used to create a backup of the HandNet-lite database. The location of the backup will be displayed at the bottom of the screen:

1. Click the *Database* tab.
2. Click the *Backup database* button.
3. If you have completed all database operations you want to perform at this time, click the *Click here when Database operations are complete* button. See **Finish Database Operations and Restart** on page **48** for more information.

Restore the Database

The Restore database button is used to restore a backup file of the database.

1. Click the *Database* tab.
2. Click the *Restore database* button.
3. Select the backup file you want to use from the pop-up window and click the *Open* button.
4. If you have completed all database operations you want to perform at this time, click the *Click here when Database operations are complete* button. See **Finish Database Operations and Restart** on page **48** for more information.

Delete the Database

The Delete database button is used to delete the working copy of the database.

➔ If you delete the database, you will lose all configuration and user information in the system. A new, empty database will replace the current database.

1. Click the *Database* tab.
2. Click the *Delete database* button.
3. Click the *Yes* button on the pop-up window.
4. If you have completed all database operations you want to perform at this time, click the *Click here when Database operations are complete* button. See **Finish Database Operations and Restart** on page **48** for more information.

Disconnect the Database

The Disconnect database button is used to disconnect the database from the MS SQL Server Express database engine.

1. Click the *Database* tab.
2. Click the *Disconnect database* button.
3. If you have completed all database operations you want to perform at this time, click the *Click here when Database operations are complete* button. See **Finish Database Operations and Restart** on page **48** for more information.

Reconnect the Database

The Connect database button is used to reconnect the database to the MS SQL Server Express database engine.

1. Click the *Database* tab.
2. Click the *Reconnect database* button.
3. If you have completed all database operations you want to perform at this time, click the *Click here when Database operations are complete* button. See **Finish Database Operations and Restart** on page **48** for more information.

Finish Database Operations and Restart

Once you have completed all database operations you want to perform at this time, click the Click here when Database operations are complete button. This will cause HandNet-lite to exit. When you restart HandNet-lite it will take the following actions:

1. If a database is currently attached, HandNet Lite will use that database.
2. If a database is not currently attached, but database files exist, HandNet Lite will reattach the database files and continue.
3. If a database is not currently attached, and there is no database file, HandNet Lite will create a new database.

Appendix A

Table A.1: Card Formats

Type	Format	Description	Format detail
Wiegand formats	1	WC01 26 bit: 16 bit ID	Facility code: 8 bits, bit 2-9 ID: 16 bits, bit 10-25 1 2 12345678901234567890123456 PFFFFFFFFFIIIIIIIIIIIIIIIIP EXXXXXXXXXXXX..... .....XXXXXXXXXXXXO
	2	WC02 32 bit: 22 bit ID	Facility code: 8 bits, bit 2-9 ID: 22 bits, bit 10-31 1 2 3 12345678901234567890123456789012 PFFFFFFFFFIIIIIIIIIIIIIIIIIIIIIIP EXXXXXXXXXXXXXXX..... .....XXXXXXXXXXXXXXXO
	3	WC03 34 bit: 16 bit ID	Facility code: 16 bits, bit 2-17 ID: 16 bits, bit 18-33 1 2 3 1234567890123456789012345678901234 PFFFFFFFFFFFFFFFFIIIIIIIIIIIIIIIIP EXXXXXXXXXXXXXXXX..... .....XXXXXXXXXXXXXXXXA
	4	WC04 34 bit: 20 bit ID	Facility code: 12 bits, bit 2-13 ID: 20 bits, bit 14-33 1 2 3 1234567890123456789012345678901234 PFFFFFFFFFFFFIIIIIIIIIIIIIIIIIIIP EXXXXXXXXXXXXXXXX..... .....XXXXXXXXXXXXXXXXO
	5	WC05 34 bit: 32 bit ID	ID: 32 bits, bit 2-33 1 2 3 1234567890123456789012345678901234 PIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIP EXXXXXXXXXXXXXXXX..... .....XXXXXXXXXXXXXXXXO
	6	WC06 35 bit: 20 bit ID	Facility code: 12 bits, bit 3-14 ID: 20 bits, bit 15-34 1 2 3 12345678901234567890123456789012345 PPFFFFFFFFFFFFIIIIIIIIIIIIIIIIIIIIP .EXX.XX.XX.XX.XX.XX.XX.XX.XX.XX.XX. .XX.XX.XX.XX.XX.XX.XX.XX.XX.XX.XX.O OXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
	7	WC07 37 bit: 19 bit ID	Facility code: 16 bits, bit 2-17 ID: 19 bits, bit 18-36 1 2 3 123456789012345678901234567890123456 7 PFFFFFFFFFFFFFFFFIIIIIIIIIIIIIIIIIIP EXXXXXXXXXXXXXXXXX..... .....XXXXXXXXXXXXXXXXXO
	8	WC08 37 bit: 35 bit ID	ID: 35 bits, bit 2-36 1 2 3 123456789012345678901234567890123456 7 PIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIP EXXXXXXXXXXXXXXXXX..... .....XXXXXXXXXXXXXXXXXO

Table A.1: Card Formats			
Type	**Format**	**Description**	**Format detail**
MagStripe formats	9	MS09 MAG1	ABA Track 2 Input ID len 25 Output min len 1 Output max len 25 Do trim leading zeroes Oriented right, no offset
	10	MS10 MAG2	ABA Track 2 Input ID len 25 Output min len 1 Output max len 25 Do trim leading zeroes Oriented left, no offset
	11	MS11 MAG3 Octal 7	ABA Track 2 Input ID len 7 Output min len 1 Output max len 25 Do trim leading zeroes Oriented right, no offset MS11 MAG3 Octal 7 is the format used for FingerKeys with a ProxIF reader.
	12	MS12 MAG 6 AT 5	ABA Track 2 Input ID len 6 Output min len 1 Output max len 25 Do trim leading zeroes Oriented left, offset 5

While these are the most common formats, you can define any additional formats that you need. See **Managing FingerKey Card Formats** on page **31** for more information.

Custom Splash Screen

1. Shut down HandNet Lite
2. Create a bitmap (.bmp) image that is 100 x 100 pixels.
3. Save the image to the program directory: C:\Program Files\Schlage\HandNet_Lite\Splash100x100.bmp. This path may vary depending on your individual installation.
4. Restart HandNet Lite. The image should appear on the splash screen.

Index

Symbols

A

B

C

D

E

T

U

V

W

About Allegion

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

For more, visit **www.allegion.com**.

aptiQ ■ LCN ■ SCHLAGE ■ STEELCRAFT ■ VON DUPRIN

70100-6210, Rev. 09/14
www.allegion.com/us

ALLEGION™