

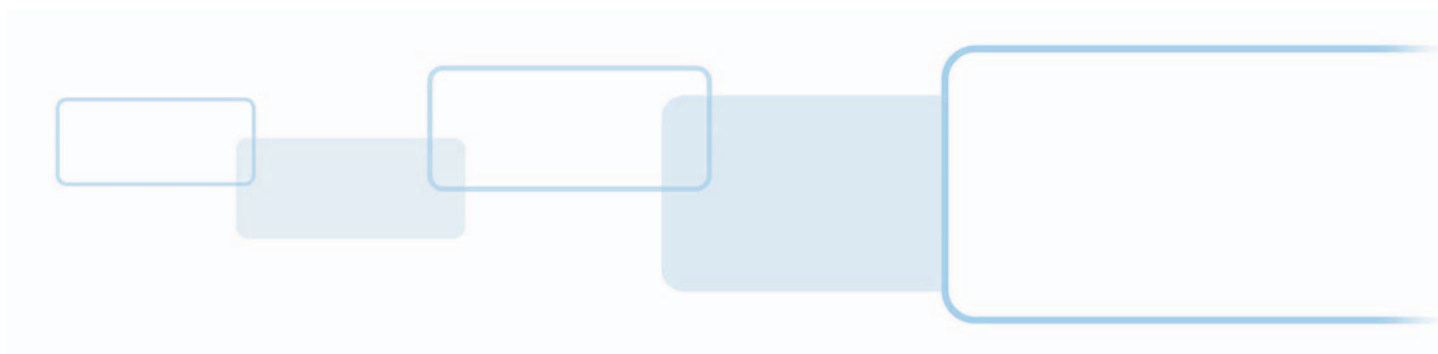
ICLASS SE[®] RB25F

BIOMETRIC READER/CONTROLLER

ADMINISTRATION GUIDE

PLT-04029, Rev. A.0

February 2019



Copyright

© 2019 HID Global Corporation/ASSA ABLOY AB. All rights reserved.

This document may not be reproduced, disseminated or republished in any form without the prior written permission of HID Global Corporation.

Trademarks

HID GLOBAL, HID, the HID Brick logo, the Chain Design, HID Biometric Manager, iCLASS SE and Seos are trademarks or registered trademarks of HID Global, ASSA ABLOY AB, or its affiliate(s) in the US and other countries and may not be used without permission. All other trademarks, service marks, and product or service names are trademarks or registered trademarks of their respective owners.

Revision history

Date	Description	Revision
February 2019	Initial release.	A.0

Contacts

For additional offices around the world, see www.hidglobal.com/contact/corporate-offices

Americas and Corporate

611 Center Ridge Drive
Austin, TX 78753
USA
Phone:866 607 7339
Fax:949 732 2120

Asia Pacific

19/F 625 King's Road
North Point, Island East
Hong Kong
Phone:852 3160 9833
Fax:852 3160 4809

Europe, Middle East and Africa (EMEA)

Haverhill Business Park Phoenix Road
Haverhill, Suffolk CB9 7AE
England
Phone:44 (0) 1440 711 822
Fax:44 (0) 1440 714 840

Brazil

Condomínio Business Center
Av. Ermano Marchetti, 1435
Galpão A2 - CEP 05038-001
Lapa - São Paulo / SP
Brazil
Phone: +55 11 5514-7100

HID Global Technical Support: www.hidglobal.com/support



Contents

Section 1: Introduction	5
1.1 Document purpose	5
1.2 Intended audience	5
1.3 Physical Access Control System overview	6
1.4 HID Biometric Manager	7
1.4.1 Credential Database	7
1.4.2 Data Import	7
1.4.3 Reader Service	7
1.5 Browser compatible device	7
1.6 RB25F	7
1.7 Panels and Door Controllers	7
1.8 Network setup examples	9
Section 2: RB25F Biometric Reader/Controller	11
2.1 RB25F hardware specifications	11
2.1.1 Biometric specifications	11
2.2 RB25F wiring function and color codes	12
2.3 System connections	13
2.3.1 Power supply connection	13
2.3.2 Network connection	13
2.3.3 Standalone operating mode connections	14
2.4 Hardware reset the RB25F	15
Section 3: HID Biometric Manager	17
3.1 HID Biometric Manager overview	17
3.1.1 Server hardware requirements	17
3.1.2 TCP Port usage	17
3.2 HID Biometric Manager initial setup	18
3.2.1 HID Biometric Manager software install	18
3.2.2 HID Biometric Manager initial login	20
3.2.3 Change default admin password	21
3.2.4 Configure time zone setting	23
3.2.5 Configure software/firmware update settings	25

3.2.6 Create Biometric Manager operators	28
3.3 Device profiles	30
3.3.1 Edit a device profile	30
3.3.2 Create a device profile.	33
3.3.3 Delete a device profile.	35
3.4 Device installation and configuration	36
3.4.1 Configure device settings	38
3.4.2 Reset a device	41
3.4.3 Uninstall a device	42
3.5 Enrollment	43
3.5.1 Enroll People.	43
3.5.2 Enroll Cards	45
3.5.3 Enroll Biometrics.	49
3.6 Write fingerprint templates to a card.	52
3.7 View Biometric Manager events.	54
Appendix A: Fingerprint enrollment guidelines.	55
A.1 General guidelines.	55
A.2 Fingerprint enrollment best practices for RB25F	56
Appendix B: Acronyms and terminology	59



Section 1

1 Introduction

1.1 Document purpose

This document gives an overview of the iCLASS SE® RB25F Biometric Reader/Controller within a biometric access system environment and provides reference information relating to the connection options for RB25F devices.

The document also provides procedures for administrations to install and setup HID® Biometric Manager™ and procedures for Biometric Manager operators to carry out tasks associated with RB25F device installation, people enrollment, and credential/biometric data management.

1.2 Intended audience

This document is intended for personnel performing the following roles:

- **RB25F device installers:** The document provides reference information relating to the iCLASS SE® RB25F Biometric Reader/Controller, RB25F wiring specification and RB25F wiring options.
- **HID Biometric Manager administrator:** The document provides procedural information for the default administrator to initially setup and configure the HID Biometric Manager application.
- **HID Biometric Manager operators:** The document provides procedural information for HID Biometric Manager operators to install and configure network detected RB25F devices, enroll people in the system, add credentials and biometric data.

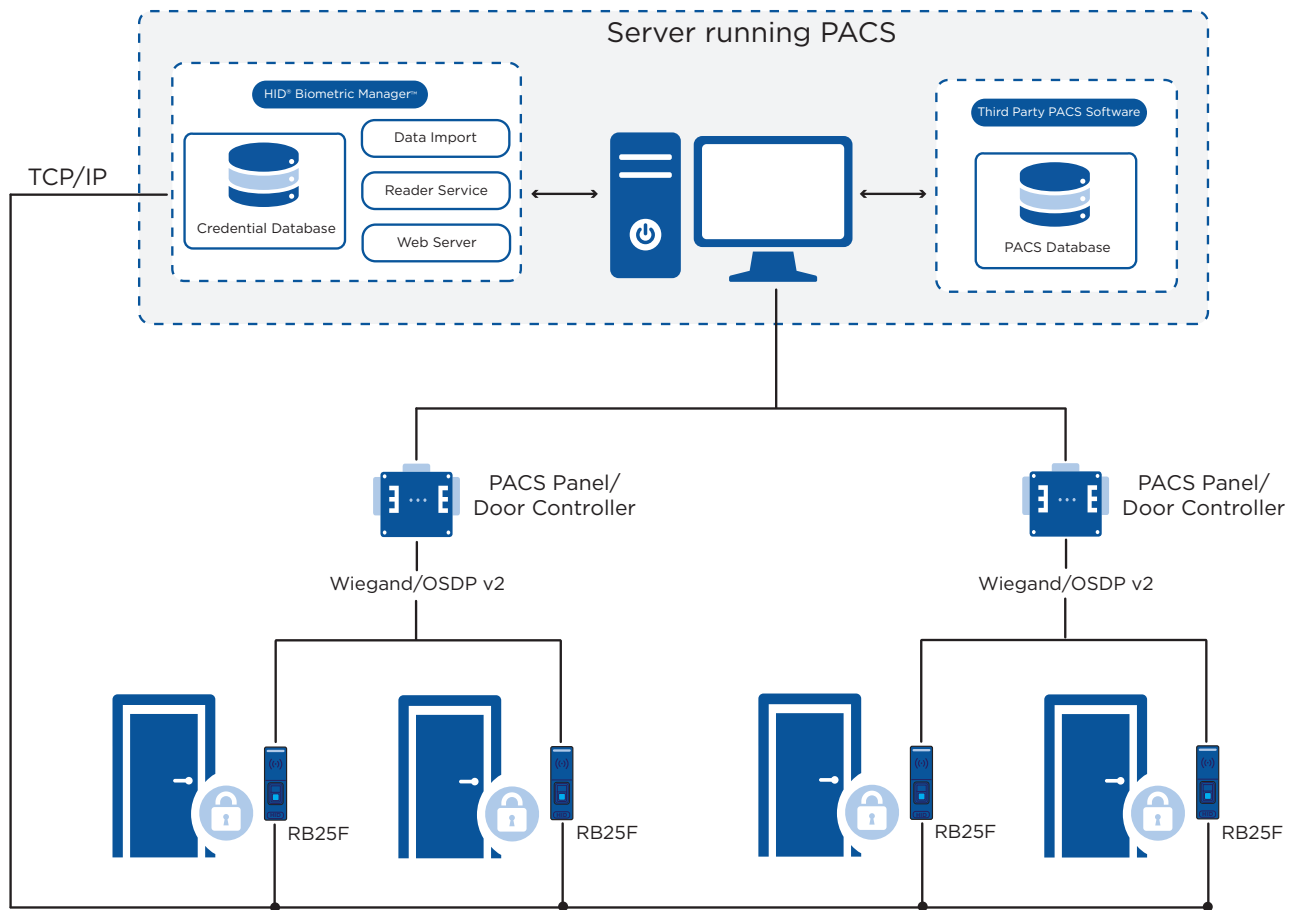
1.3 Physical Access Control System overview

A Physical Access Control System (PACS) provides services for enrolling card holders, assigning access rights, configuring access points and their associated access criteria, monitoring, and reporting. These components are focused on access authorization. The HID Biometric Manager and RB25F solution components are designed to be integrated into the PACS to provide strong authentication at access points.

When a card holder presents their credential to a RB25F access point reader, it performs authentication functions to establish whether the user is who he/she claims to be. If the authentication is successful the PACS panel or controller is notified of the request for access. The panel then checks the access rights for the presented credential to see if the card holder is authorized for access. If authorization is successful it opens the door.

The diagram below provides a high level view of the various system solution components as deployed within a PACS. The function of each component is described in the following sub sections. The components with HID Biometric Manager service box are typically deployed on the same server as the PACS headend software.

Note: Multiple RB25F devices and PACS Panel/Door Controllers can be added. HID Biometric Manager can control up to 2,000 RB25F devices.





1.4 HID Biometric Manager

The HID Biometric Manager is an application that acts as both a web server and a container for background tasks and jobs.

The web server allows browser compatible devices to configure RB25F device settings, register credential holders, and to distribute this information to the devices. It also collects and stores logged events from the RB25F.

1.4.1 Credential Database

The Credential Database is a SQL database that the PACS Service uses to store the credential data that has been gathered through manual registration or Data Import. It also stores configuration data and transaction logs for all installed RB25F devices.

1.4.2 Data Import

The HID Biometric Manager Data Import component allows credential and credential holder information to be imported into the HID Biometric Manager database from a third party PACS headend. This ensures that the output of the RB25F matches expected input of the third party controller.

1.4.3 Reader Service

This runs as a background service and automatically synchronizes data between the HID Biometric Manager and the RB25F devices.

1.5 Browser compatible device

The HID Biometric Manager provides a web server which supplies content to any device which supports a compatible browser and is accessible on the network.

This interface is used to install and configure RB25F readers. It is also used to perform user registration including fingerprint enrollment. Any one of the RB25F devices can be selected as the enrollments device from the browser.

Other functions include the ability to view transactions on the device in real time, and to download and trigger updates for both the HID Biometric Manager software and the RB25F device firmware.

1.6 RB25F

The RB25F is a biometric card and fingerprint reader. It authenticates users according to one of four methods as configured by the HID Biometric Manager. These are fingerprint only, card only, and two variations of card with finger. One stores the fingerprint data on the card, the other stores the fingerprint data on the RB25F device.

When the credential holder is authenticated, the data is output to a third party controller.

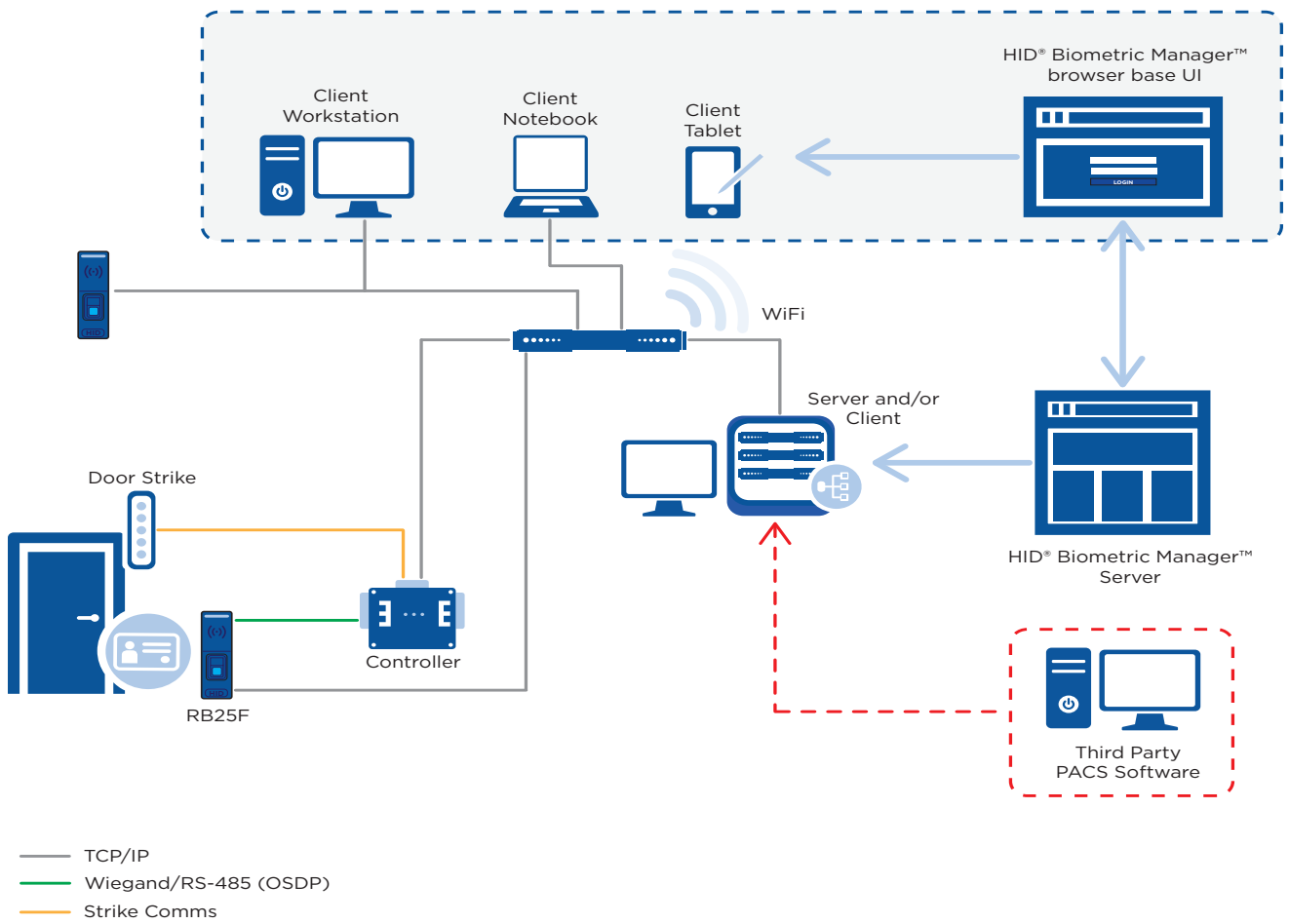
1.7 Panels and Door Controllers

These components are standard PACS hardware panels that are wired to door sensors and controls, card readers, and general digital input and output to control and monitor other security devices. They make access decisions based on credential IDs and, similar to the pivCLASS Authentication Module (PAM), are designed to continue functioning when communication with the PACS headend is interrupted. A PACS panel makes an authorization decision about whether the credential has access rights to a particular area. The authorization decision is made after the authentication is successfully completed by the RB25F which ensures the credential is authentic.

The following diagram shows an example of the system.

Note:

- The entire system is located inside the firewall.
- Multiple RB25F devices and PACS Panel/Door Controllers can be added. HID Biometric Manager can control up to 2,000 RB25F devices.





1.8 Network setup examples

The HID Biometric Manager installation wizard is expected to cope with the vast majority of network configurations. When using Biometric Manager during discovery and installation of RB25F devices, it defaults to hostname RB25F Server.

Scenario 1 - DHCP network, RB25F devices have dynamic IP, Server has a static IP

In this system setup the server has a static IP or the DHCP server assigns an IP with a permanent lease.

RB25F devices have an Ethernet connection on the same LAN as the server running Biometric Manager. The network is configured so that the DHCP server dynamically assigns IPs (which may have a limited lease time) to RB25F.

Scenario 2 - DHCP network, RB25F devices have dynamic IP, Server has a dynamic IP

In this system setup the server has a DHCP assigned IP.

RB25F devices have an Ethernet connection on the same LAN as the server running Biometric Manager. The network is configured so that the DHCP server dynamically assigns IPs (which may or may not have limited lease time).

HID Biometric Manager is installed on the server using the setup install wizard. During installation of RB25F devices in Biometric Manager, you must select and use the default server hostname. In the event where the server IP address changes, the hostname will reflect back to the server hostname.

Note: Setting HID Biometric Manager to a static IP will cause issues on this network.

Scenario 3 - Biometric manager installed on a PC and connects to DHCP network

This is the same as Scenario 2 except HID Biometric Manager is running on a PC. This means that it is likely that Biometric Manager will not be running all the time. When Biometric Manager is not running, RB25F devices will be in an off-line mode. In off-line mode they will run as configured and log events, however enrollment will not be possible.

Scenario 4 - Network without DHCP

In this system setup HID Biometric Manager is installed on the server or PC using the setup install wizard. The RB25F device discovery and installation process will assign a static IP address and hostname. During installation of the device in Biometric Manager you must select and use the server hostname. In the event where the server IP address changes, the hostname will reflect back to the server hostname.

Note: Setting HID Biometric Manager to a static IP will cause issues on this network.

This page is intentionally left blank.

Section 2

2 RB25F Biometric Reader/Controller

This section provides reference information relating to the iCLASS SE® RB25F Biometric Reader/Controller, RB25F wiring functions and color codes, as well as RB25F system connection options.

2.1 RB25F hardware specifications

For more detailed information relating to RB25F specifications refer to the *iCLASS SE® RB25F Biometric Reader/Controller* product data sheet.

RB25F	Specification
Mounting	Mullion size mounted on door or any flat surface
Dimensions (width x length x depth)	1.93" x 7.95" x 2.17" (4.9 cm x 20.2 cm x 5.5 cm)
Product Weight (g)	13.04 oz (0.38 kg)
Operating Voltage Range (VDC)	12V DC
Operating Temperature	-4° F to 153° F (-20° C to 66° C)
Environmental Rating	IP67 Indoor/Outdoor and IK09 Impact Ratings
CPU and Memory	64 bit, 1.2 GB, Quad Core CPU. 8GB storage and 1 GB RAM
Panel connection	Pigtail, 18" (45.72 cm)
Communications	Ethernet (10/100), Wiegand, Open Supervised Device Protocol (OSDP) via RS485

2.1.1 Biometric specifications

Biometric feature	Specification
Image resolution / bit depth / Image area	500 dpi / 8 bit, 256 grayscale / 272 x 320 pixels
Template output format	ANSI 378 or ISO 19794-2
Supported users on device	Up to 250,000 users
1:1 Fingerprint Verification Authentication	Max. 50,000 users
1:N Fingerprint Identification Authentication	Max. 5,000 users
Card holders	Max. 250,000
Events storage	1,000,000
Live Finger Detection	Supported

2.2 RB25F wiring function and color codes

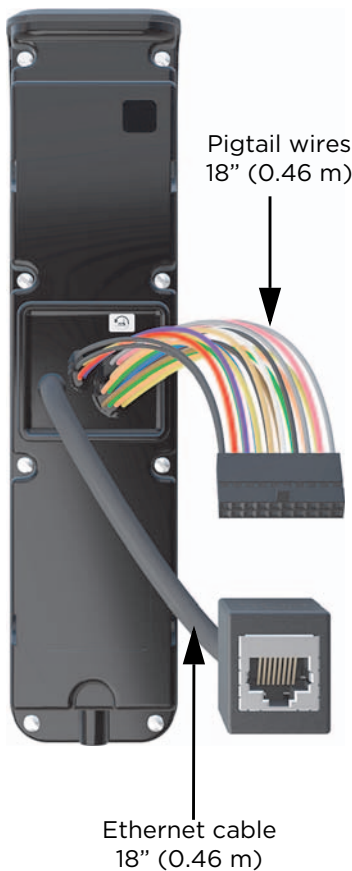
The following shows RB25F wiring functions and color codes.

IMPORTANT: The 19 pigtail wires should be cut to size for wall mounted installations. DO NOT cut the Ethernet cable.



CAUTION

Wiring the reader incorrectly may cause permanent damage the reader.



Function group	Wire color	Function	AWG	Max. length ¹
RS-485	Green	RS-485 A	24	4,000 ft (1,219 m)
	Tan	RS-485 B		
	Black	RS-485 Ground		
Relay (Reserved for future use)	Gray	Relay - Common	22	500 ft (152 m)
	Yellow	Relay - Normally Open		
	Orange	Relay - Normally Closed		
Inputs (Reserved for future use)	Pink	REX Input (TTL)		
	Gray	DPS Input (Supervised)		
	Black	Input Ground		
Wiegand Port	Green	D0		
	White	D1		
	Brown	RED		
	Orange	GREEN		
	Yellow	BUZ		
	Blue	HOLD		
	Violet	TPR		
DC Power	Black	Ground		
	Red	Power +12 V		

Function group	Connector	Function	Cable	Max. length
Network	RJ45 socket	Ethernet	CAT5/5E/6	328 ft (100 m)

¹RS-485 = Max. bus length: 4,000 ft - 24 AWG (1,219 m)

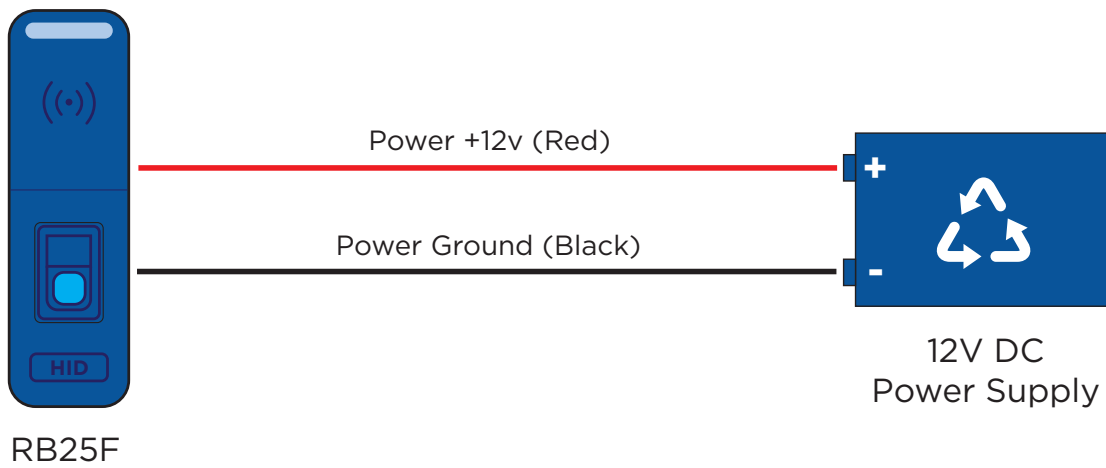
Max. length between nodes: 1,640 ft - 24 AWG (500 m)

2.3 System connections

2.3.1 Power supply connection

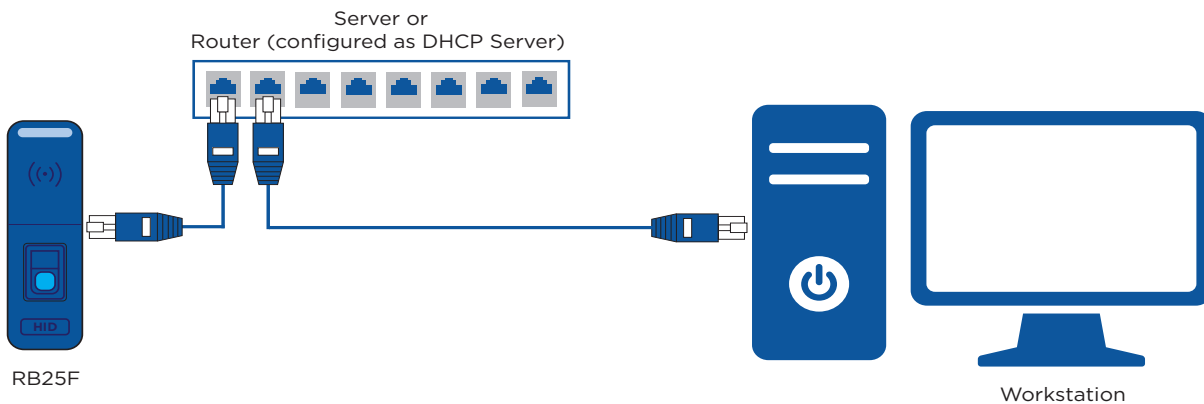
For the RB25F power supply use a 12V DC power supply adapter capable of at least 2A, with IEC/EN 60950-1 approval. If additional power consuming devices are included, make sure to use a power adapter that is able to supply the total current needed.

Note: It is best practice to use separate power supplies for the RB25F and the electric locks.



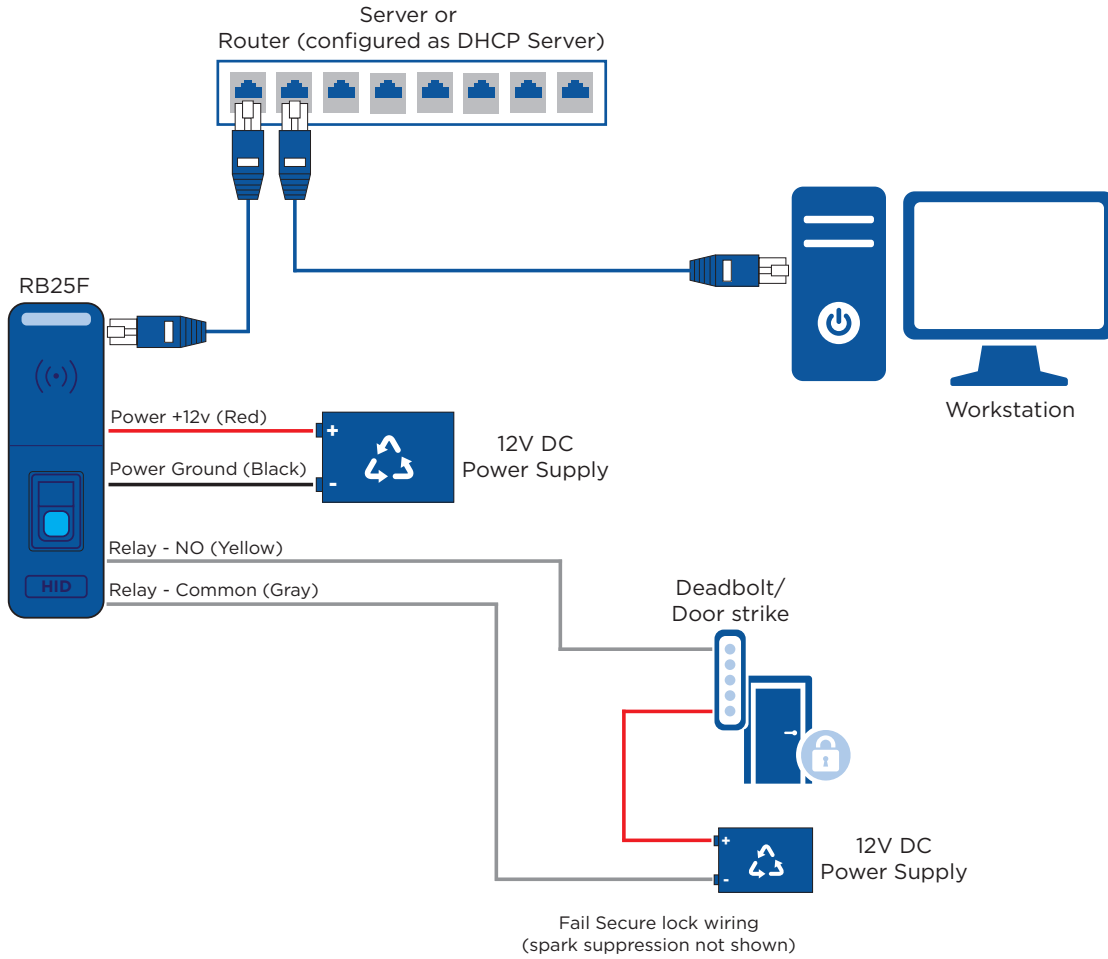
2.3.2 Network connection

Network connection to a network that has a server or a router configured for DHCP.



2.3.3 Standalone operating mode connections

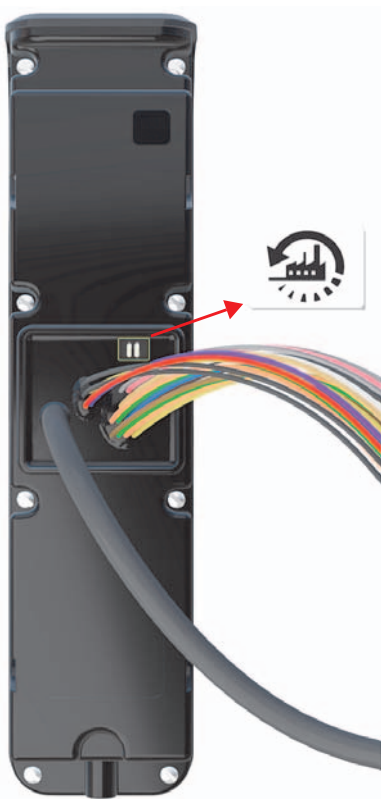
RB25F devices can be used in standalone operating mode without any additional I/O devices.



2.4 Hardware reset the RB25F

Resetting the RB25F device to factory defaults should, where possible, be carried out through the HID Biometric Manager application, see *Section 3.4.2 Reset a device*. However, in the event where communication between HID Biometric Manager and the RB25F is not possible, carry out the following hardware reset at the reader:

1. Unscrew the installation locking screw from the bottom of the RB25F.
2. Remove the RB25F from the backplate.
3. From the back of the reader, remove the label that covers the contacts.



4. With power supplied to the reader, short the contacts together using a suitable metal object.
5. Maintain the short for a full five seconds. The RB25F will beep while you hold the short.
6. One long beep of two seconds confirms the reset.

All user data, firmware, IP settings, Host IP will be returned to the default. You will need to install and update the device in order to return it to the former working level.

This page is intentionally left blank.



Section 3

3 HID Biometric Manager

3.1 HID Biometric Manager overview

HID® Biometric Manager™ is a web application that streamlines the management and configuration of RB25F devices and allows application operators to manage people enrollment, credentials and fingerprint templates. HID Biometric Manager uses the following operator roles to control access to management tasks:

- **Super administrator:** The super administrator is the initial default user account (cannot be deleted). This operator installs and initially configures Biometric Manager software, and creates/administers operator roles within the application. See *Section 3.2 HID Biometric Manager initial setup*.
- **Administrator:** This operator role has full access to Biometric Manager web application with functions to:
 - Install and manage RB25F devices. See *Section 3.4 Device installation and configuration*.
 - Enroll people in the system, add credentials, collect and store associated biometric data. See *Section 3.5 Enrollment*.
- **Enrolment:** This operator role has full access to Biometric Manager web application, however is limited to the day-to-day activities of enrolling people in the system, adding credentials, collecting and storing associated biometric data. See *Section 3.5 Enrollment*.

3.1.1 Server hardware requirements

Server hardware requirements:

- Intel® i5 2.3 GHz
- RAM 8 GB
- Available Disk Space 20 GB
- Windows® 7 SP2 (Minimum), Windows® 10 (Preferred)

3.1.2 TCP Port usage

The following listed the TCP ports used by HID Biometric Manager:

- 1883 Communication (MQTT Broker)
- 61616 Communication (MQTT Broker)
- 80 REST (Initial MQTT Configuration)
- 10500 Device discovery
- 22 (SSH) Firmware upgrade

3.2 HID Biometric Manager initial setup

3.2.1 HID Biometric Manager software install

It is recommended that HID Biometric Manager is installed on a DHCP network server that automatically provides and assigns IP addresses, default gateways and other network parameters to client devices.

1. Download the **HID Biometric Manager.exe** file from the download site to your server:

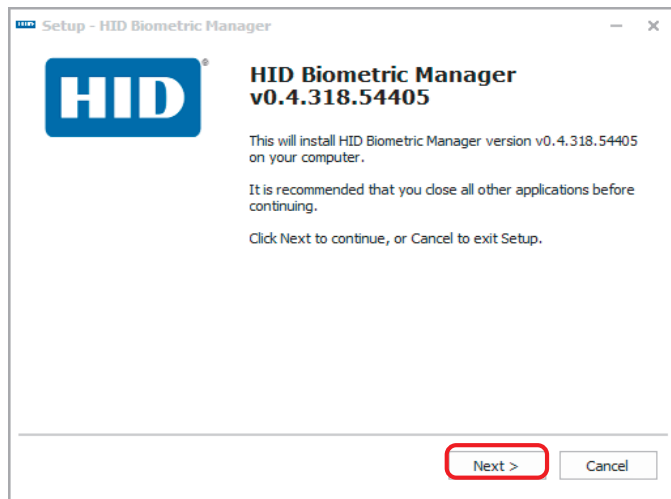
<https://www.hidglobal.com/rb25f>

2. Double-click on the **HID Biometric Manager.exe** file to launch the installation wizard.

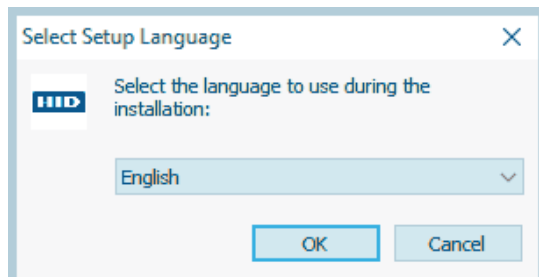
Note: If the server system language is configured to one of the supported languages then the install wizard instructions and Biometric Manager will automatically default to the server system language. Supported languages:

- English
- German
- Spanish
- French
- Italian
- Portuguese
- Russian
- Simplified Chinese
- Japanese
- Korean

3. On the initial installation wizard screen, click **Next**.

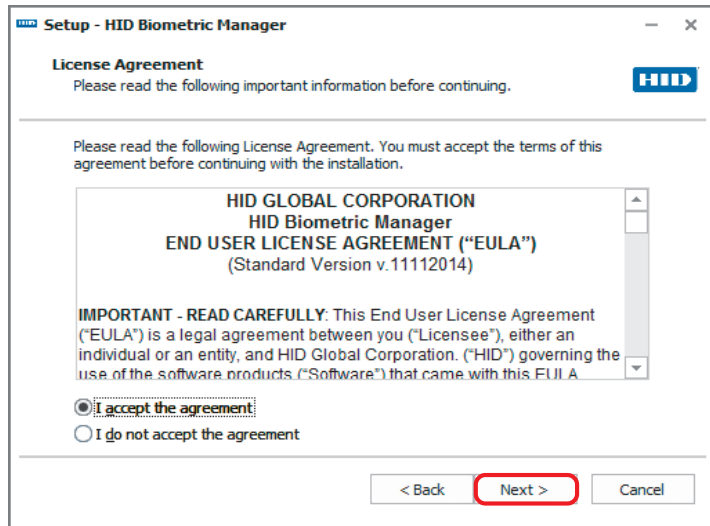


4. Select the HID Biometric language.

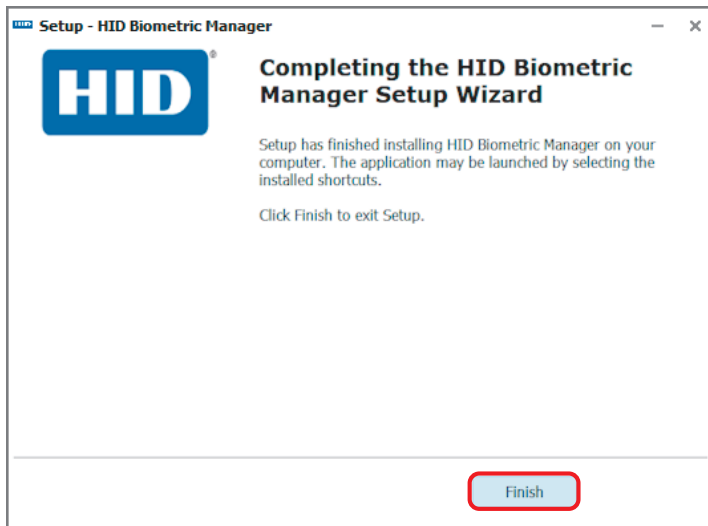


5. Read the License Agreement. Select **I accept the agreement**, and click **Next**.

Note: If you do not accept the License Agreement, click **Cancel** to end the installation setup process.



6. Follow the installation wizard prompts until the setup has finished installing HID Biometric Manager on your machine.



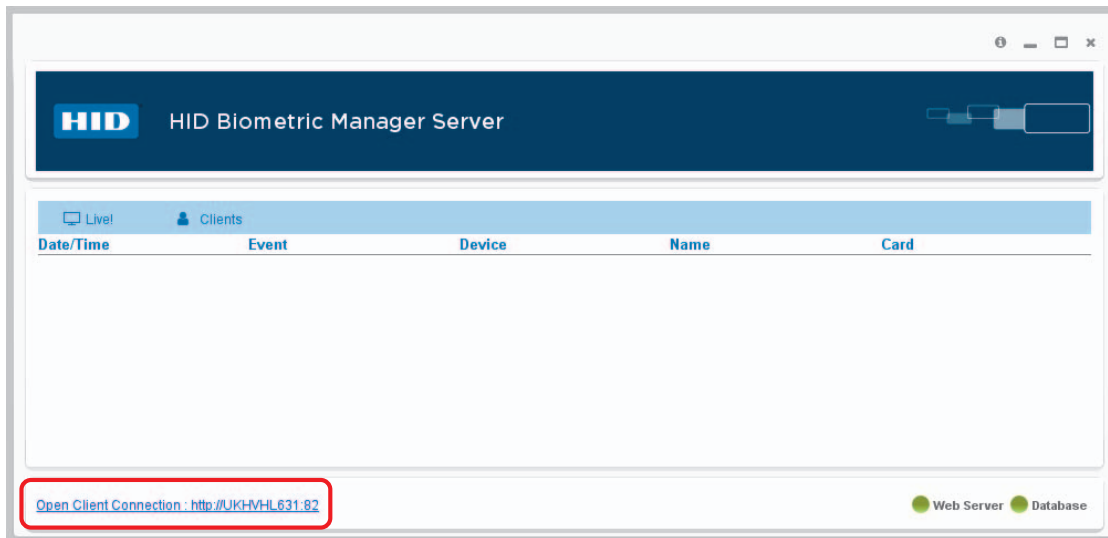
3.2.2 HID Biometric Manager initial login

On the server where HID Biometric Manager has been installed:

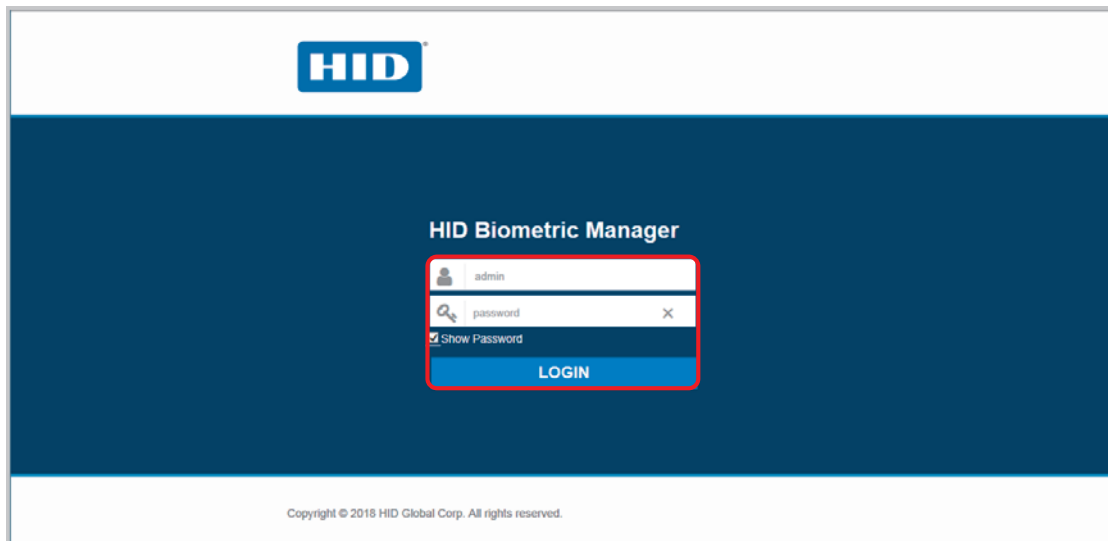
1. Double-click on the HID Biometric Manager desktop shortcut or navigate to the installation folder (usually, **C:\Program Files (x86)\HID Global\Biometric Manager**) and double-click on the **HID Biometric Manager.exe** file.
2. On the HID Biometric Manager Server application screen, click on the **Open Client Connection** link to access the HID Biometric Manager application login screen. Record the **Client Connection** link url as this can be distributed and used to access the HID Biometric Manager application from a client PC on the same network.

Note: If the **Open Client Connection** link url fails to connect to HID Biometric Manager due to a Port issue, change the default port number (443) in the link url to:

`http://hostname:82/HIDBiometric/HIDBiometricManager.html`



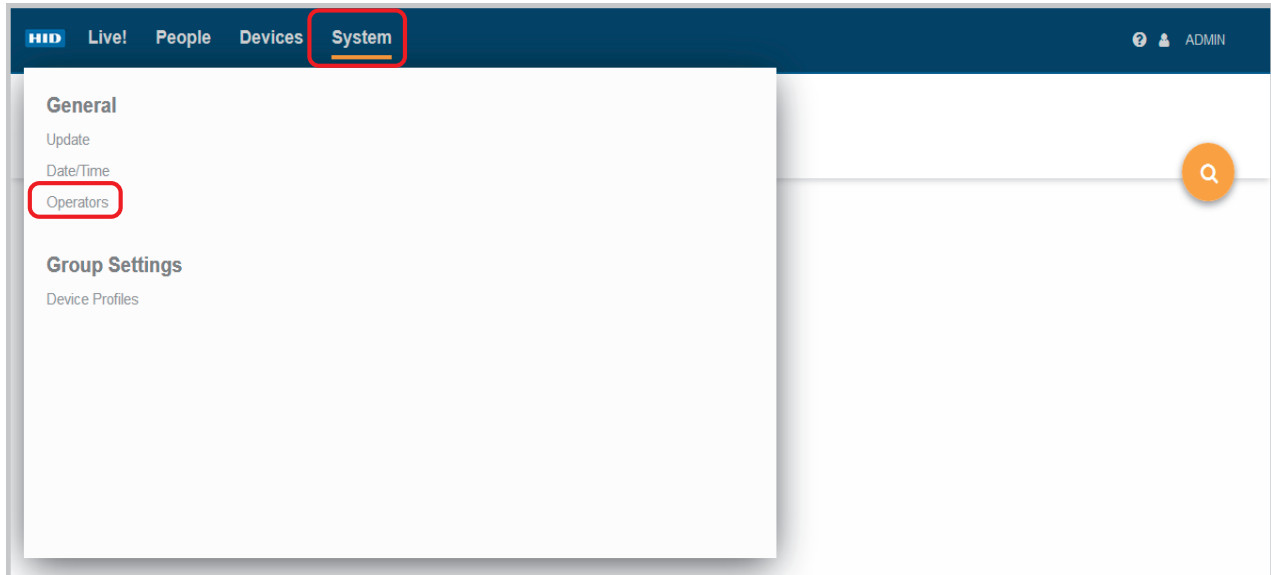
3. Enter the default User Name (**admin**) and Password (**password**) and click **LOGIN**.



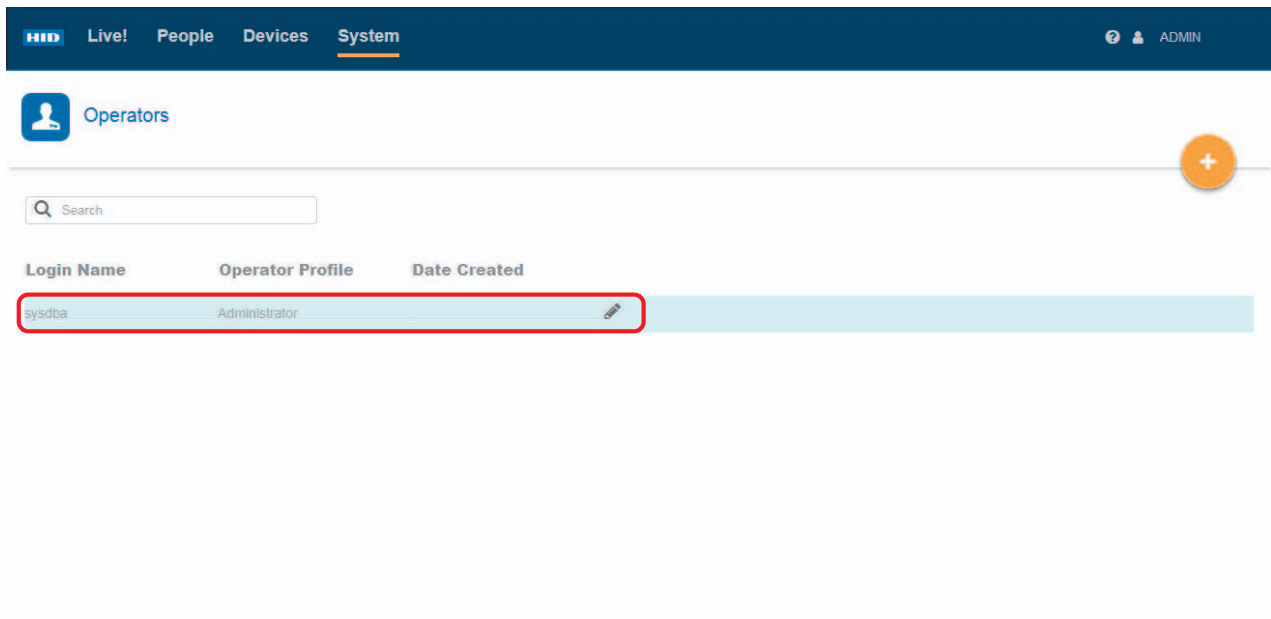
3.2.3 Change default admin password

For security reasons it is recommended that the default admin login credentials are immediately changed.

1. Click on the **System** option and select **Operators**.



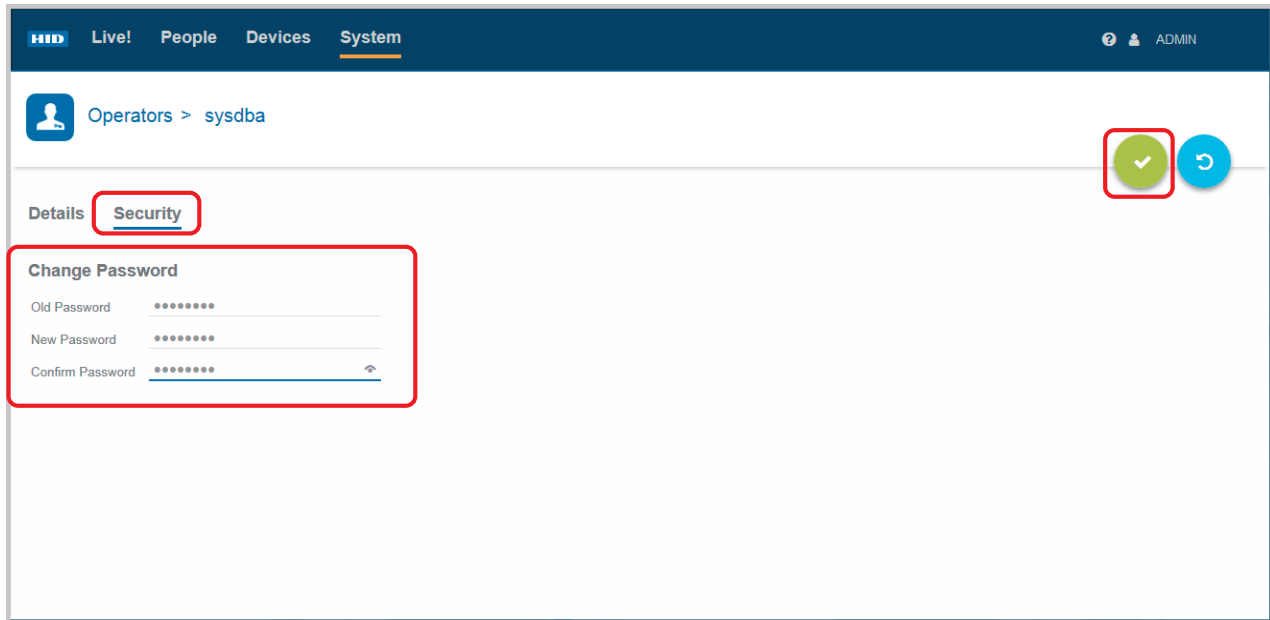
2. Click on the **Edit** icon [] associated with the displayed system admin user.



3. Select the **Security** option.
4. Under **Change Password**:
 - Enter the default **Old Password**.
 - Enter a **New Password**, then re-enter the new password to confirm.

Note: There are currently no password format rules. Clicking on the eye icon when entering the new password will display the password.

5. Click the **Save** icon to save this new password.

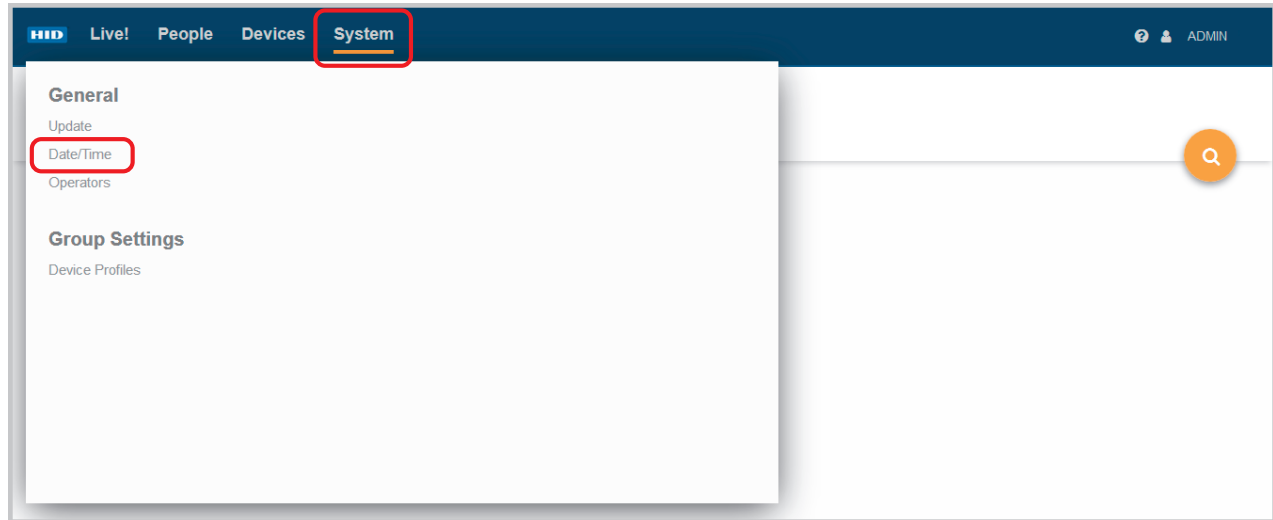


6. Exit HID Biometric Manager and login again using the default username (**admin**) and new password.

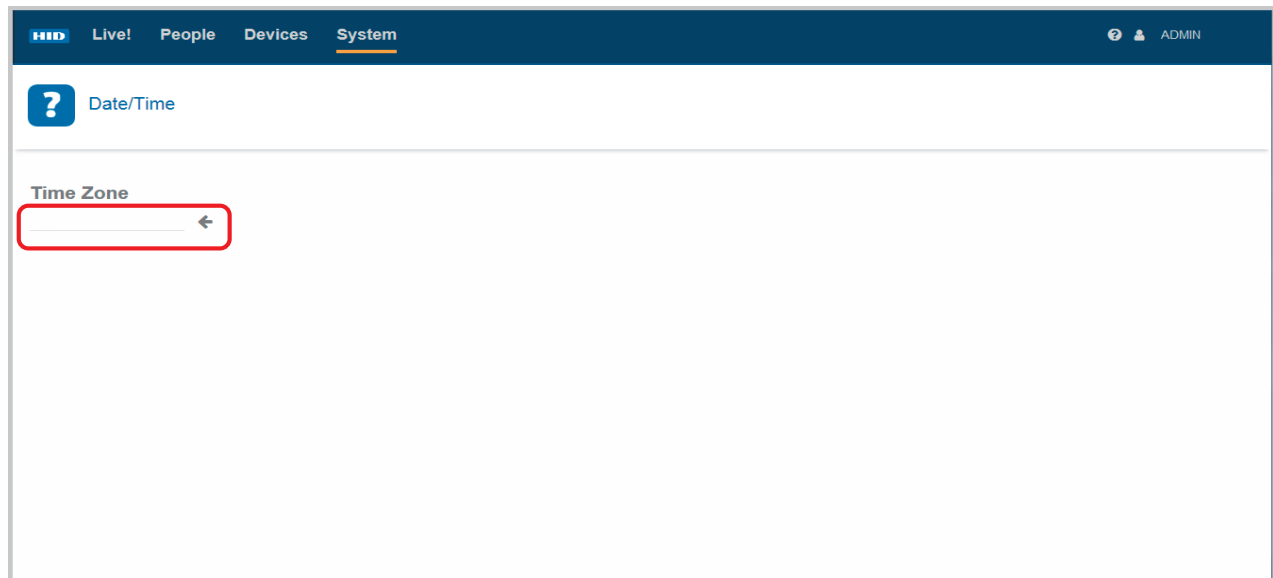
3.2.4 Configure time zone setting

Setting the time zone will configure the time zone for the instance of Biometric Manager running on the server.

1. Click on the **System** option.
2. Select the **Date/Time** option to access system time zone settings.

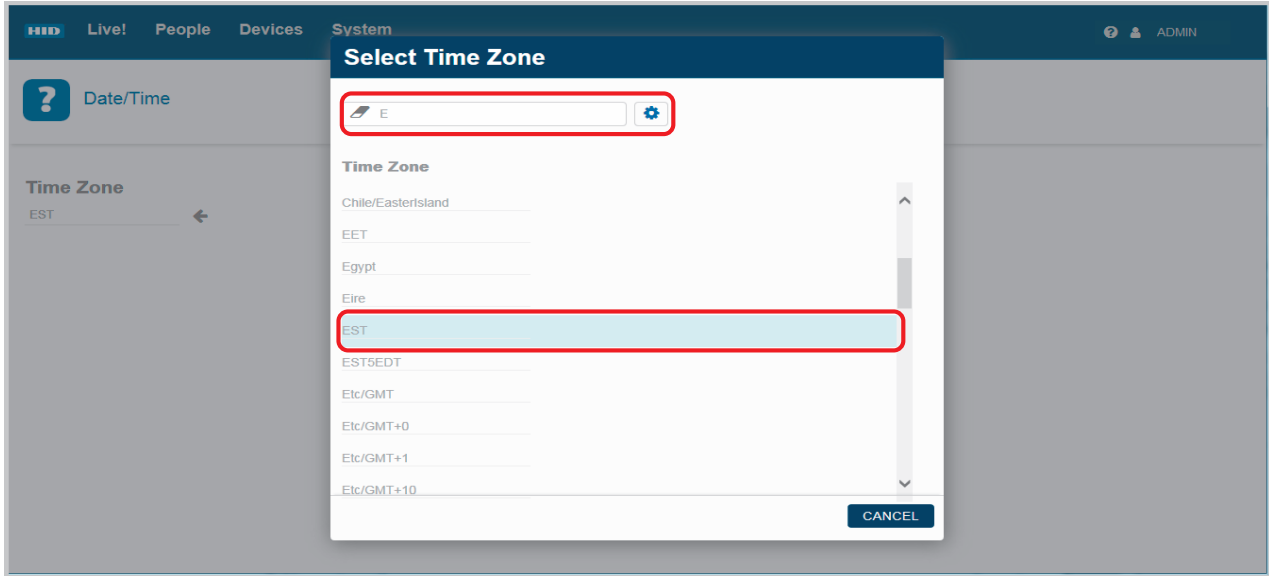


3. Select the **Time Zone** arrow icon to access a list of selectable time zones.

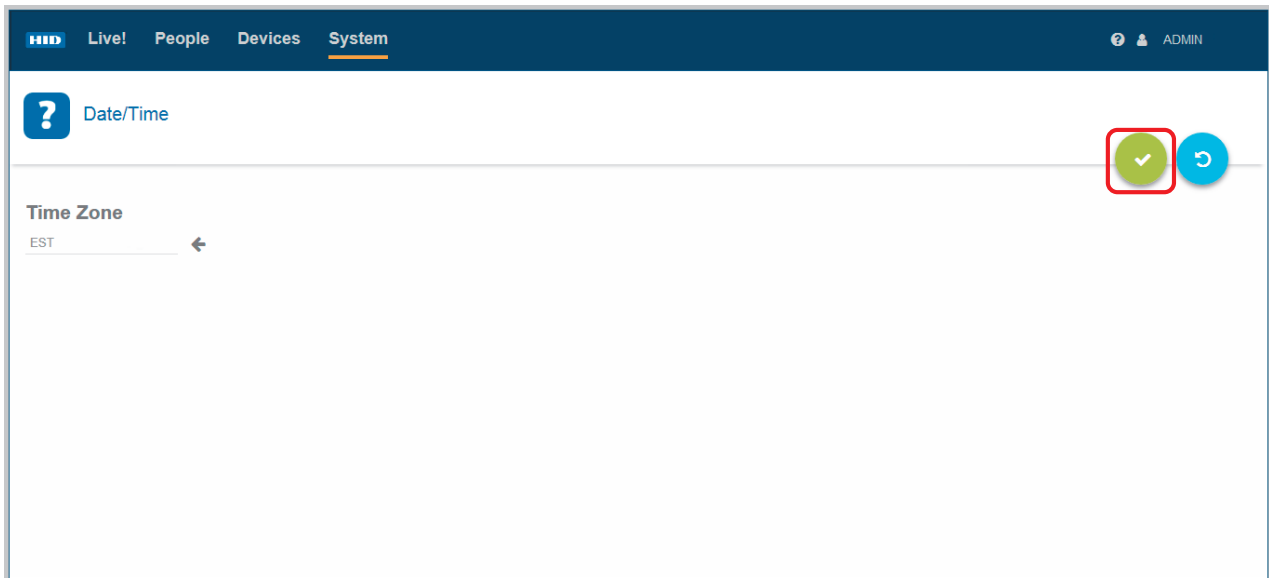


4. Select the desired Time Zone from the displayed list.

Note: Use the Search field to narrow your search criteria for a listed time zone.



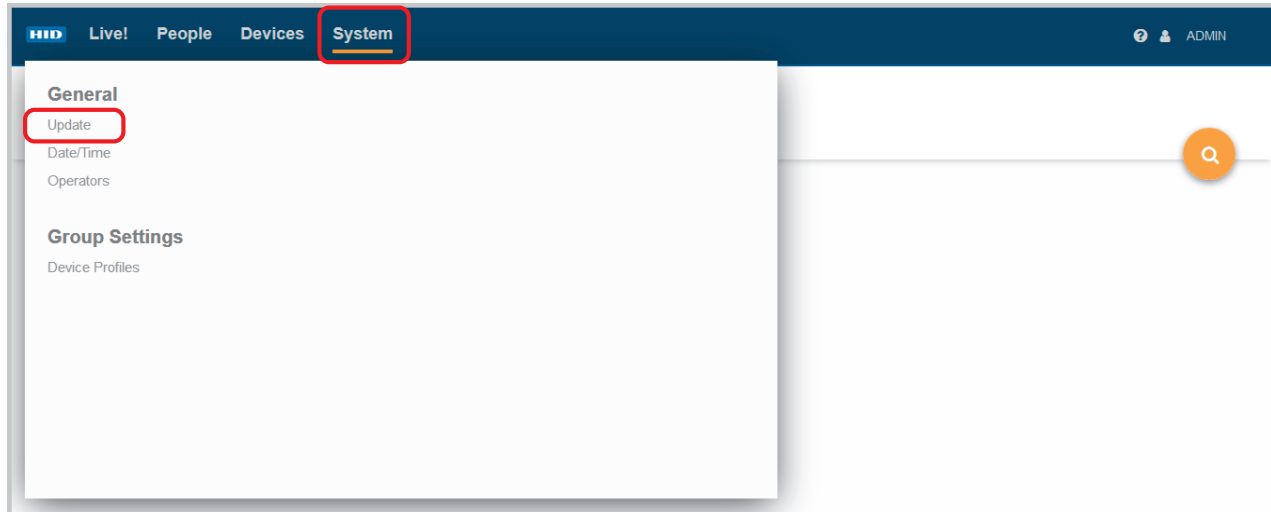
5. On the **Date/Time** screen click the **Save** icon to save your time zone setting.



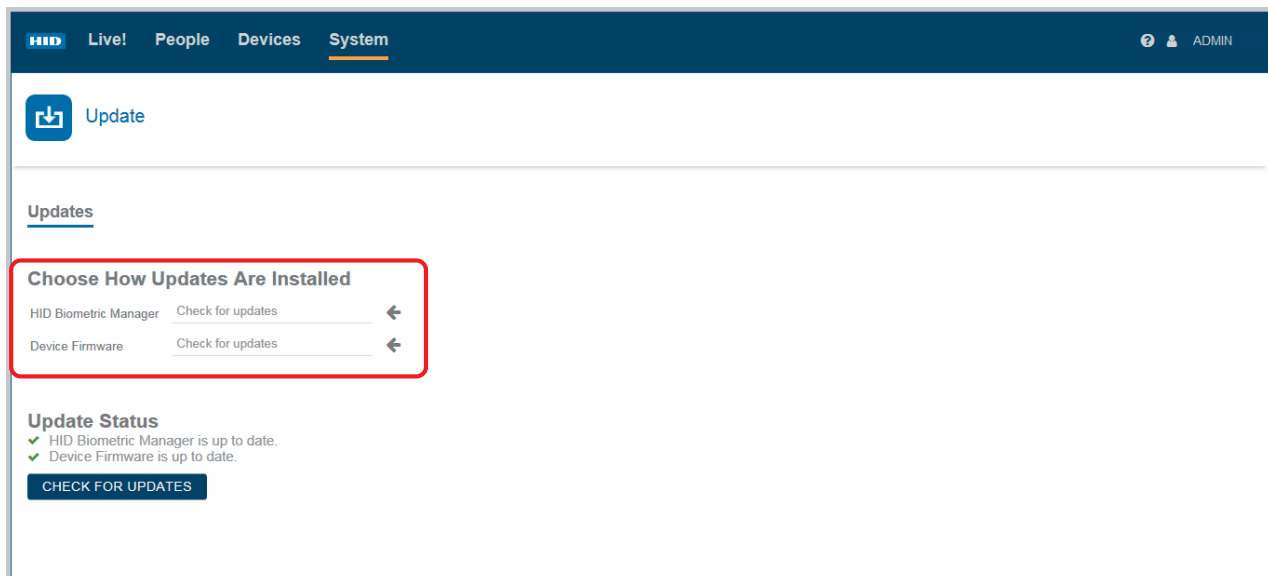
3.2.5 Configure software/firmware update settings

To configure how HID Biometric Manager software and device firmware are updated:

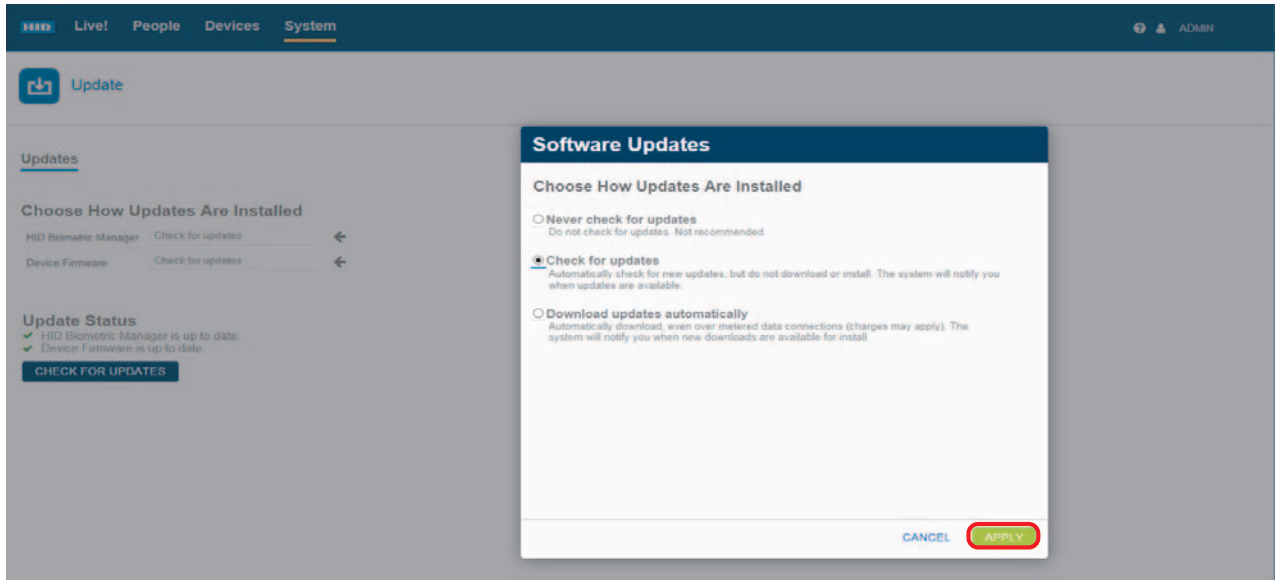
1. Click on the **System** option.
2. Select the **Update** option to access software and firmware update settings.



3. Select the arrow icon associated with:
 - **HID Biometric Manager:** To access options to configure how Biometric Manager software updates are installed.
 - **Device Firmware:** To access options to configure how device firmware updates are installed.

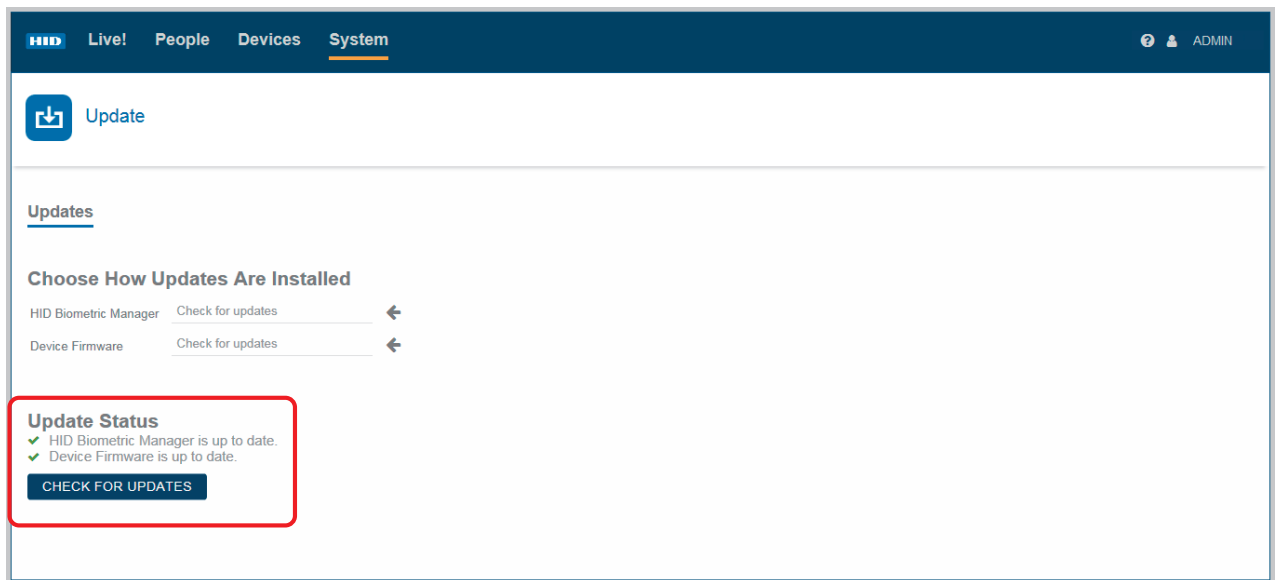


4. Select the desired update option and click **Apply**.

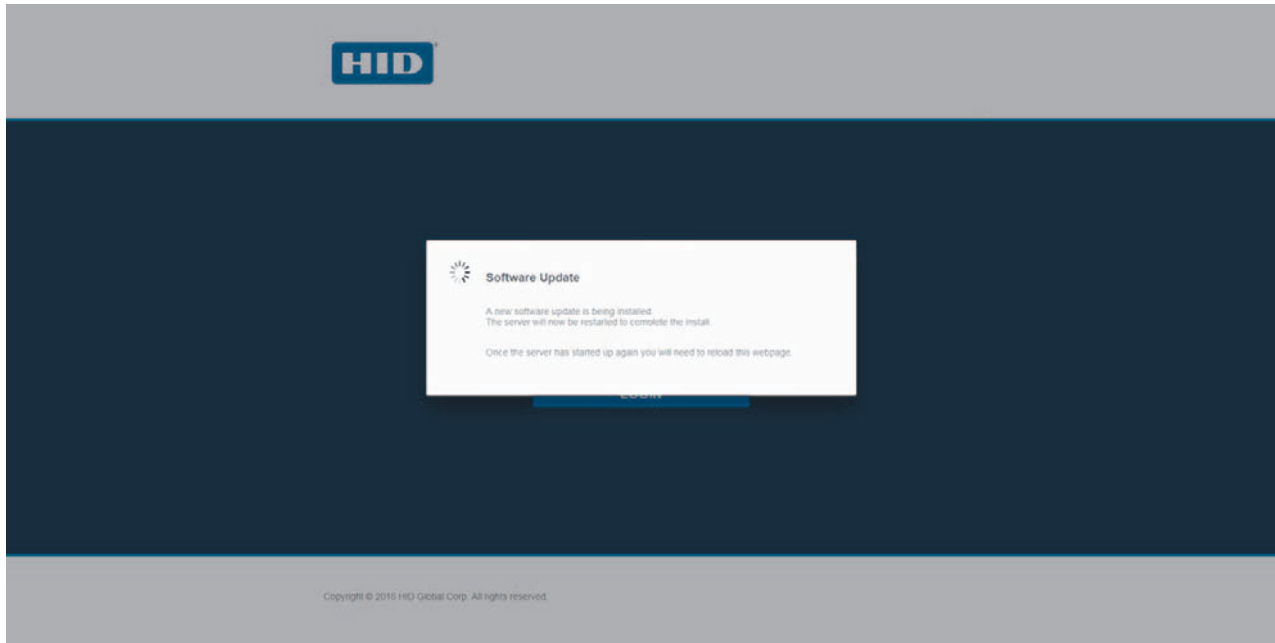


5. Click **CHECK FOR UPDATES** to check if software/firmware updates are available.

Note: Update Status information is displayed on the screen.



6. If new software is available and selected, the installation progress is displayed in your browser. Once the installation is complete the hid Biometric Manager Server application will automatically shut down and re-start and the following message is displayed.



7. Wait for the server application to re-start and then refresh the browser.
8. You will be prompted to log back into the HID Biometric Manager. The software update is now complete.

Note: Any previous shortcuts that were set up are not affected by the software update process.

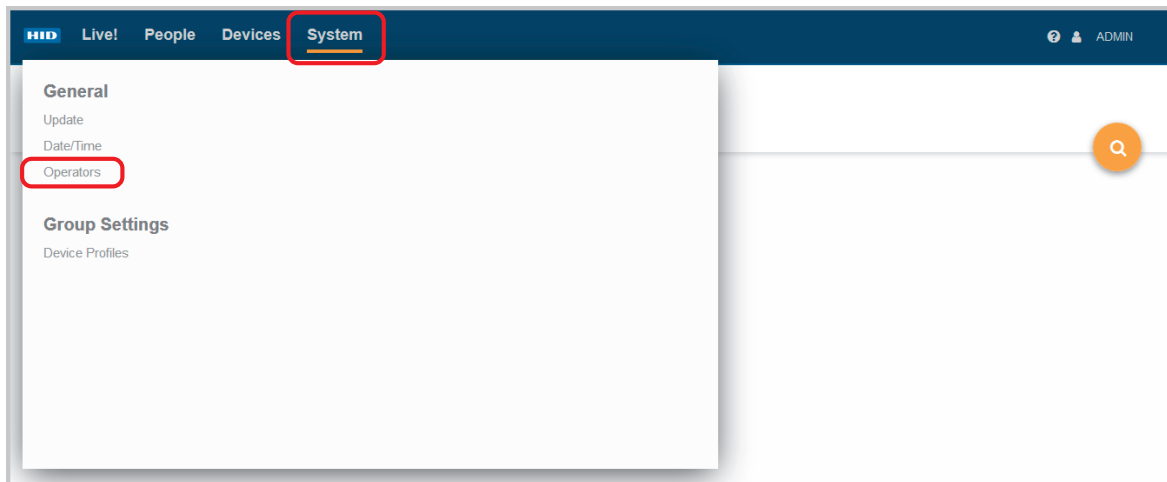
3.2.6 Create Biometric Manager operators

HID Biometric Manager uses the following operator roles to control access to management tasks:

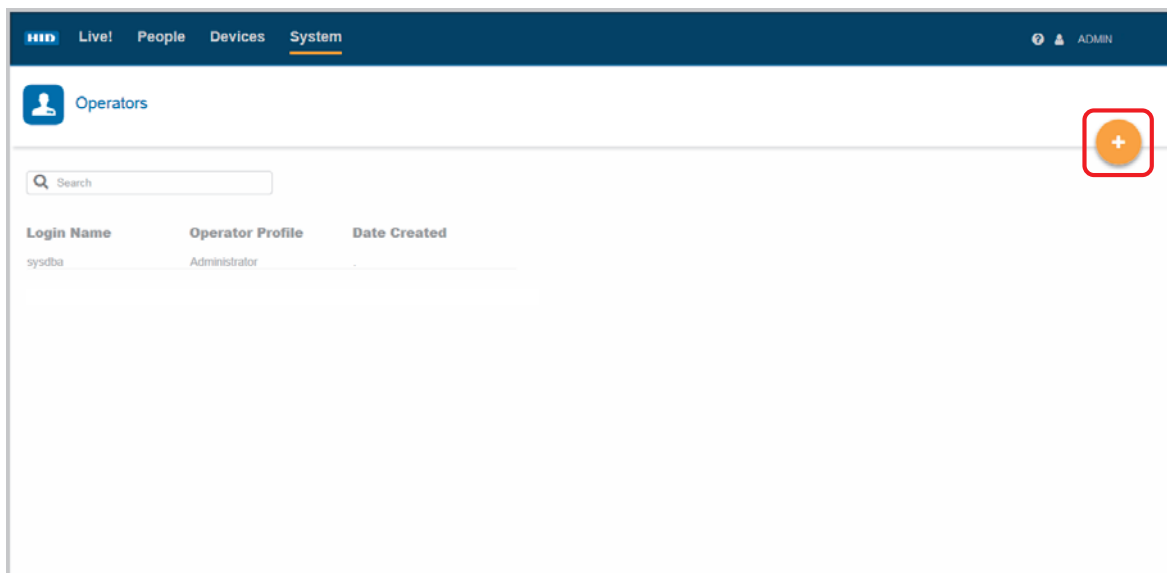
- **Administrator:** This operator role has full access to Biometric Manager web application with functions to install and manage RB25F devices, enroll people in the system, add credentials, and collect and store associated biometric data.
- **Enrolment:** This operator role has full access to Biometric Manager web application, however is limited to the day-to-day activities of enrolling people in the system, adding credentials, collecting and storing associated biometric data.


To create Biometric Manager operator roles:

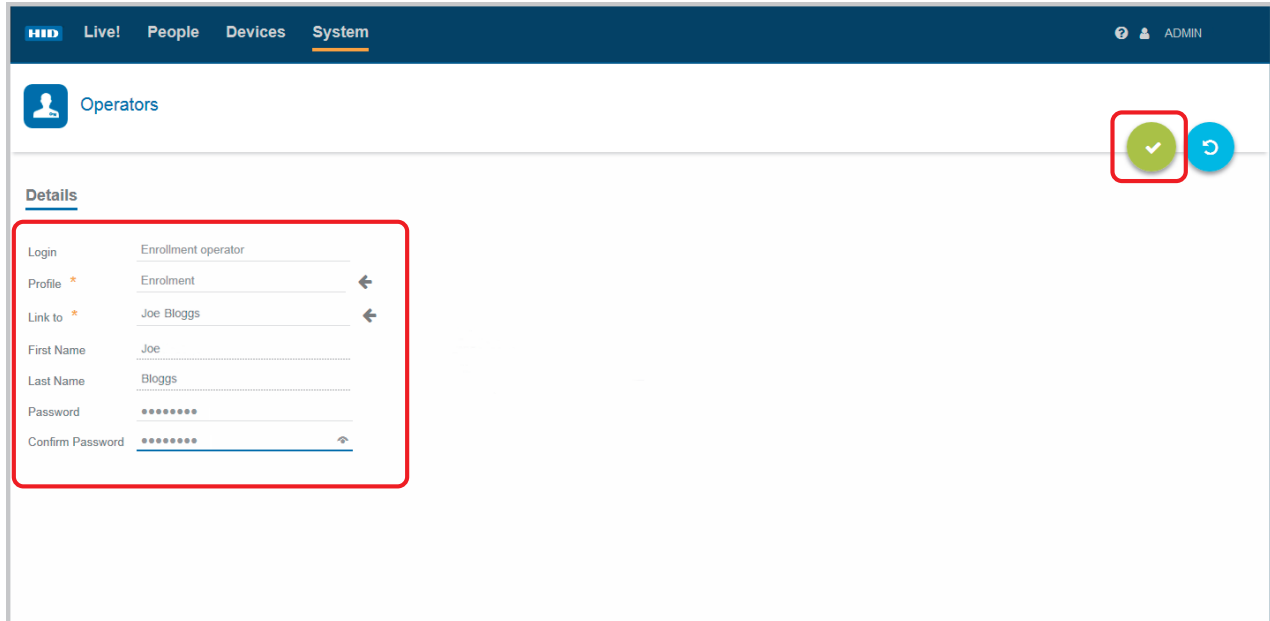
1. Click on the **System** option.
2. Select the **Operators** option to access software and firmware update settings.



3. To add an operator, click the **New** icon [+].



4. On the **Operators Details** screen enter the following:
 - **Login:** Enter a login name for this operator.
 - **Profile:** Select the operator profile, **Administrator** or **Enrolment**.
 - **Link to:** Link this operator profile to a person.
 - **Password/Confirm Password:** Enter a password (re-enter to confirm) for this operator.
5. Click the **Save** icon [] to save the operator profile.




The screenshot displays the 'Operators' management interface. At the top, there are navigation tabs: 'Live!', 'People', 'Devices', and 'System'. The 'System' tab is active. In the top right corner, there is a user profile icon and the text 'ADMIN'. Below the navigation, there is a header for 'Operators' with a person icon. In the top right of the main content area, there are two icons: a green checkmark inside a red square (the 'Save' icon) and a blue circular refresh icon. Below this is a 'Details' section with a form. The form fields are: 'Login' (text input with 'Enrollment operator'), 'Profile' (dropdown menu with 'Enrolment' selected and a left arrow), 'Link to' (dropdown menu with 'Joe Bloggs' selected and a left arrow), 'First Name' (text input with 'Joe'), 'Last Name' (text input with 'Bloggs'), 'Password' (password field with 8 dots), and 'Confirm Password' (password field with 8 dots and a right arrow). A red box highlights the entire form area.

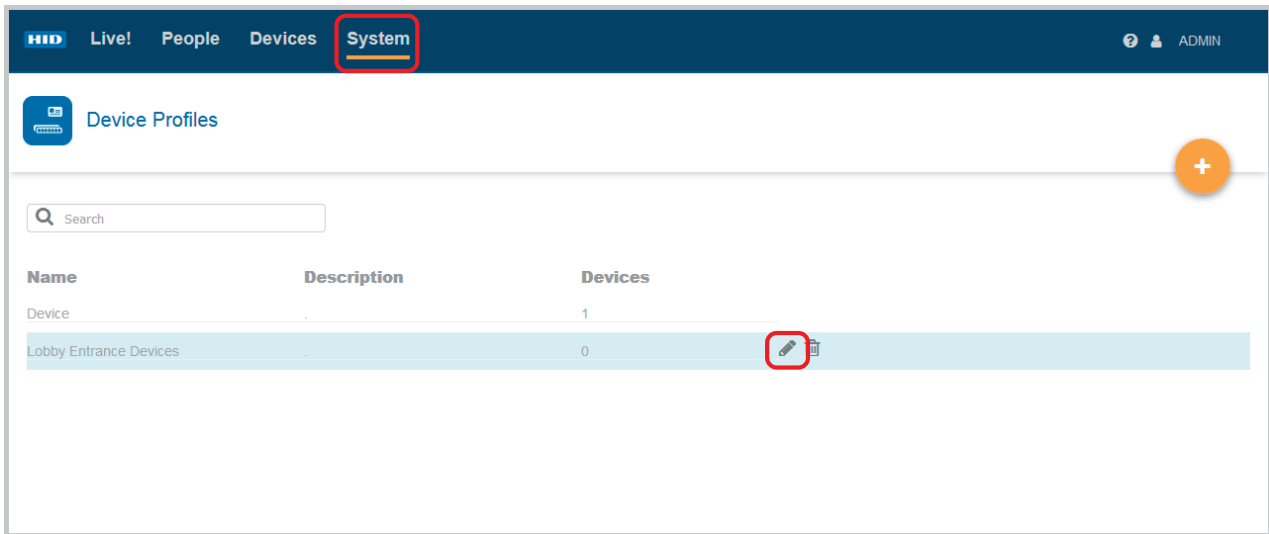
3.3 Device profiles

A device profile contains a set of attributes that you can associate with a device, or group of devices, and is the primary means by which you can manage devices. HID Biometric Manager comes with a default device profile named **Devices** and installed devices are automatically placed in this default device profile.

3.3.1 Edit a device profile

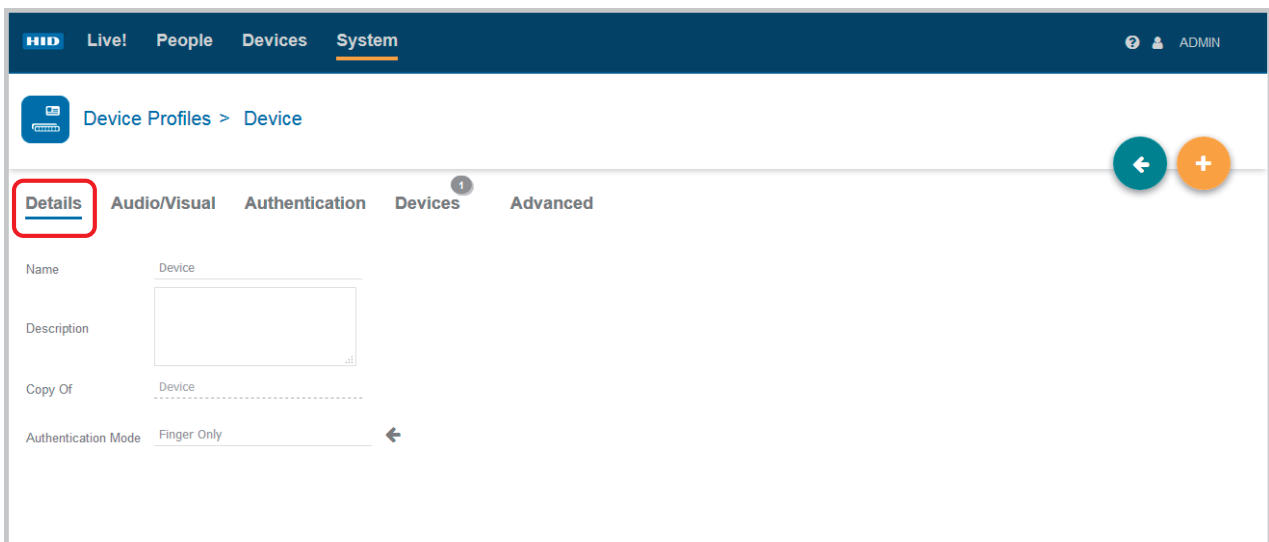
To edit the attributes of device profile:

1. On the **System** screen, highlight a device profile from the displayed list. The **Edit/Delete** icons appear on the screen for the highlighted device profile.
2. Click on the **Edit** icon [] associated with the device profile.



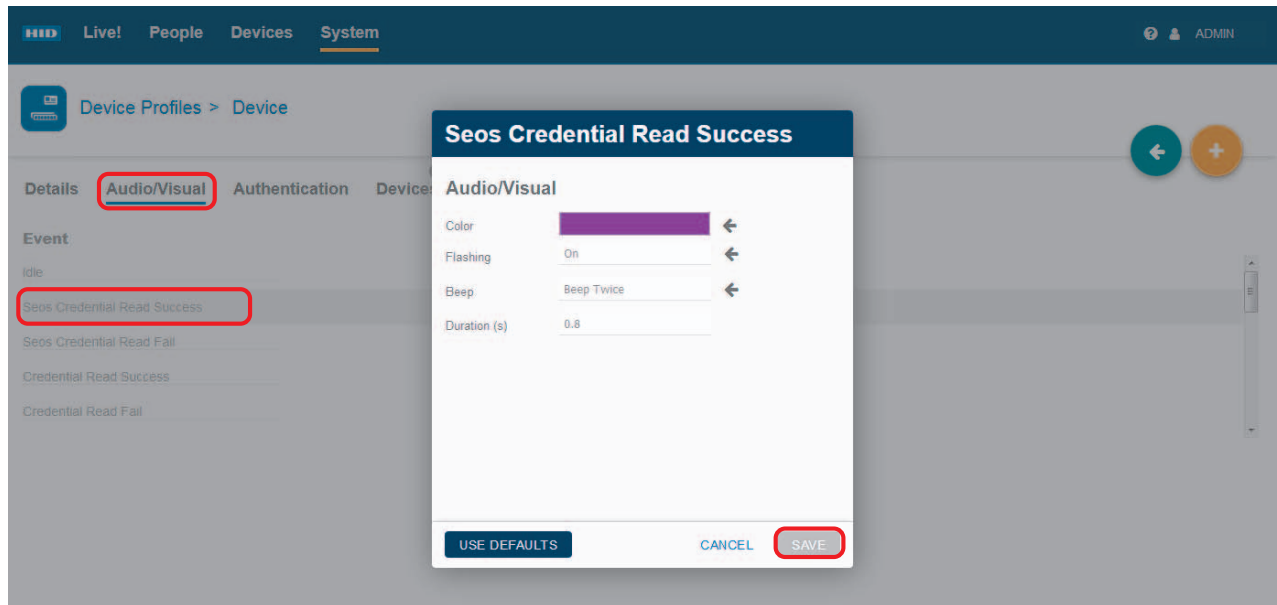
3. On the **Device** screen, if not already displayed, select **Details**. On the **Details** screen you can edit the device profile **Name** and **Description** and select the **Authentication Mode**.

Note: For a definition of the **Authentication Modes**, see *Appendix B - Acronyms and terminology*.



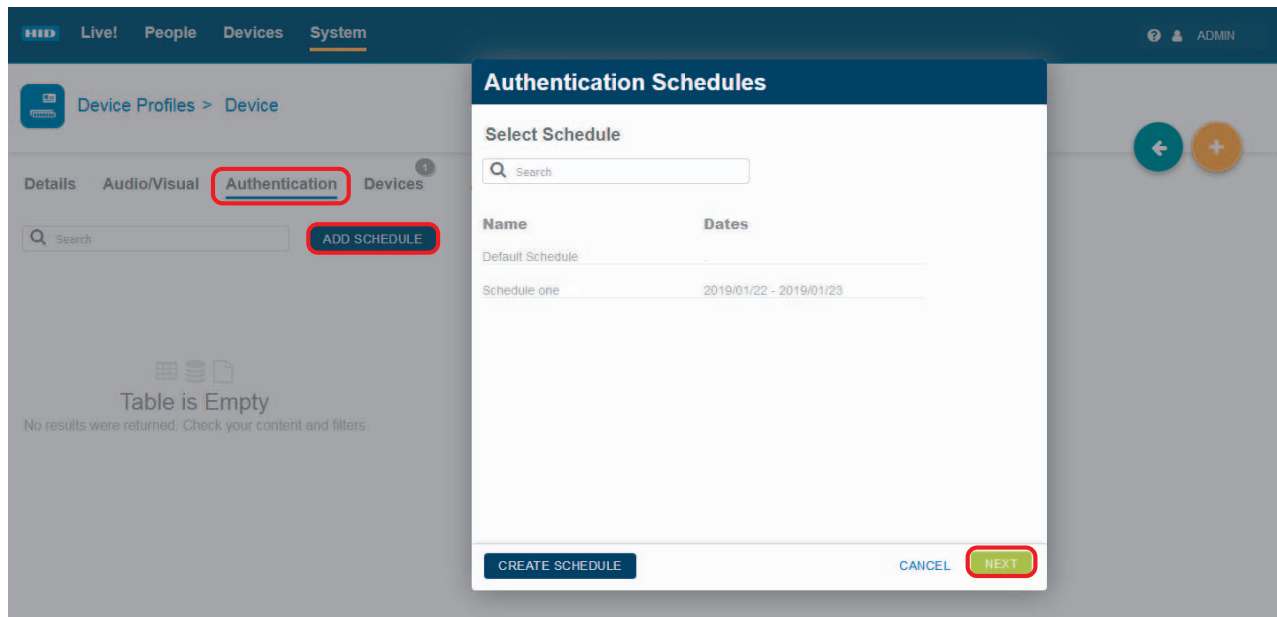
4. On the **Device** screen, select **Audio/Visual**.
5. Click on an **Event** type from the displayed list to edit the attributes for the selected event.
6. Click **SAVE** to save the selected settings.

Note: Click **SAVE DEFAULTS** to revert back to the default settings for the selected event.

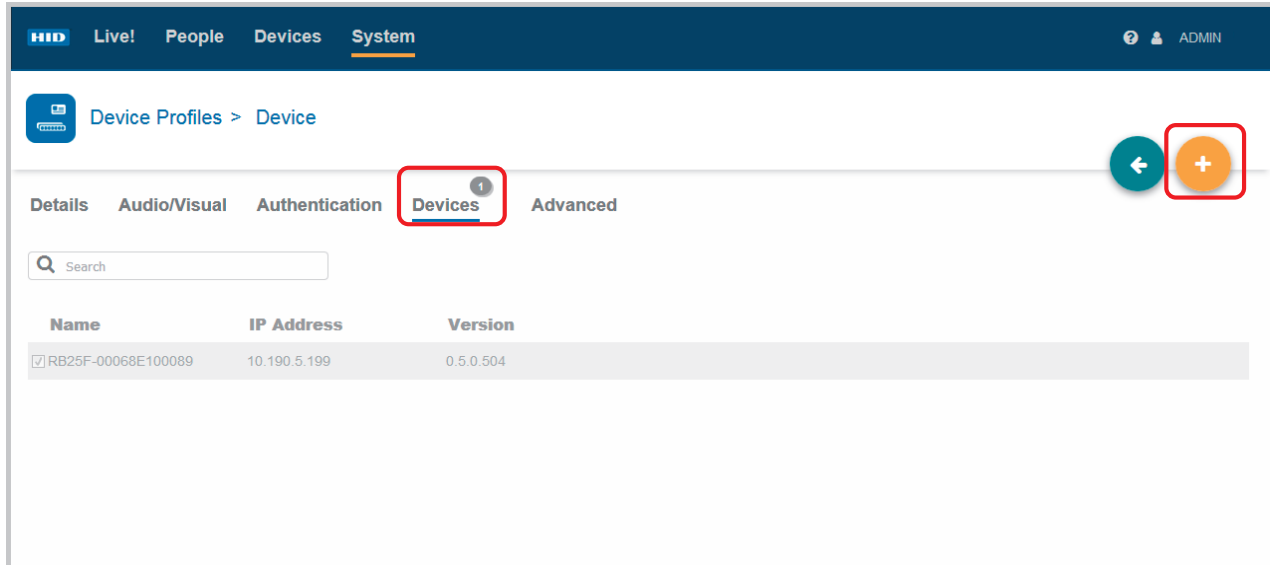


7. On the **Device** screen, select **Authentication**.
8. Click **ADD SCHEDULE**, select a Schedule from the list and click **Next**.

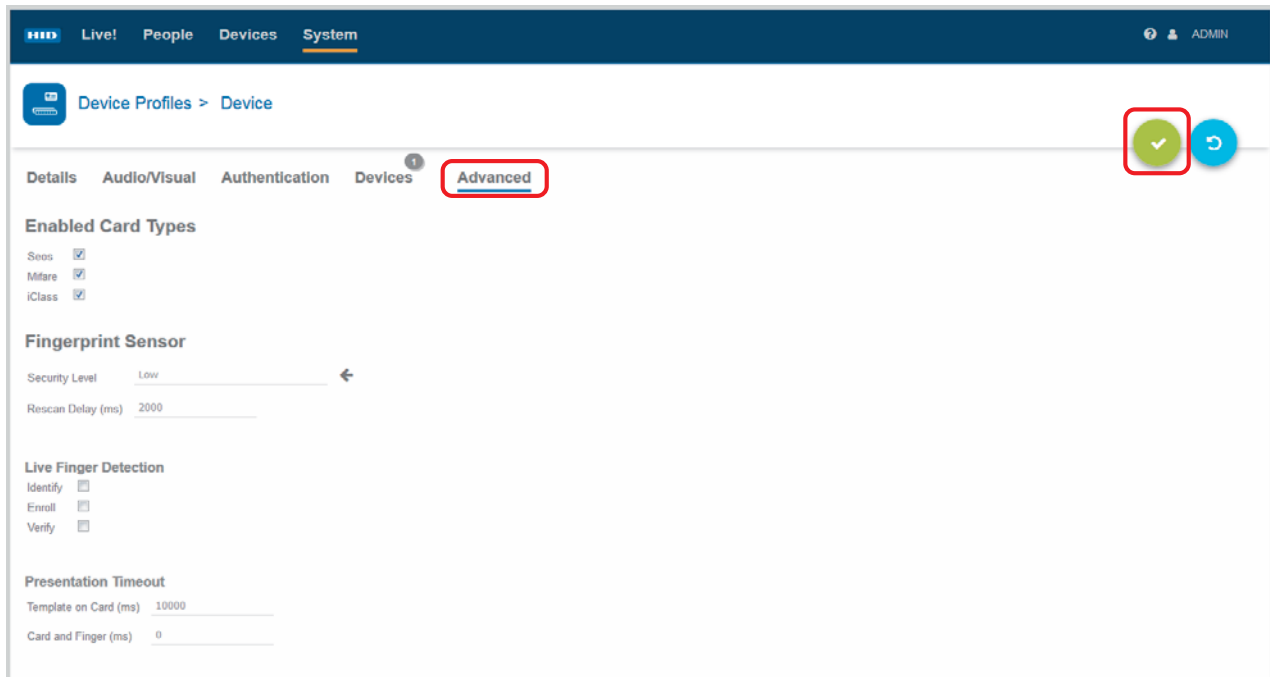
Note: Click **CREATE SCHEDULE** to create a new authentication schedule.



- On the **Device** screen, select **Devices** to view the list of devices that belong to this device profile. Any changes made to this device profile will be applied to these listed devices.
- Click the **Add** icon [+] to add a device to this device profile.



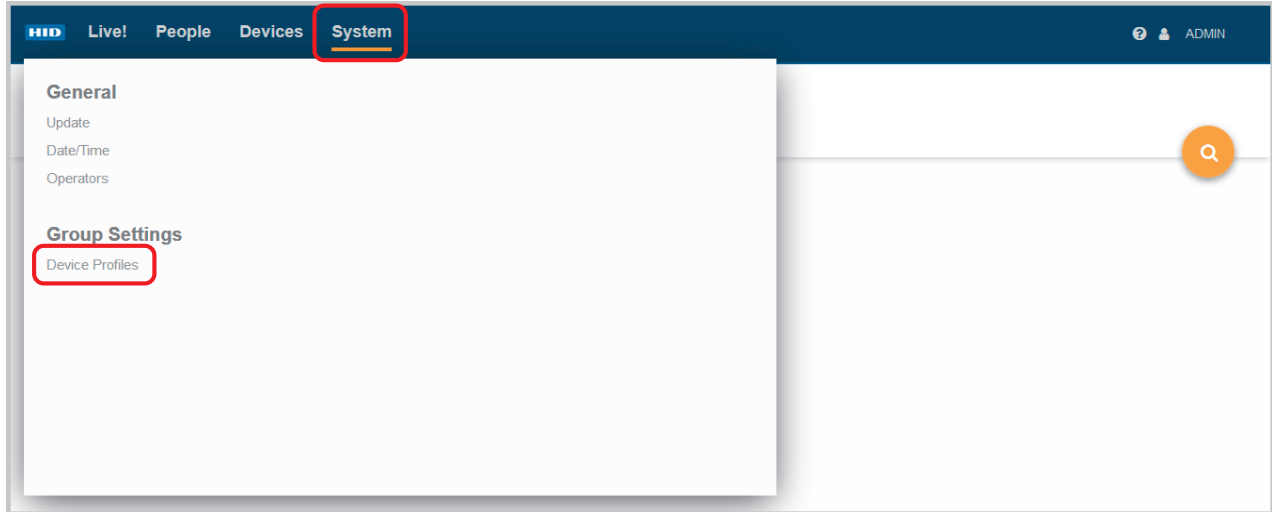
- On the **Device** screen, select **Advanced**.
- Select the required card types to enable and the fingerprint sensor settings.
- Click **SAVE** to save the selected settings.



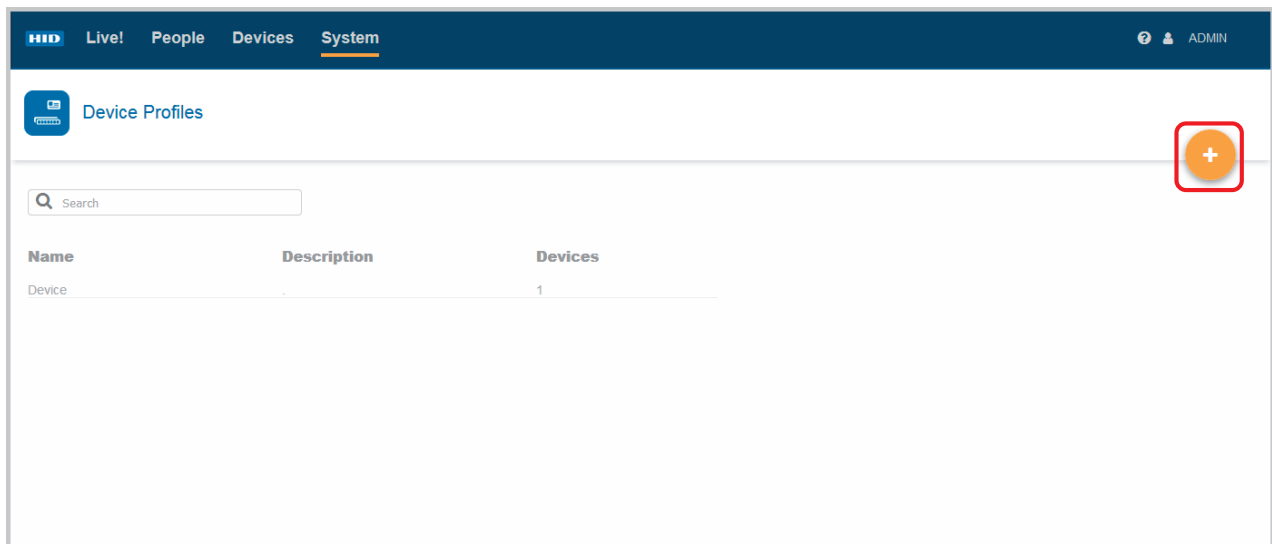
3.3.2 Create a device profile

To create a new device profile:

1. Click on **System** and select the **Device Profiles** option.

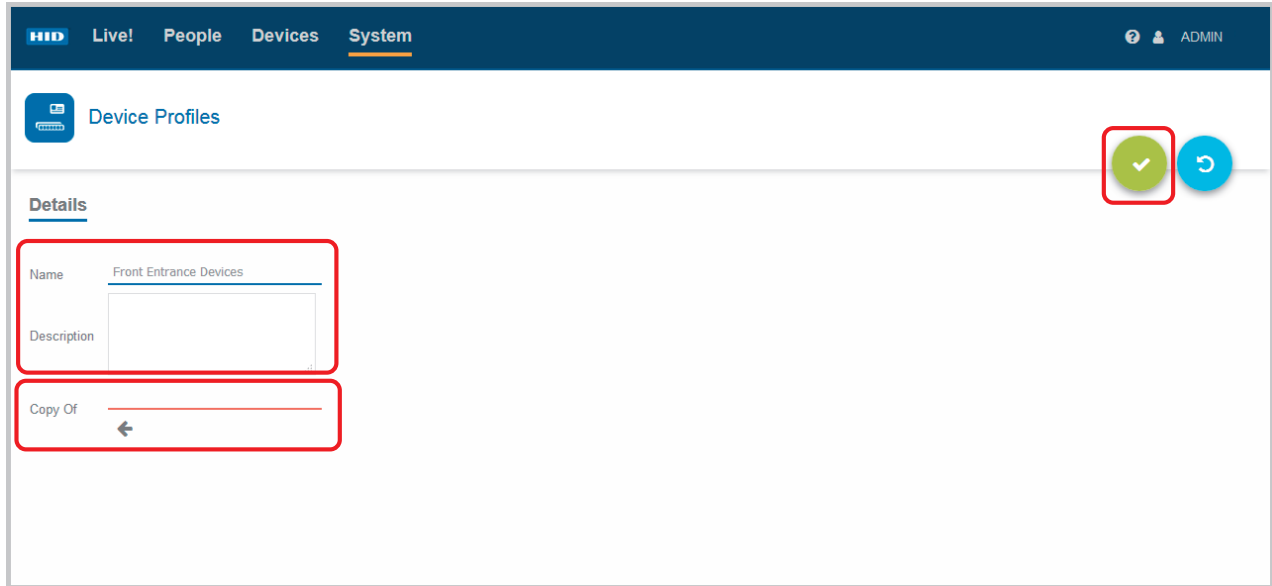


2. Click the **Add** icon [+].

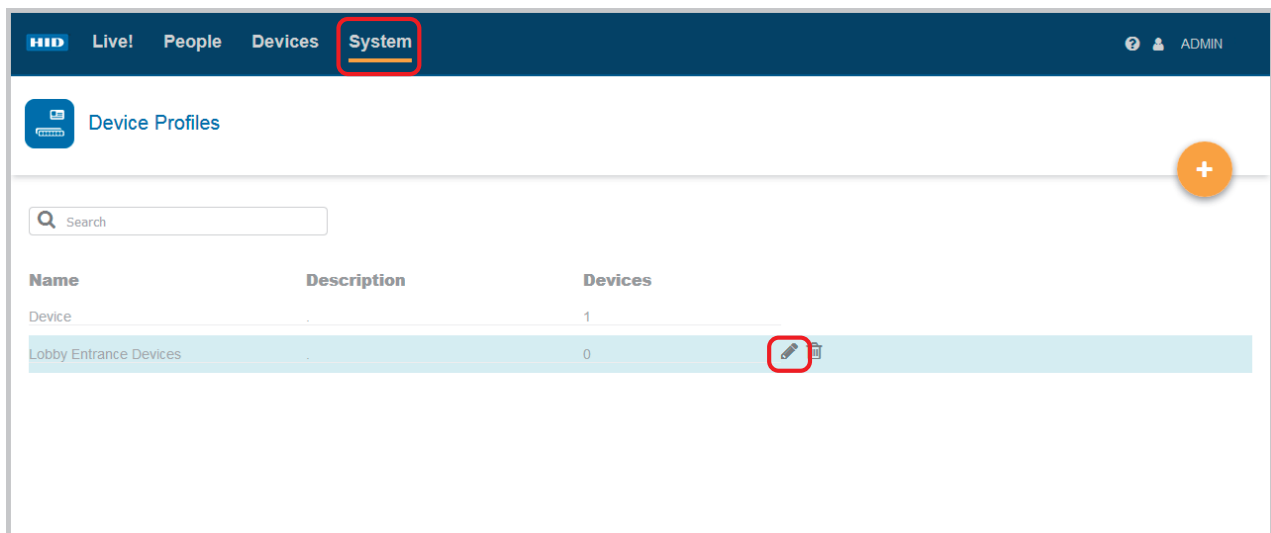


3. Enter a **Name** and optional **Description** for the new device profile, then click the **Save** icon [✓].

Note: Select the arrow icon associated with **Copy Of** to select an existing profile to copy. Device Profile attributes can now be edited. See *Section 3.3.1 Edit a device profile*.




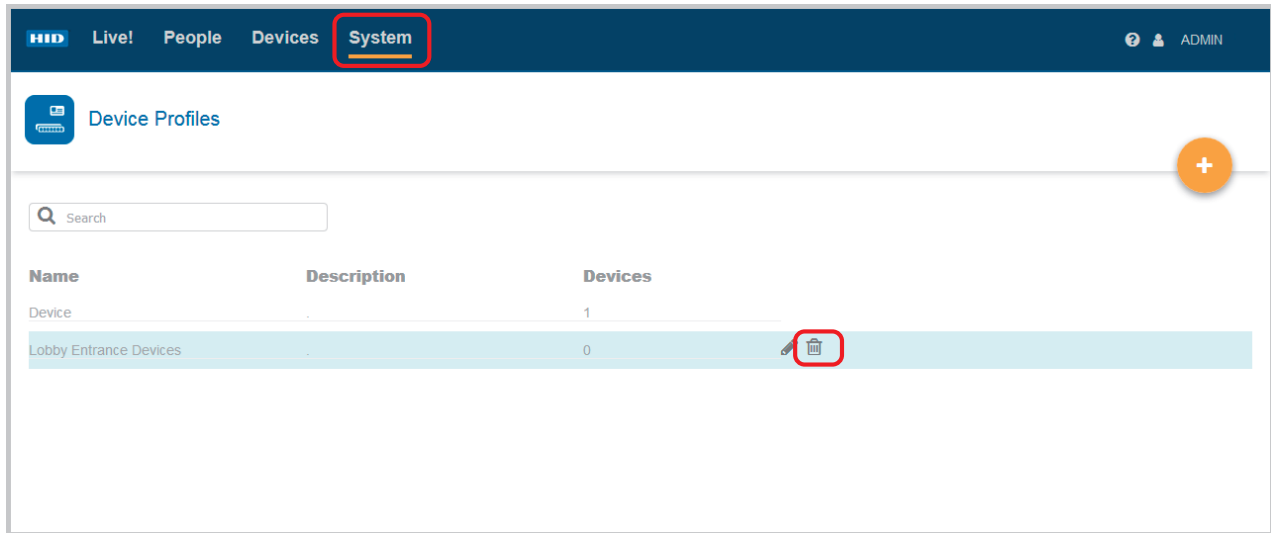
4. The created device profile is listed on the Device Profiles screen. To edit a profile, highlight a device profile from the displayed list. The **Edit/Delete** icons appear on the screen for the highlighted device profile.
5. Click on the **Edit** icon [✎] associated with the device profile to access the profile attributes. See *Section 3.3.1 Edit a device profile*.



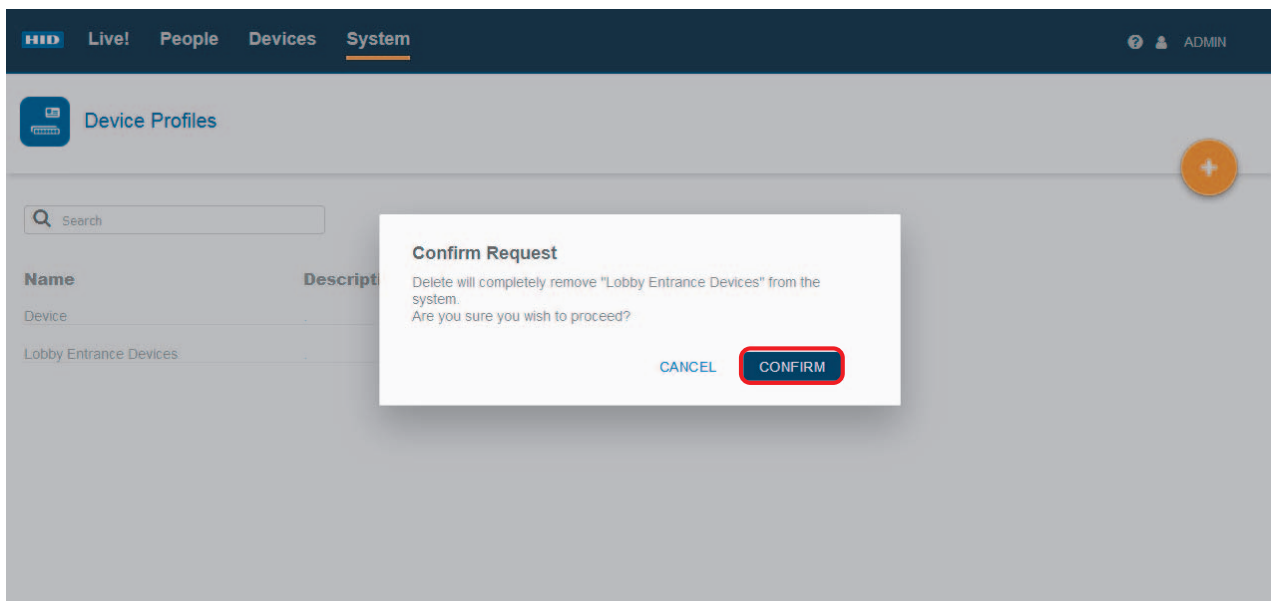
3.3.3 Delete a device profile

To delete a device profile:

1. On the **System** screen, highlight a device profile from the displayed list. The **Edit/Delete** icons appear on the screen for the highlighted device profile.
2. Click on the **Delete** icon [] associated with the device profile.




3. Click **CONFIRM** to proceed with the device profile delete action.

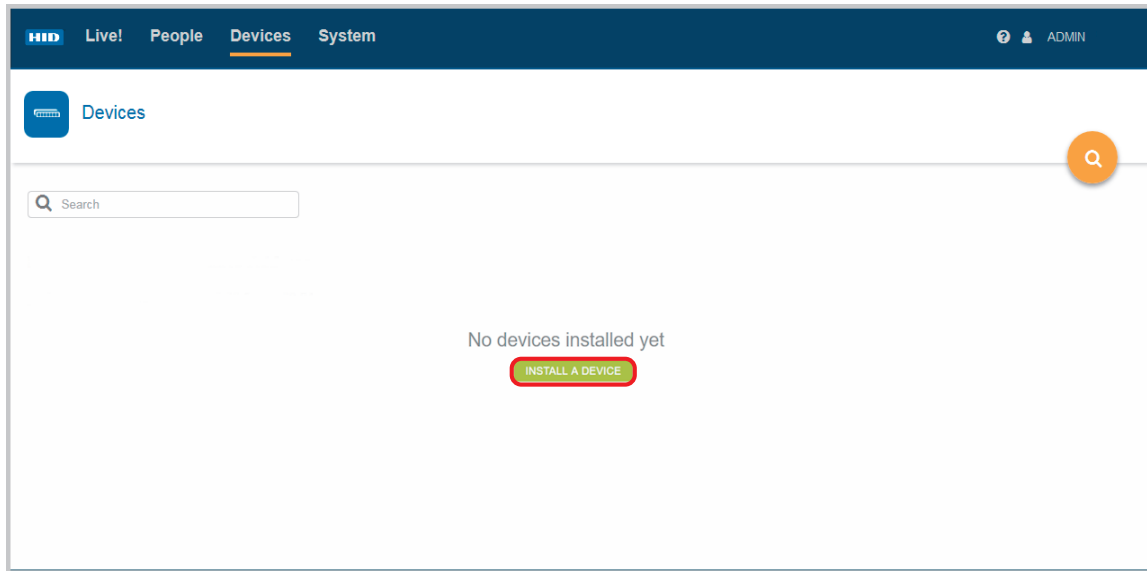


3.4 Device installation and configuration

Device installation and configuration with HID Biometric Manager can only be carried out by the **Administrator** operator role. For initial configuration or when no devices are installed, Biometric Manager opens on the **Devices** screen with the option to install a device. If devices are already installed Biometric Manager opens on the **People** screen, see *Section 3.5 Enrollment*.

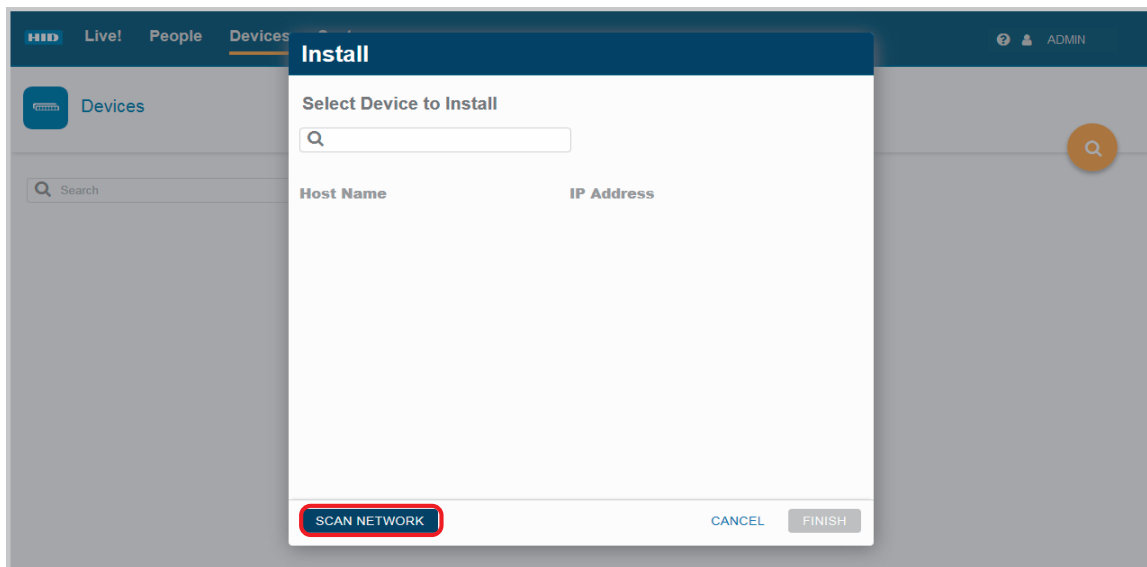
1. Launch HID Biometric Manager and login as **Administrator** operator.
2. To initially install a device, on the **Devices** screen, click **INSTALL A DEVICE**.

Note: If devices are already installed, to add additional devices click the **Install** icon [].

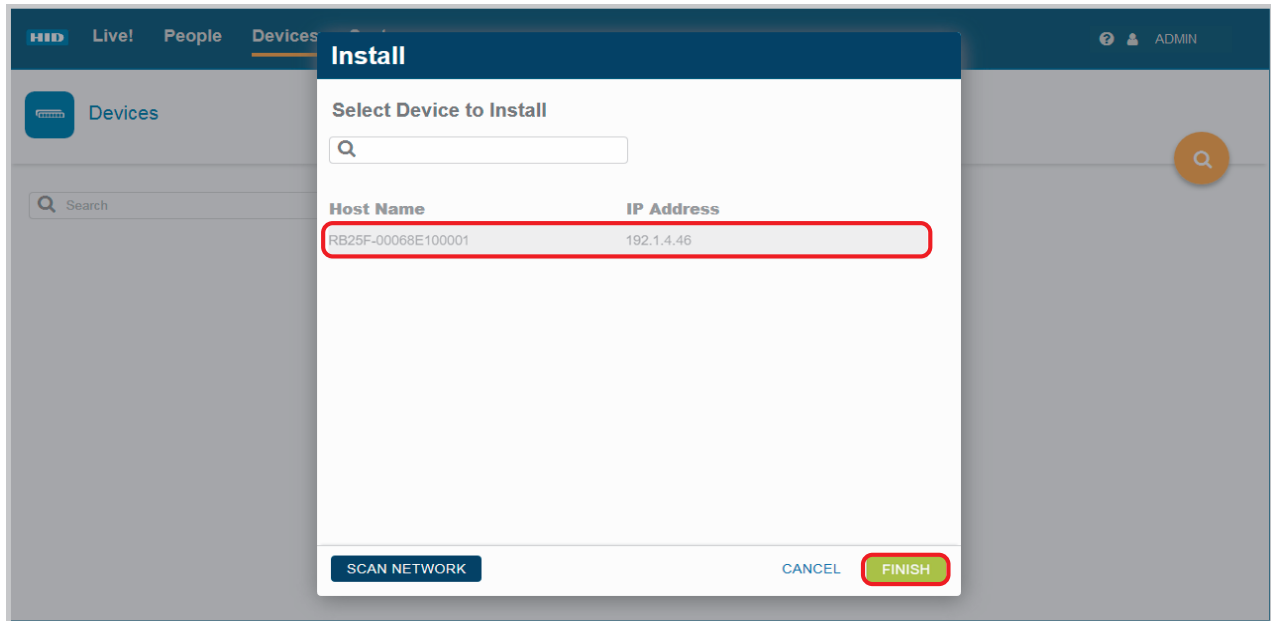


3. In the **Install** dialog, click **SCAN NETWORK** to ensure the complete list of available devices are shown.

Note: If no devices are found check the availability of port 10500. Also use the Search function and enter the device MAC address (the MAC address label is located on the back of the reader).

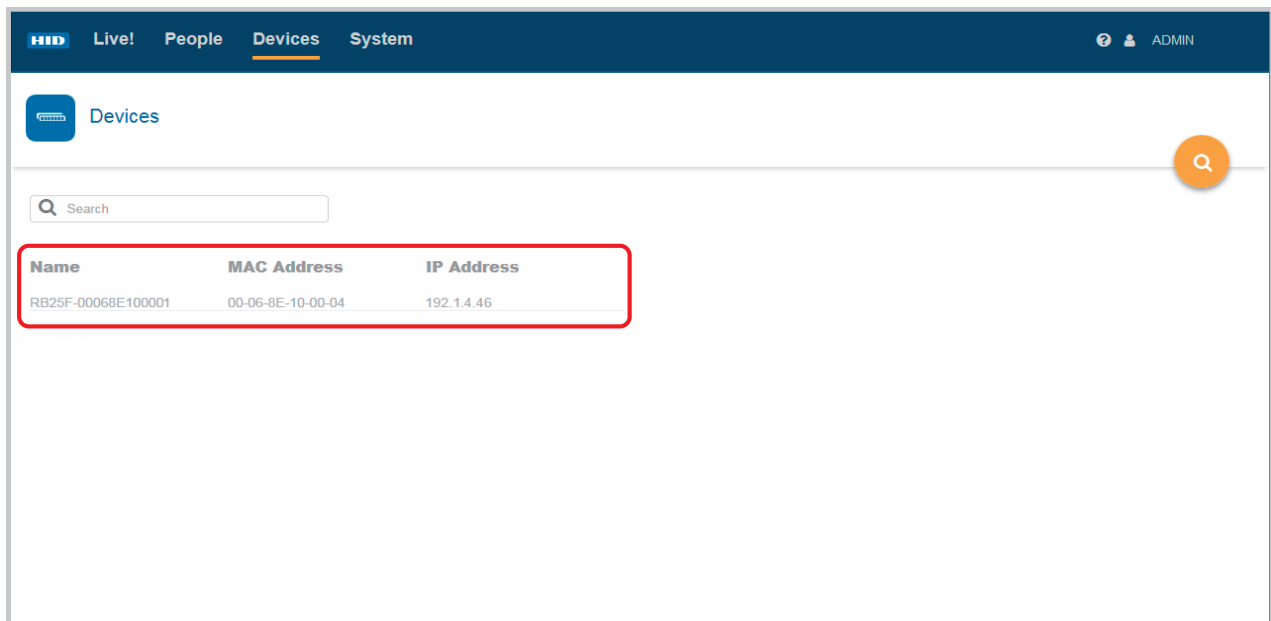


4. Select a device from the displayed list and click **FINISH**.



When the installation has completed the **Devices** screen displays the installed device.


Note: Installed devices are automatically added to the default device profile named **Device**. The default device profile can be edited or new profiles can be added to the system.

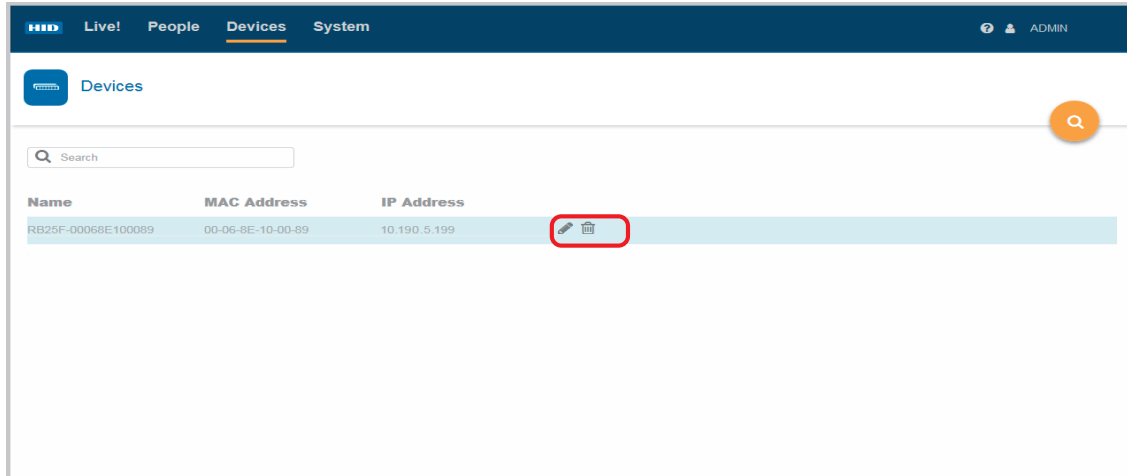


Note: To uninstall a device, see *Section 3.4.3 Uninstall a device*.

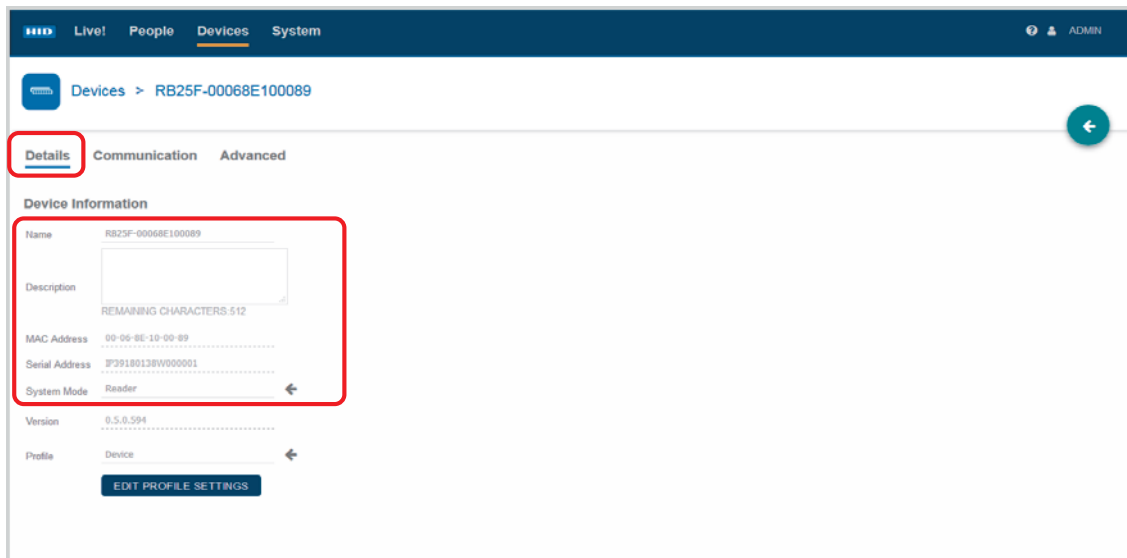
3.4.1 Configure device settings


To access and configure settings associated with an installed device:

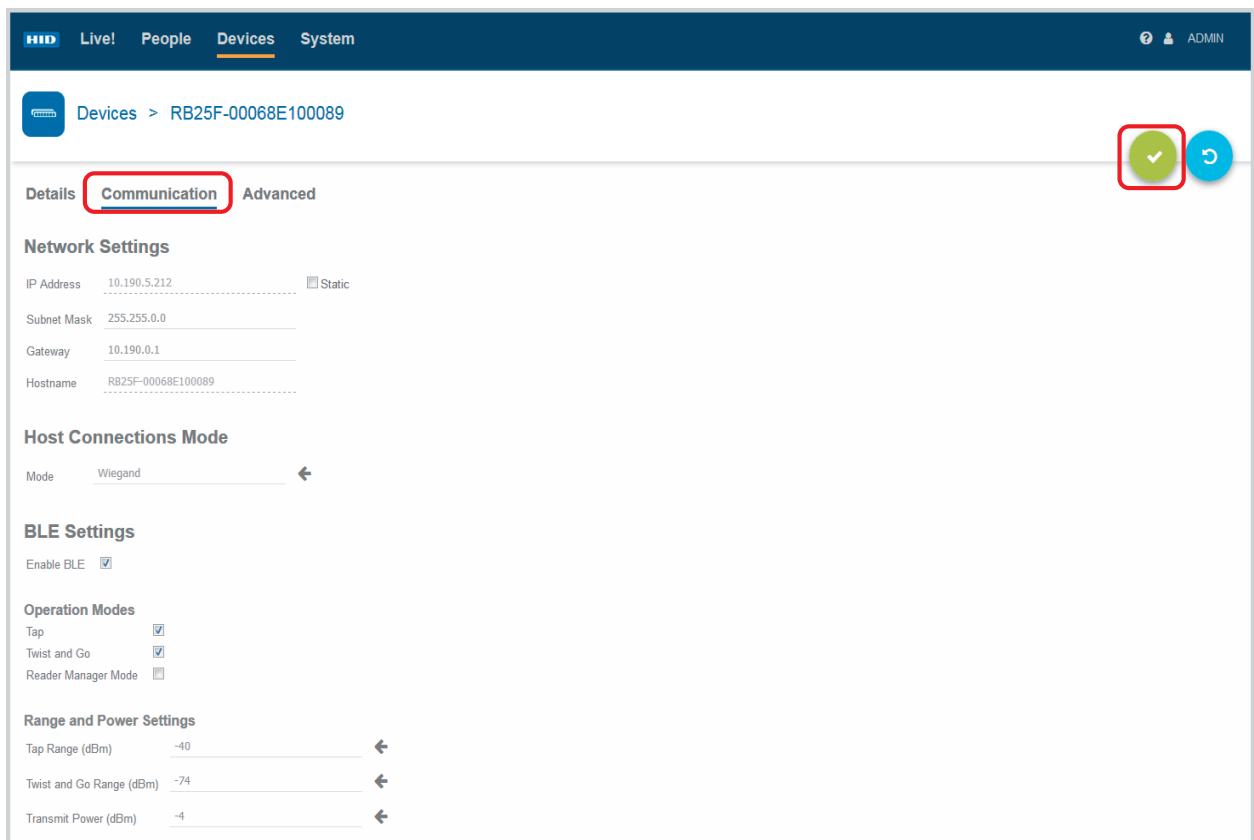
1. On the **Devices** screen, highlight a device entry from the displayed list. The **Edit/Delete** icons appear on the screen for the highlighted device.
2. Click on the **Edit** icon [] associated with the device to access the device settings screen.



3. On the **Devices** screen, if not already displayed, select **Details**.
4. Under **Device Information** you can edit the following:
 - **Name/Description:** Enter a logical name for the device. As an option enter a description for the device.
 - **Profile:** Click on the arrow icon to select a device profile. Click on the edit icon to configure the settings for the displayed device profile, see *Section 3.3.1 Edit a device profile*.
 - **System Mode:** Click on the arrow icon to select and set the system mode. For a description of the System Modes, see *Appendix B - Acronyms and terminology*.



5. On the **Devices** screen, select **Communication**.
6. On the Communication screen you can configure:
 - **Network Settings:** Select the **Static** option and enter a static IP address.
 - **Host Communications Mode:** Set as either Wiegand or OSDP (not both).
Note: If OSDP is selected as the Host Communication Mode OSDP settings for Baud Rate and OSDP Address become available for configuration.
 - **BLE Settings:** Select the desired operation mode.
 - **Range and Power Settings:** Set the read range for **Tap** and **Twist and Go** and the setting for **Transmit Power**.
7. When the communication settings have been selected click the **Save** icon [].




The screenshot displays the HID Biometric Manager web interface. At the top, there is a navigation bar with 'Live!', 'People', 'Devices', and 'System' tabs. The 'Devices' tab is active, and the breadcrumb path is 'Devices > RB25F-00068E100089'. The 'Communication' tab is selected and highlighted with a red box. In the top right corner, there is a green checkmark icon in a circle, also highlighted with a red box, and a blue refresh icon. The settings are organized into sections: 'Network Settings' (IP Address: 10.190.5.212, Subnet Mask: 255.255.0.0, Gateway: 10.190.0.1, Hostname: RB25F-00068E100089), 'Host Connections Mode' (Mode: Wiegand), 'BLE Settings' (Enable BLE: checked), 'Operation Modes' (Tap: checked, Twist and Go: checked, Reader Manager Mode: unchecked), and 'Range and Power Settings' (Tap Range (dBm): -40, Twist and Go Range (dBm): -74, Transmit Power (dBm): -4).

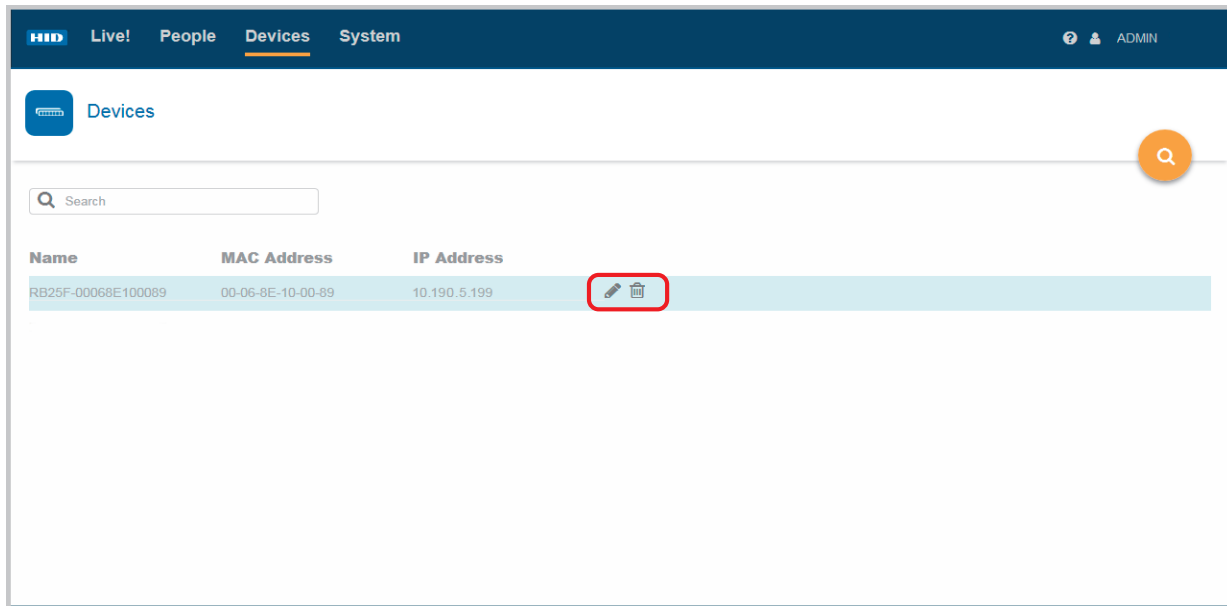
- 8. On the **Devices** screen select **Advanced**. On the **Advanced** screen you have options to:
 - Restore all device settings to the original factory defaults, see *Section 3.4.2 Reset a device*.
 - Change the device password.
 - Configure the device security level.
- 9. Click **SYNC** option. For the selected device all settings are copied from HID Biometric Manager to the RB25F.



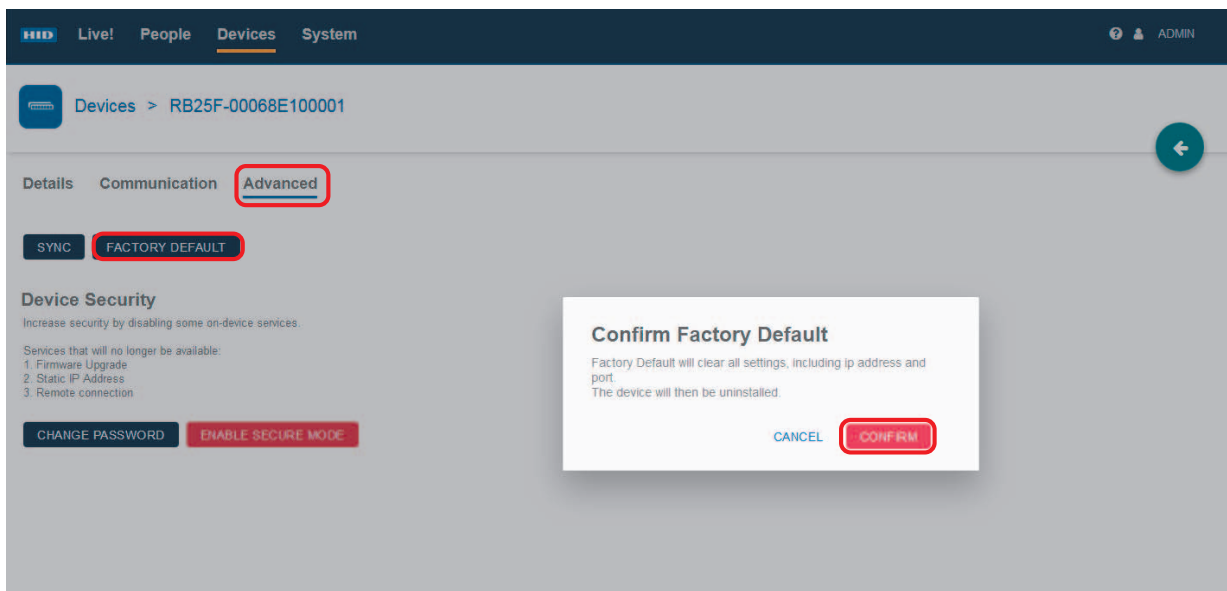
3.4.2 Reset a device

To restore all device settings (firmware, IP settings, Host IP, etc.) to the original factory defaults:

1. On the **Devices** screen, highlight a device entry from the displayed list. The **Edit/Delete** icons appear on the screen for the highlighted device.
2. Click on the **Edit** icon [] associated with the device to access the device settings screen.



3. On the **Devices** screen select **Advanced** and the **FACTORY DEFAULT** option.
4. Select **FACTORY DEFAULT** to confirm the action.

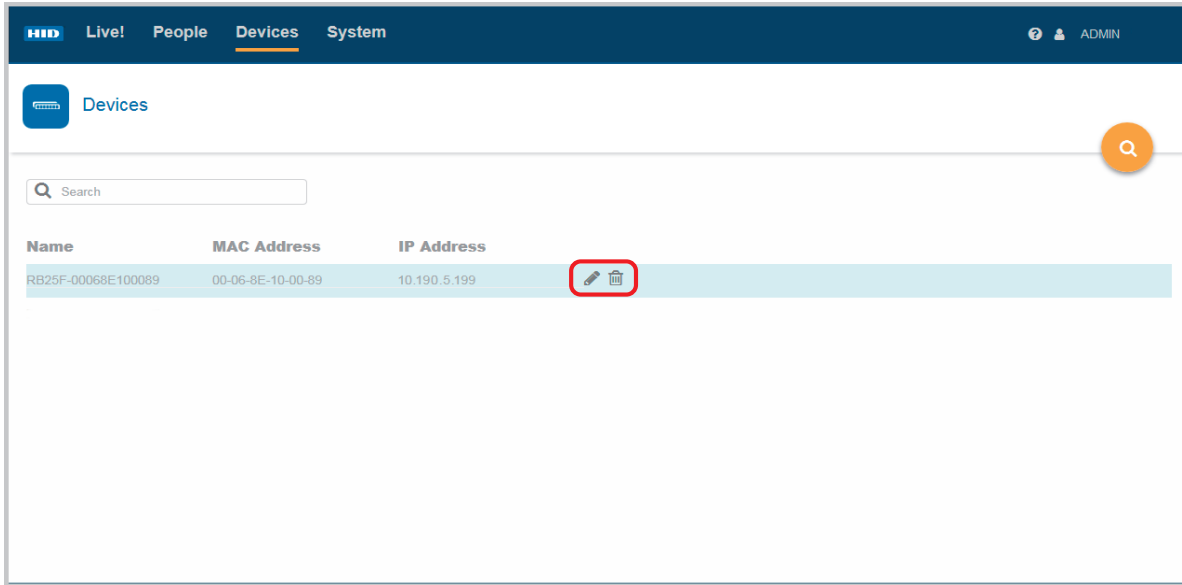


Note: Where communication between HID Biometric Manager and the RB25F is not possible, factory default reset can be carried out at the reader, see *Section 2.4 Hardware reset the RB25F*.

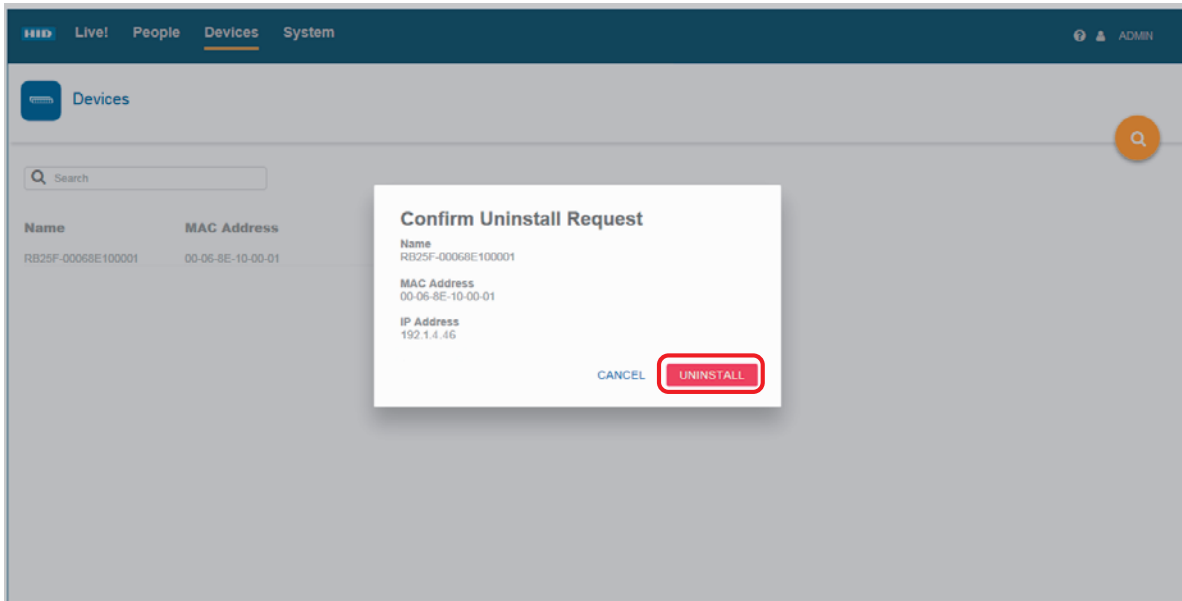
3.4.3 Uninstall a device

To uninstall a device:

1. On the **Devices** screen, highlight a device entry from the displayed list. The **Edit/Delete** icons appear on the screen for the highlighted device.
2. Click on the **Delete** icon [] associated with the device.



3. Click **UNINSTALL** to confirm the uninstall action.



4. You will be notified of a successful device uninstall, click **OK**.

Note: If all devices have been uninstalled in Biometric Manager, you will have to option to install a devices on the **Devices** screen, see *Section 3.4 Device installation and configuration*.

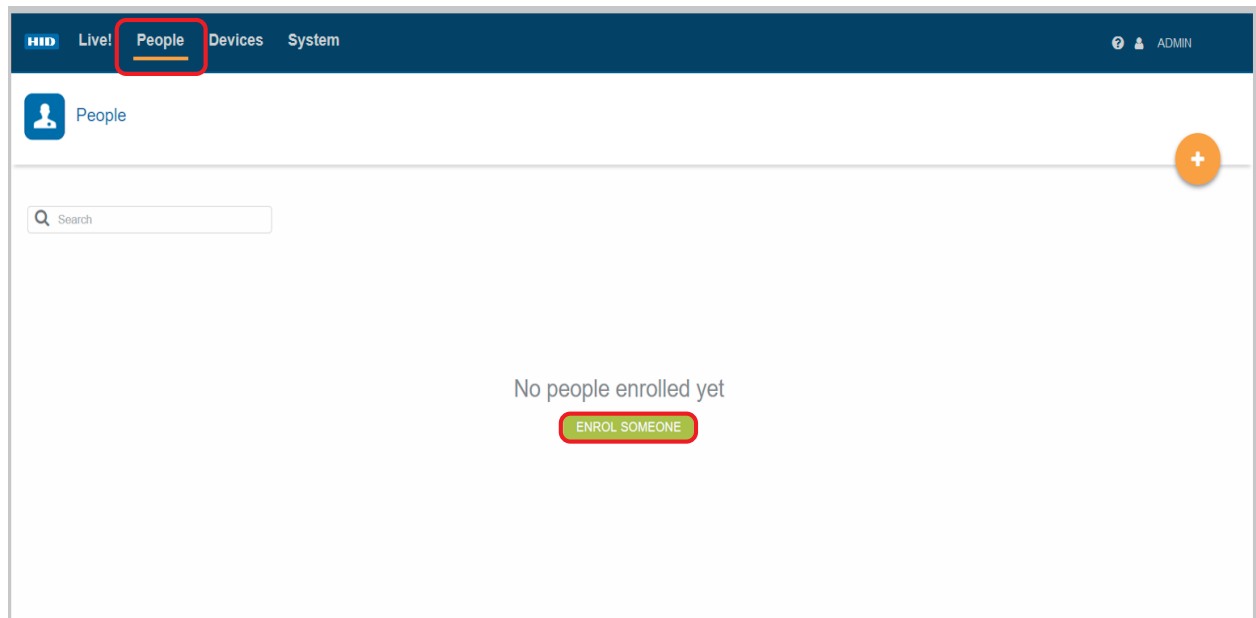
3.5 Enrollment

Enrolling people in the system, adding credentials and collecting associated biometric data can be carried out by an **Administrator** operator or a **Enrolment** operator.

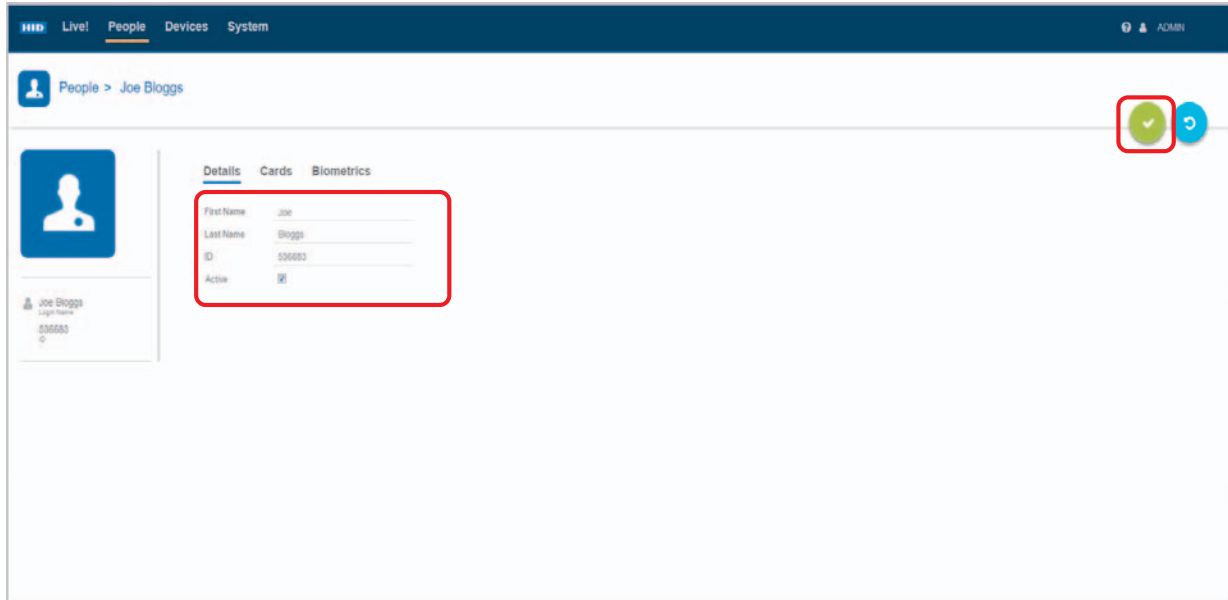
3.5.1 Enroll People

1. Launch HID Biometric Manager and login as either **Administrator** operator or **Enrolment** operator.
2. Click on the **People** option. If no people are enrolled in Biometric Manager the **People** screen is empty and you have the option to enroll a person. Click **ENROL SOMEONE**.

Note: If people are already enrolled, to enroll additional people, click the **Add** icon [+].

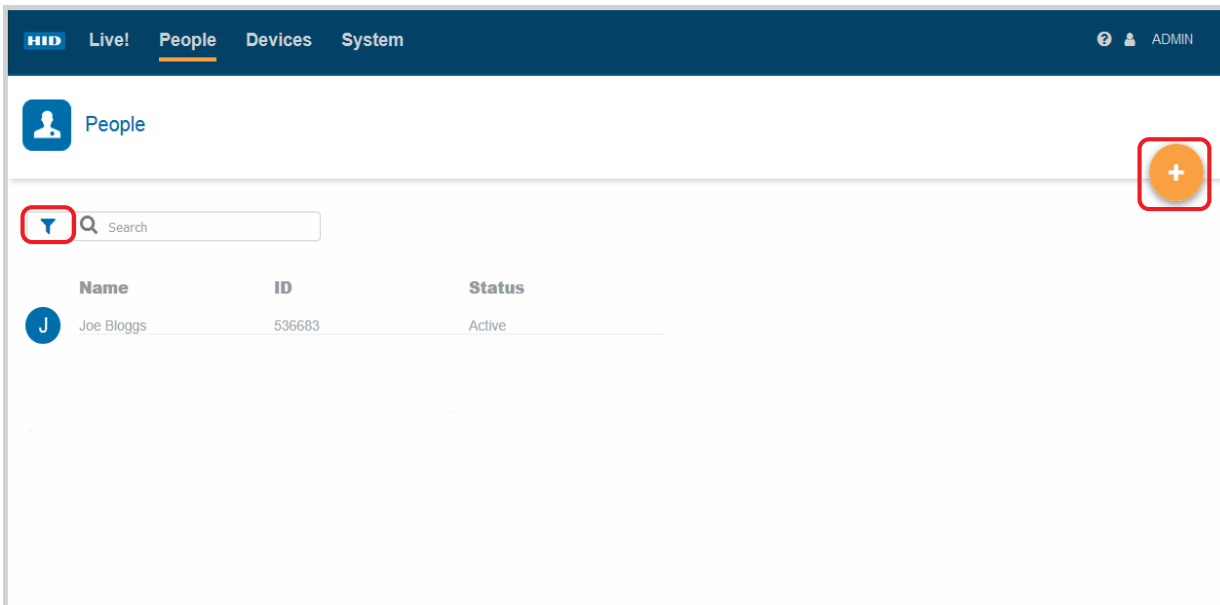


3. Enter the persons details (**First Name/Last Name**). The **ID** number is assigned by the system
4. Select the **Active** option to make this enrolled person active in the system.
Note: If the **Active** option is not selected the enrolled person will have an inactive status in the system and the person record is not displayed on the **People** screen.
5. Click the **Save** icon [✓].



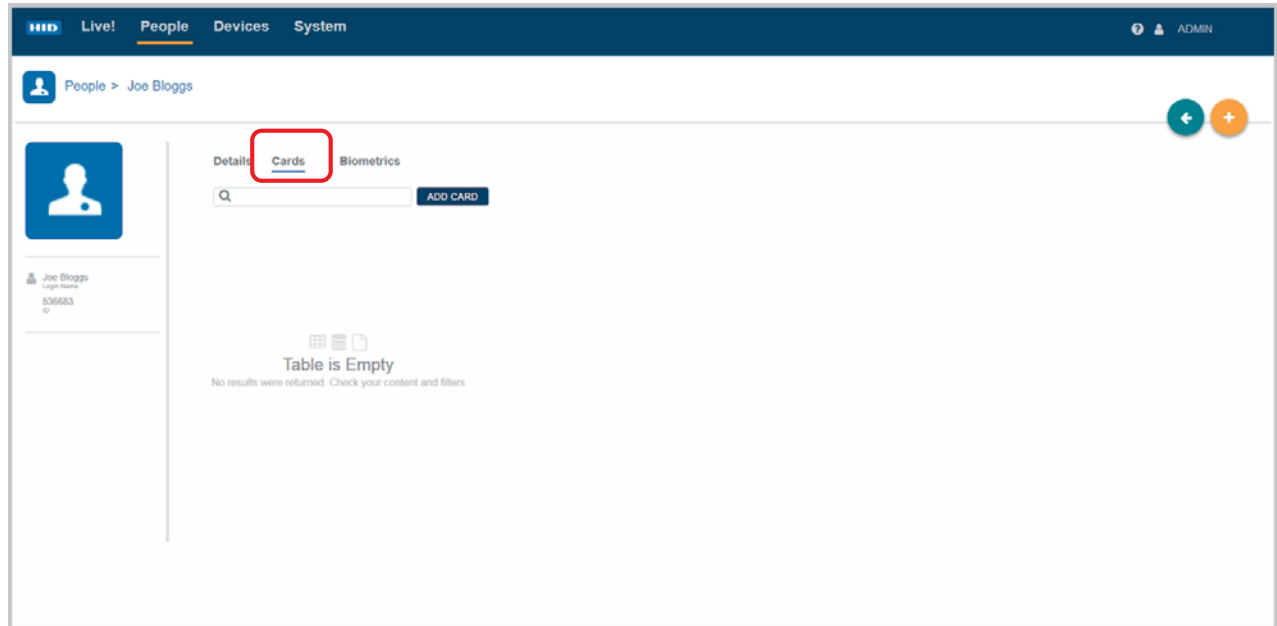
The enrolled person record is displayed on the **People** screen. To add additional people, click on the **New** icon [+] and enter the new persons details.

Note: To display people that have an inactive status, click the filter icon [▼] and select the **Show Inactive People** option.

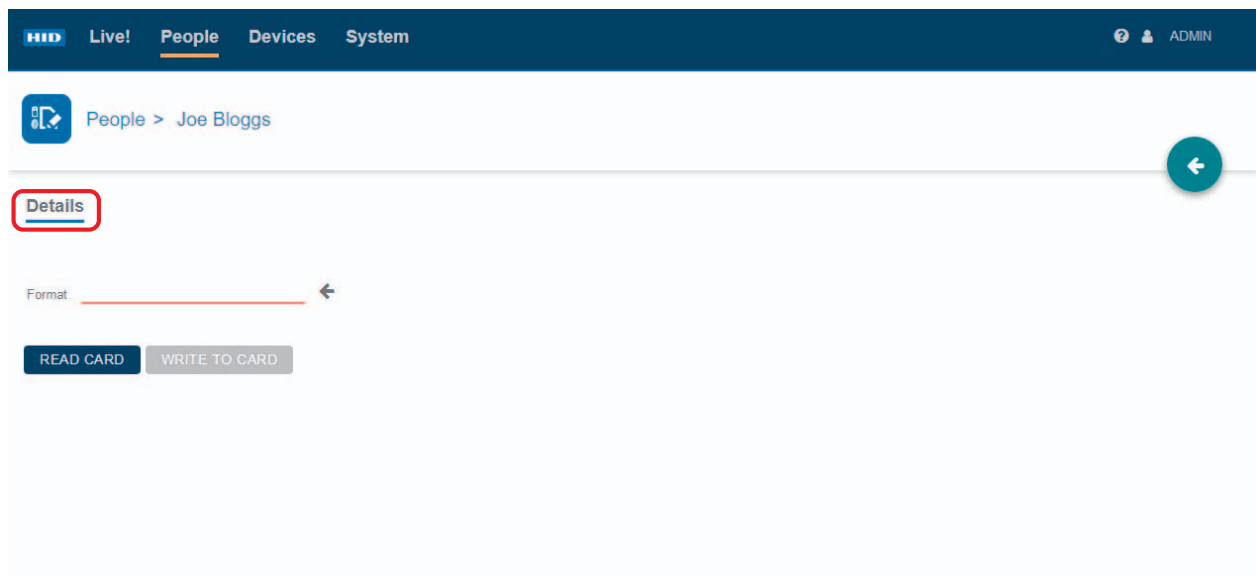


3.5.2 Enroll Cards

1. On the **People** screen select a displayed person record.
2. On the Cards screen click **ADD CARD**.

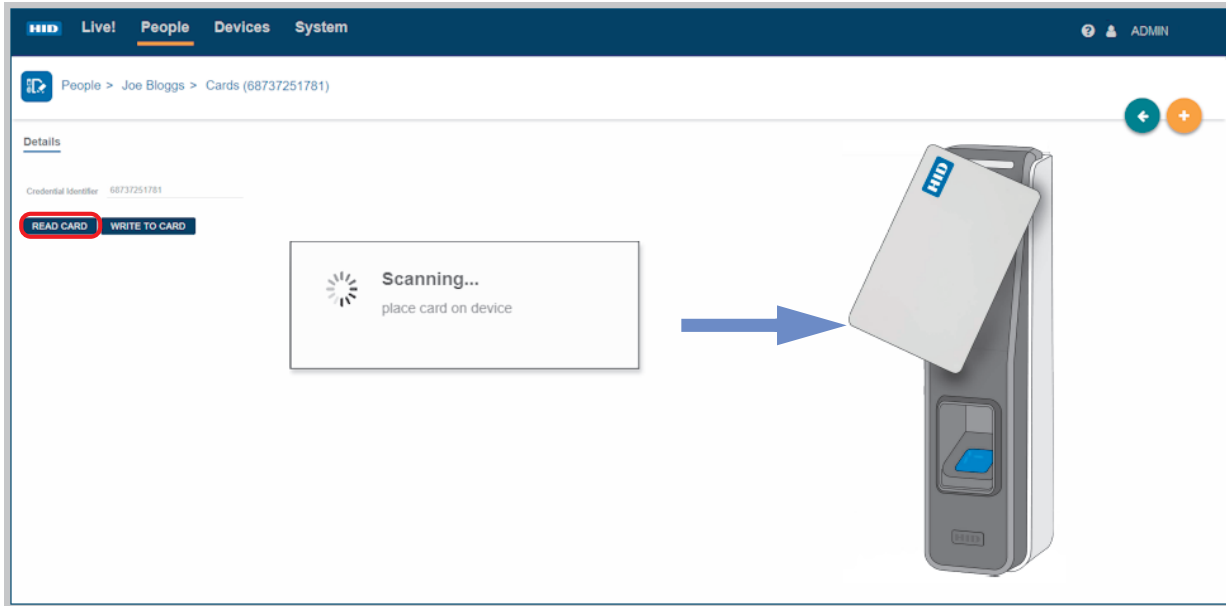


3. At this point on the **Details** screen you can either scan a card to obtain the card details or, if no card is available, manually enter card details.
 - *Scan card for card details.*
 - *Manually enter card details.*



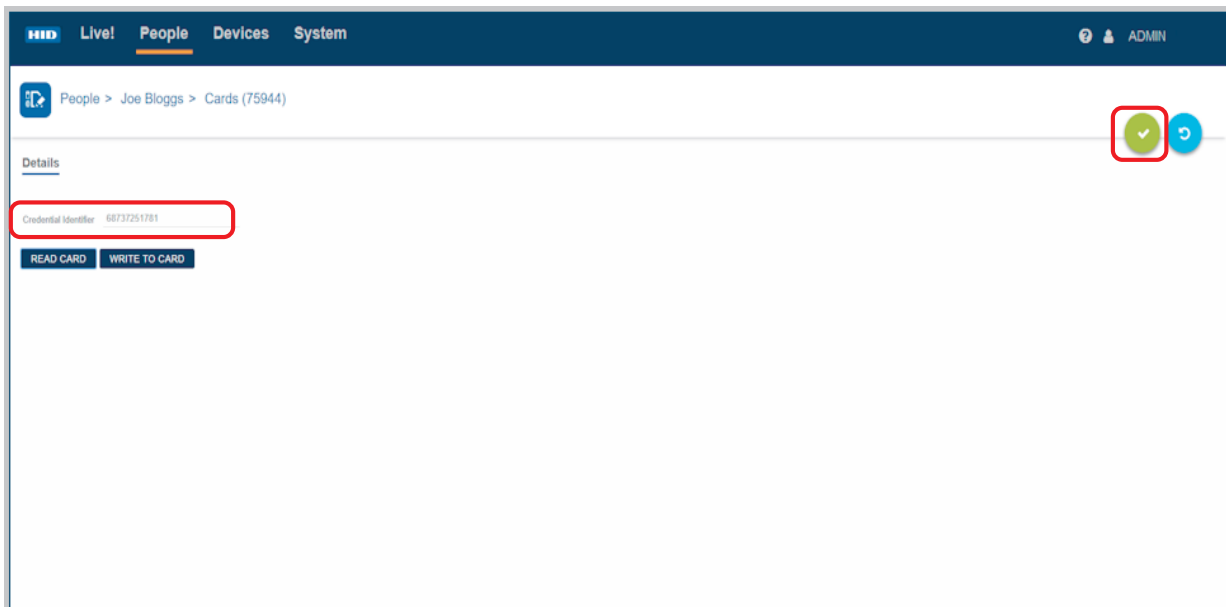
Scan card for card details

1. On the **Details** screen, click **READ CARD**.
2. Optionally select the reader.
3. Within five seconds, present a HID Seos card to the RB25F device.



4. Click the **Save** icon [✓] to save this Credential Identifier.

Note: The Credential Identifier recorded in HID Biometric Manager must be copied over to the third party PACS software running on the PACS Server.

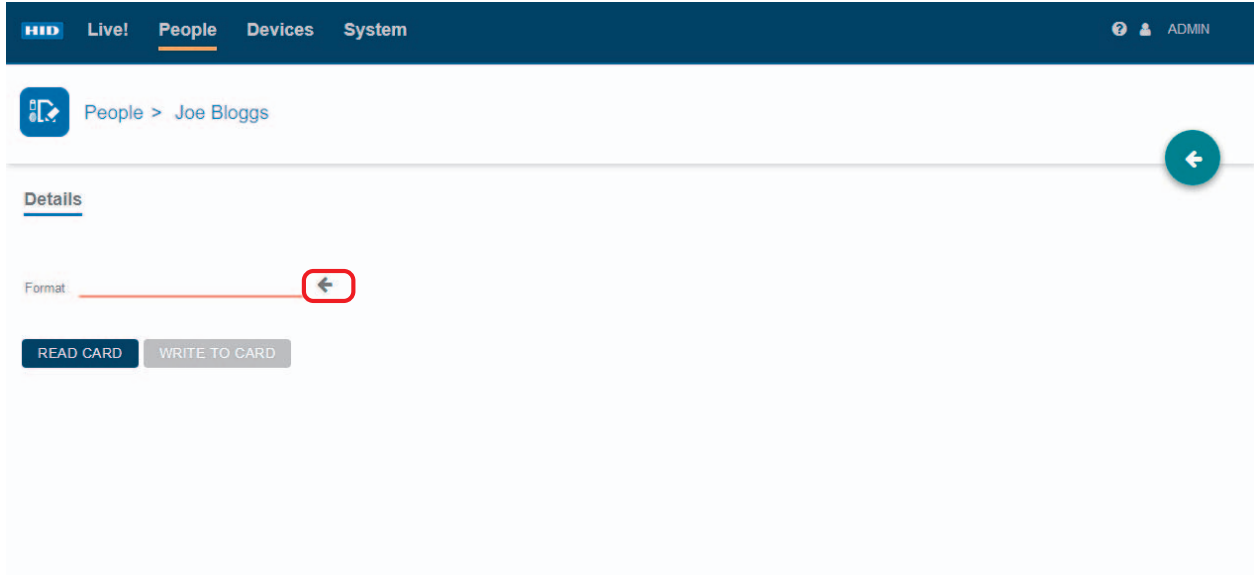


The operator can now collect and add biometric data associated with this enrolled person, see *Section 3.5.3 Enroll Biometrics*.

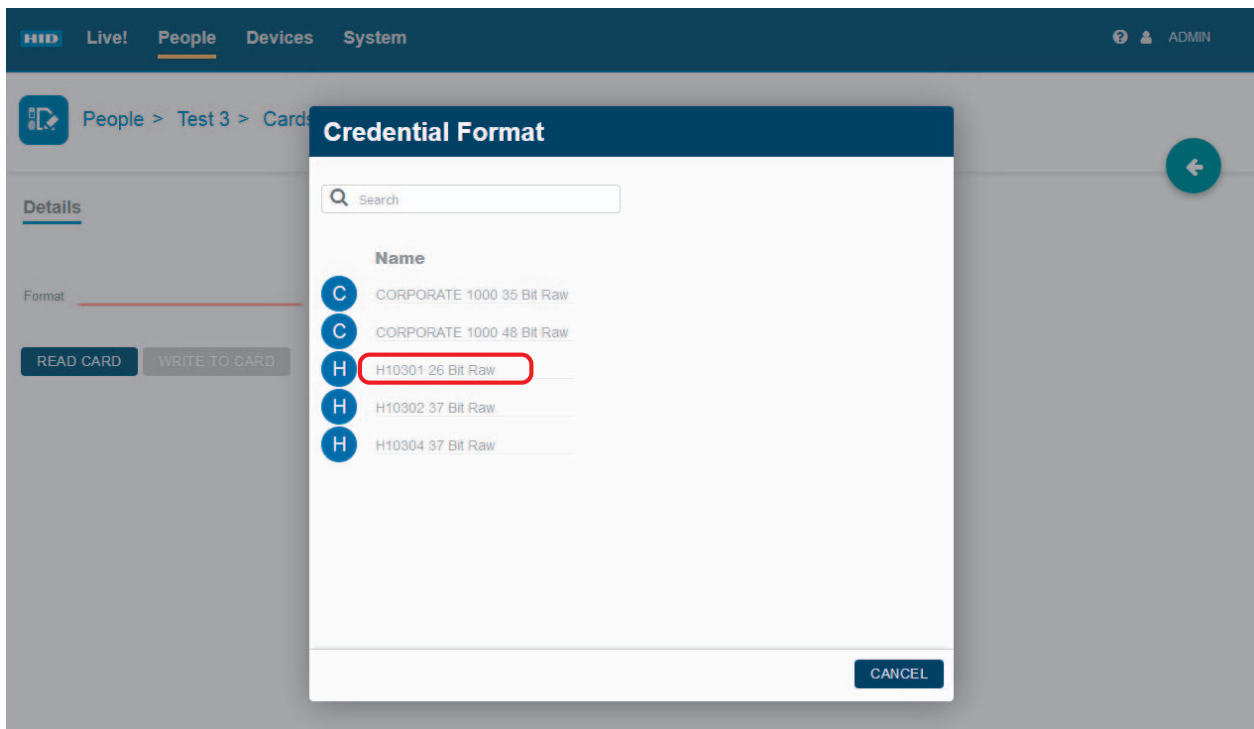
Manually enter card details

If no card is available to scan, card details can be entered manually:

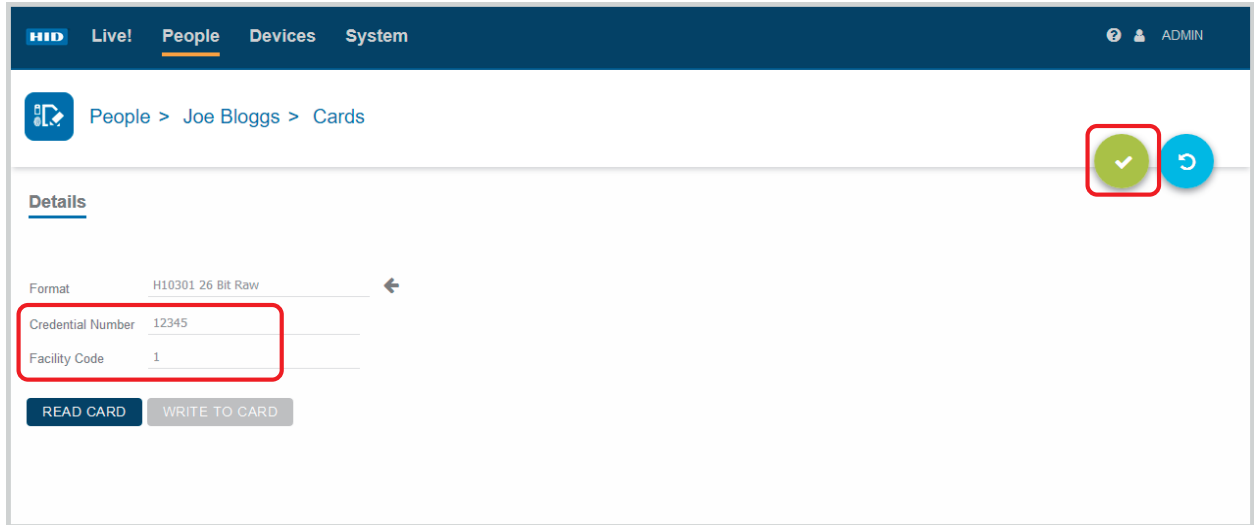
1. On the **Details** screen, select the arrow icon [←] associated with the **Format** field.



2. Select the **Credential Format**, recommended **H10301 26 Bit Raw**.

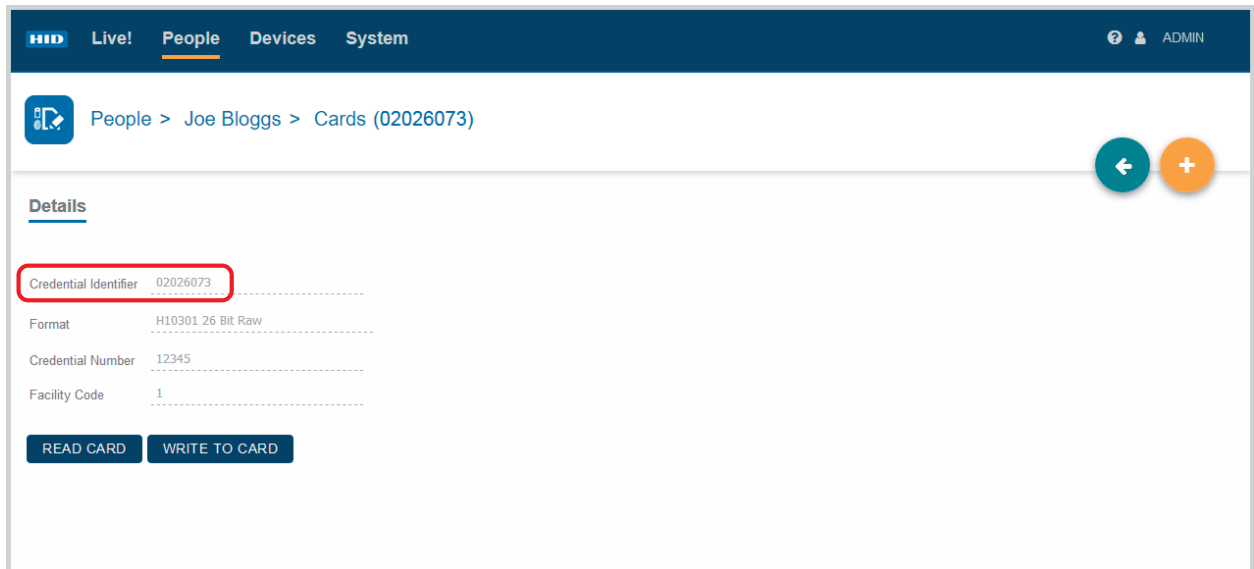


- 3. Enter a Credential Number (decimal) and Facility Code.
- 4. Click the **Save** icon [✓] to save these card details.



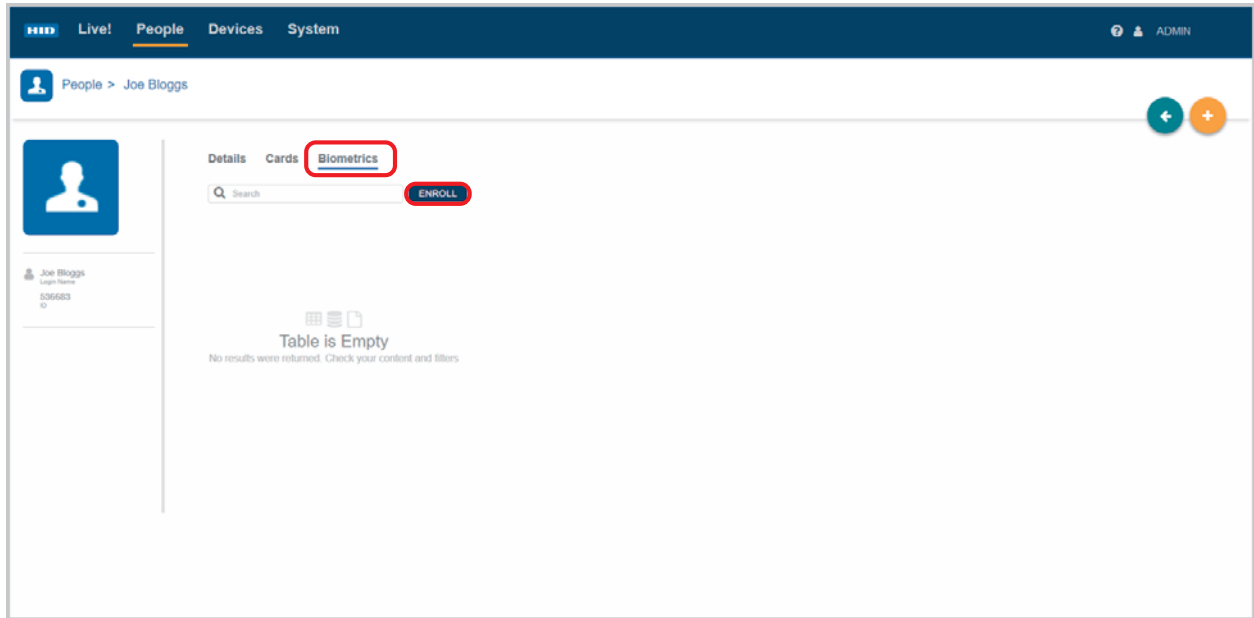
The manually entered card details are displayed with the decimal **Credential Number** converted to hexadecimal in the **Credential Identifier** field.

Note: The Credential Identifier created in HID Biometric Manager must be copied over to the third party PACS software running on the PACS Server.



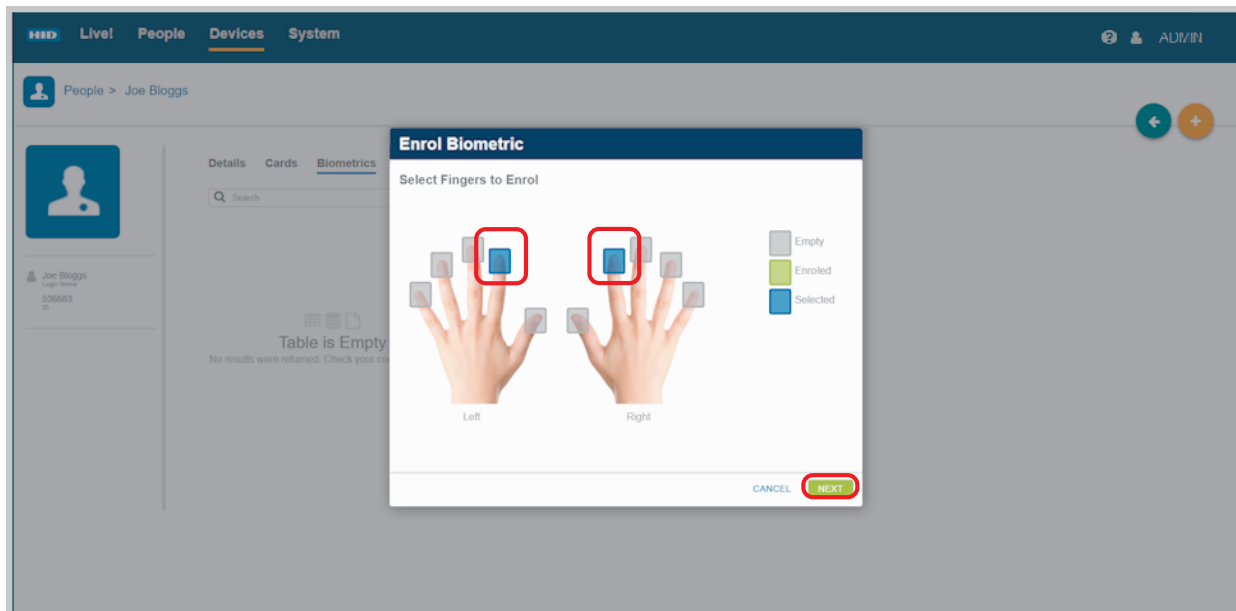
3.5.3 Enroll Biometrics

1. On the **People** screen select a displayed person record.
2. Click the **Biometrics** option.
3. Click **ENROLL** to start the biometric enrollment process.



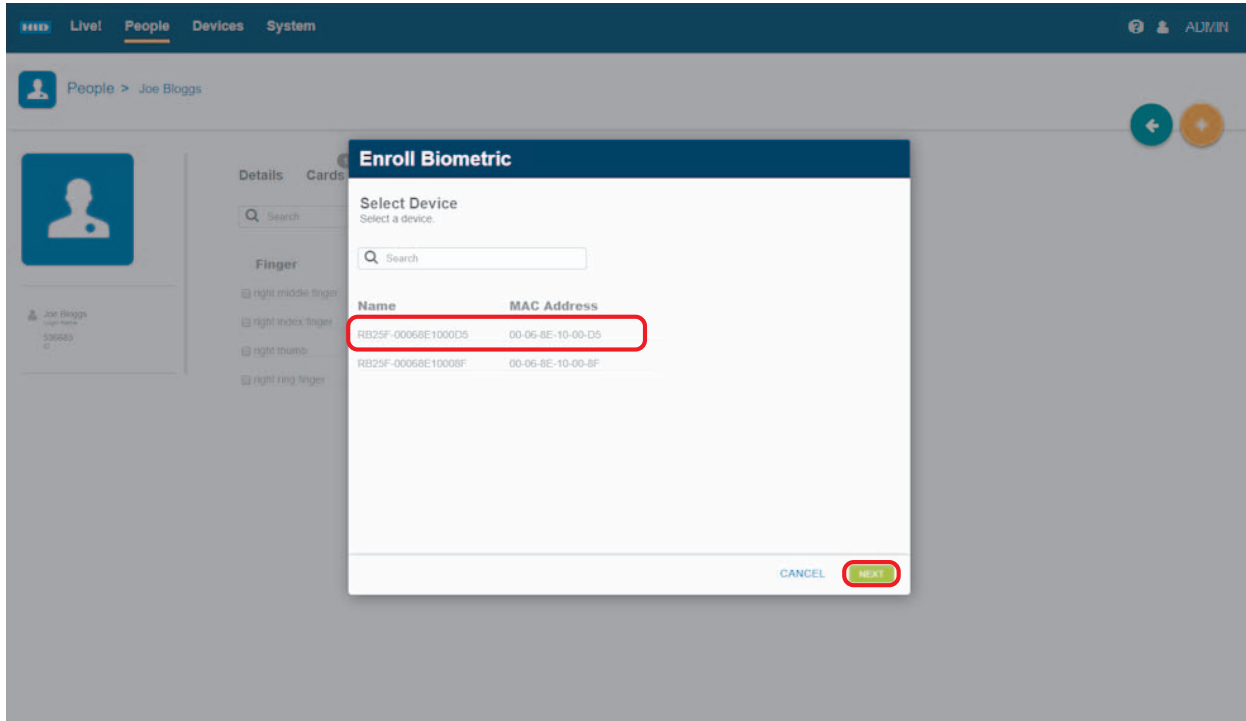
4. In the **Enrol Biometric** dialog select the fingers you wish to enroll and click **Next**.

Note: If you intend to make use of the **Template on Card** option as the authentication mode you will only be able to copy two of these templates to the card. However the system can store all ten fingers, if needed.



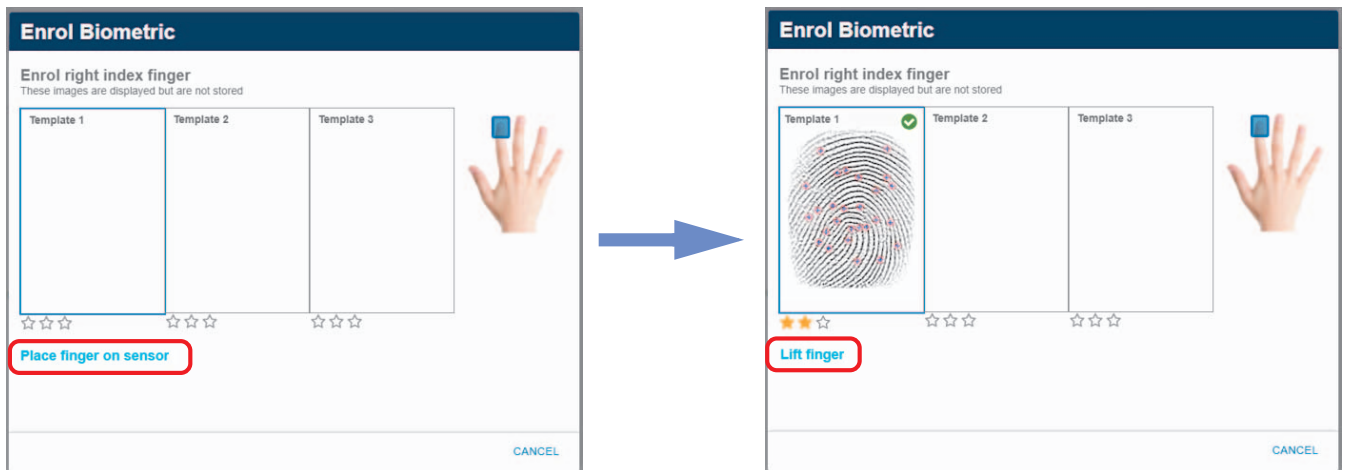
- 5. Select a device from the displayed list and click **Next**.

Note: Device names can be changed to a logical name for easier identification, see *Section 3.4.1 Configure device settings*.



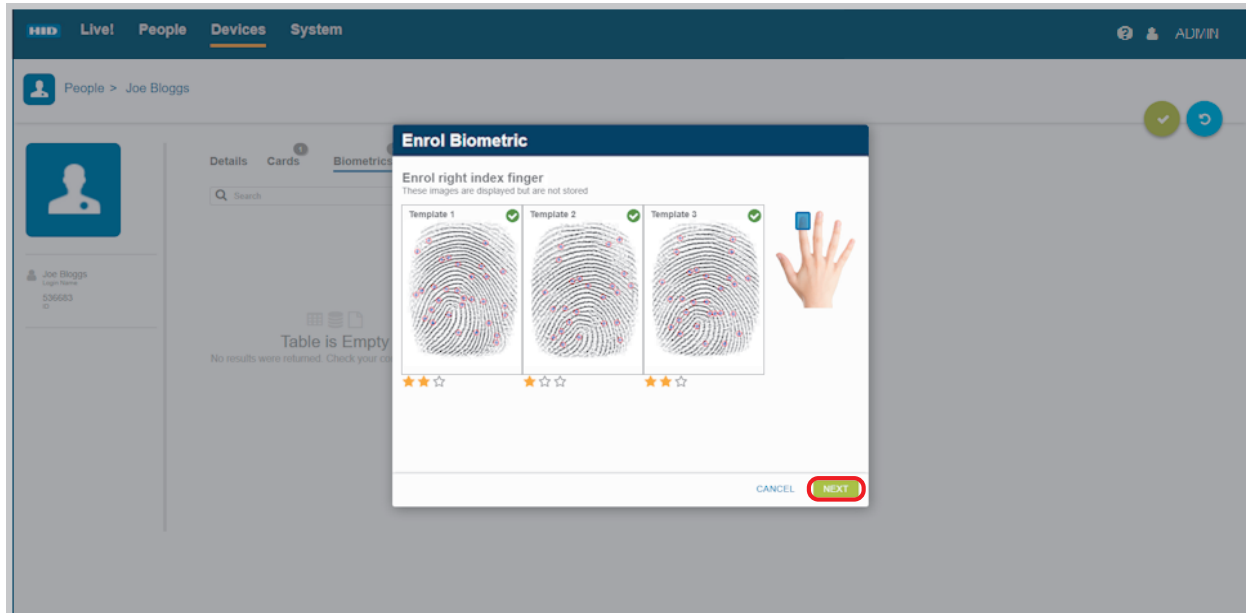
- 6. For the highlighted finger you will be prompted to **<Place finger on sensor>** followed by **<Lift finger>**. It is recommended that you follow the on-screen prompts, in the correct sequence, to ensure a successful finger scan.

Note: For information regarding the correct method of presenting fingers to the scanner during the biometric enrollment process, see *Appendix A - Fingerprint enrollment guidelines*.



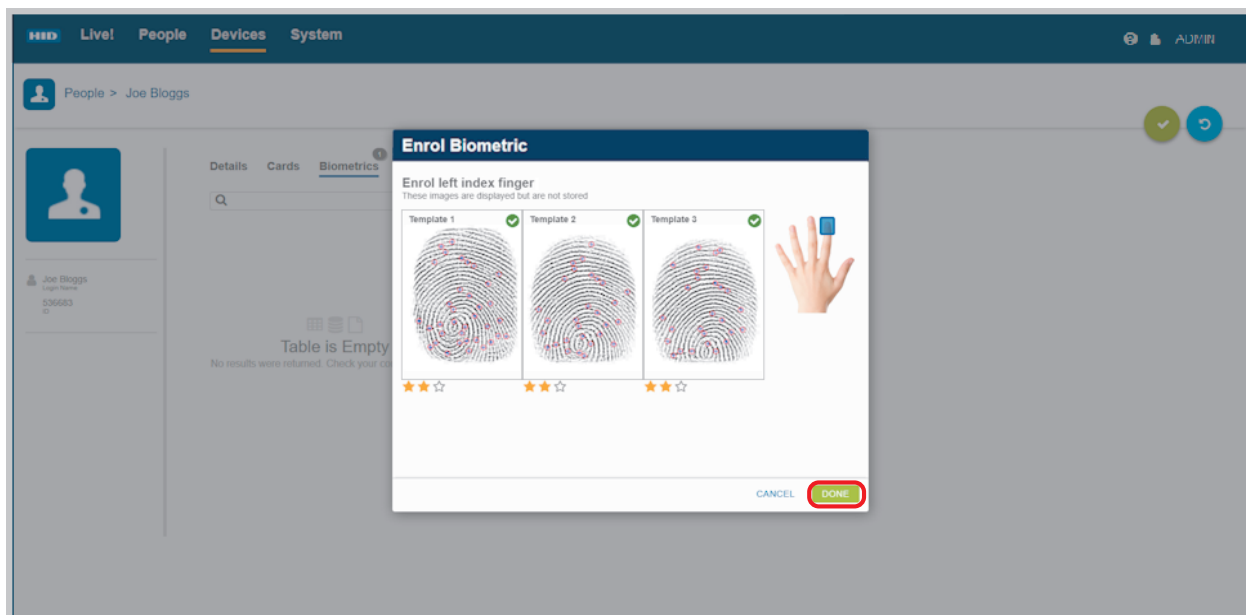
- Continue to follow the on-screen prompts until you have successfully scanned the first finger three times. Click **Next**.

Note: A score of at least one star per scan is needed. A poor score will require that you scan the finger another three times.



- You will be prompted to proceed onto the next finger scan. Follow the on-screen instructions until you have successfully scanned the next finger three times.
- When all of the selected fingers have been successfully scanned, click **Done**.

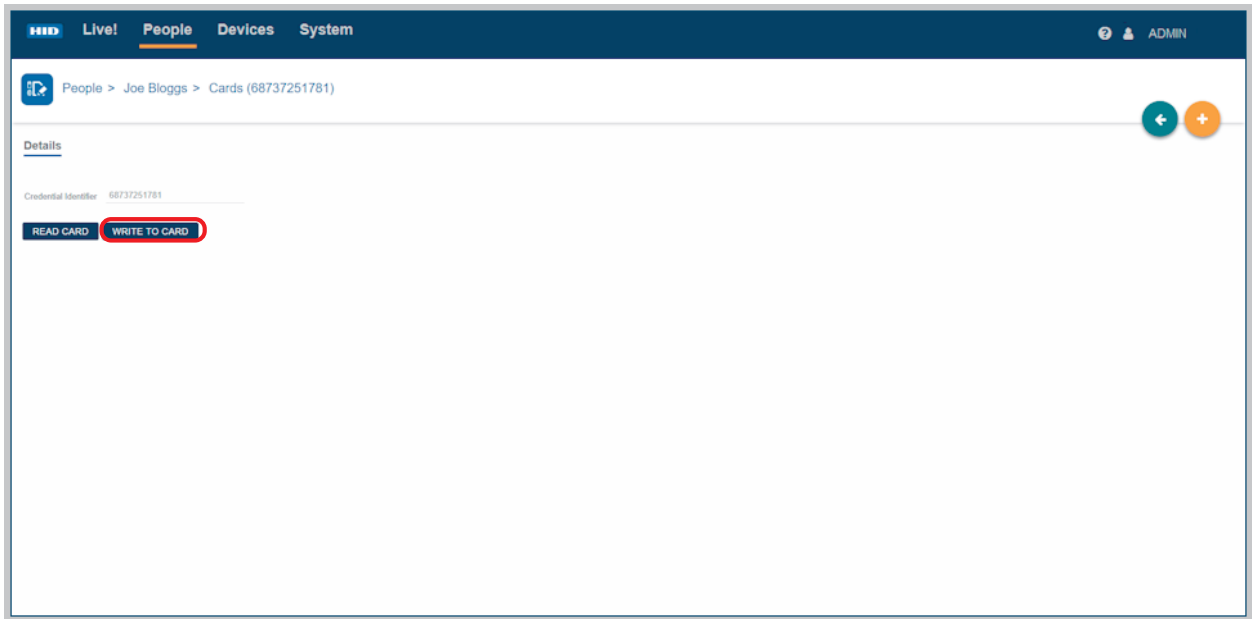
The enrolled fingerprint images will be associated with a card that has been allocated a short random card number in the system.



3.6 Write fingerprint templates to a card

If you intend to make use of the **Template on Card** option as the authentication mode you will only be able to copy two fingerprint templates to the card.

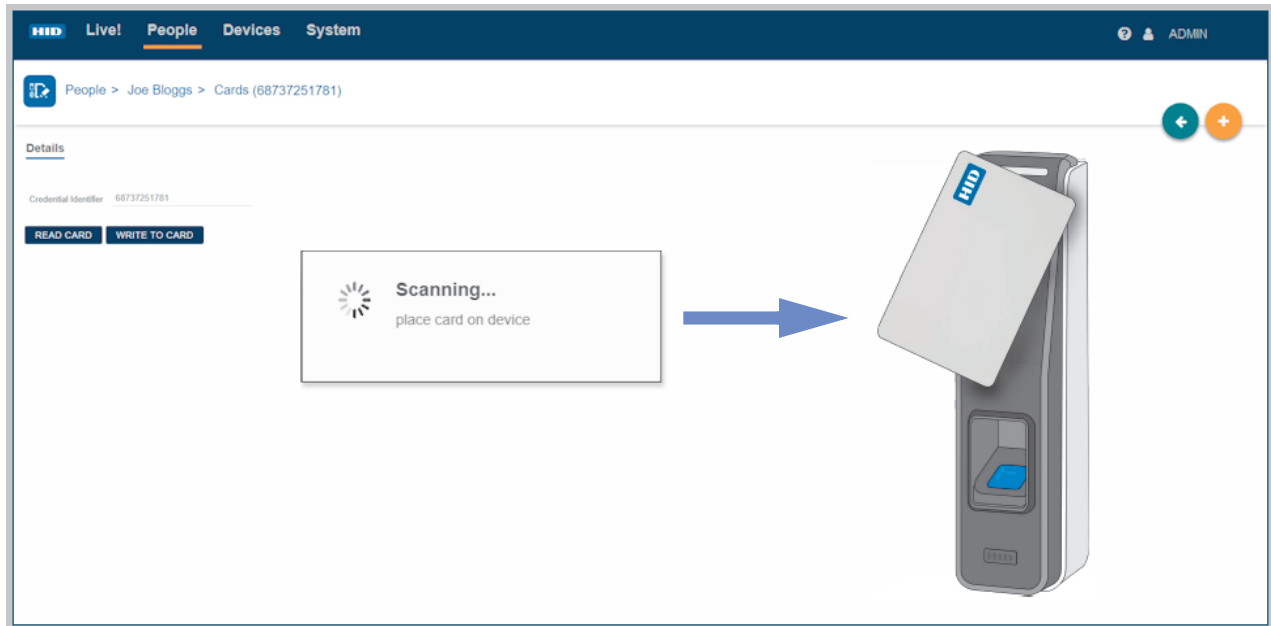
1. On the **People** screen select a displayed person record.
2. On the **Cards** screen select a displayed **Credential Identifier**.
3. Click **WRITE TO CARD** to copy the templates to the card.



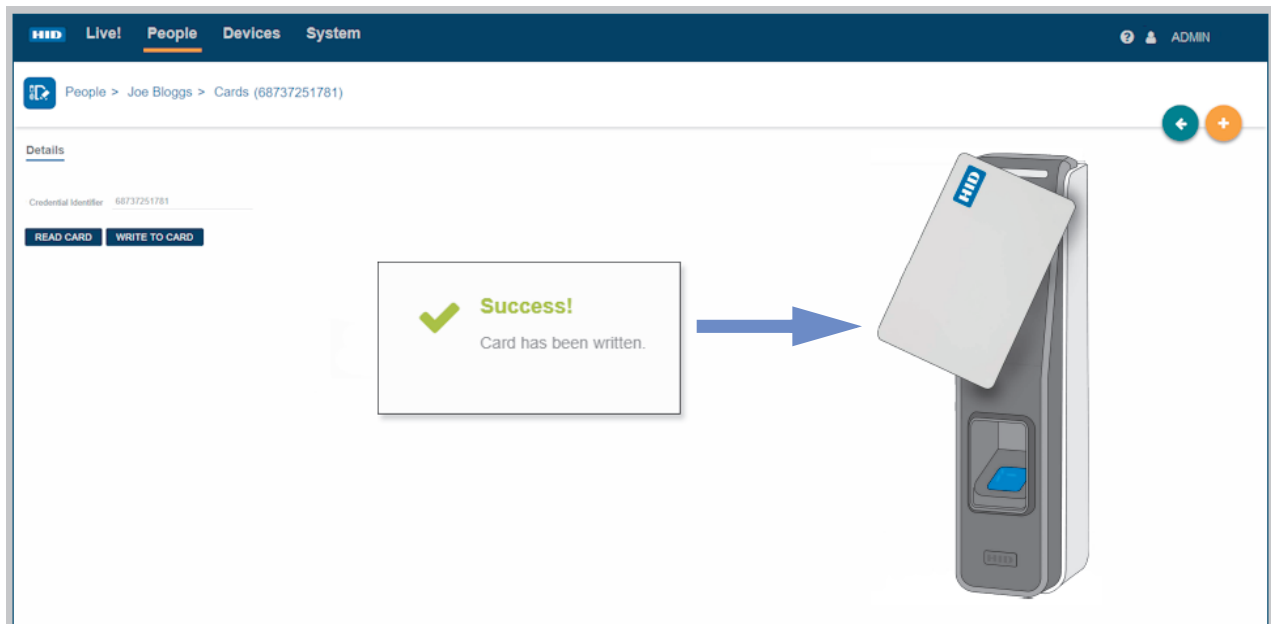
4. Select the fingers (maximum of two) you wish to be written to the card and click **WRITE TO CARD**.



5. You will have approximately five seconds to present the HID Seos card to the RB25F device in order to write the profiles to the card. The LED bar will flash while writing to the card. Keep the card in the reader field until the LED bar returns to its default color.



6. You will be notified when the card has been successfully written to.



For a **Template on Card** authentication mode, the enrolled person can now enter the door by presenting this card, immediately followed by the correct finger scan on the RB25F.

3.7 View Biometric Manager events

Actions carried out in Biometric Manager are logged. To view a HID Biometric Manager events, click the **Live!** option.

Note: Event information is only displayed after a device has been added.

The screenshot shows the HID Biometric Manager interface. At the top, there is a navigation bar with 'Live!' (highlighted with a red box), 'People', 'Devices', and 'System'. The 'Live!' button is a blue circle with a white exclamation mark. Below the navigation bar, there is a 'Transactions' section with a 'Details' sub-section. The 'Details' section shows a list of transactions for a user named 'Joe Bloggs'. The transactions are displayed in a table format with columns for Date/Time, Event, Device, Name, and Card.

Date/Time	Event	Device	Name	Card
2018-10-15 09:32:00	Biometric Match 1:1 Succeeded	RB25F	Joe Bloggs	6673251781
2018-10-15 09:31:56	RFID Credential Read	RB25F		
2018-10-15 09:20:05	RFID Credential Read	RB25F		
2018-10-15 09:20:04	RFID Credential Write	RB25F		
2018-10-15 09:20:02	RFID Credential Write	RB25F		
2018-10-15 09:10:44	RFID Credential Write	RB25F		
2018-10-15 09:10:39	RFID Credential Write	RB25F		
2018-10-15 09:09:53	RFID Credential Read	RB25F		
2018-10-15 09:09:52	RFID Credential Write	RB25F		
2018-10-15 09:09:50	RFID Credential Write	RB25F		
2018-10-15 09:09:04	RFID Credential Read	RB25F		
2018-10-15 09:09:03	RFID Credential Write	RB25F		
2018-10-15 09:08:58	RFID Credential Write	RB25F		
2018-10-15 06:33:33	Configuration Updated	RB25F		
2018-10-15 06:33:33	Configuration Updated	RB25F		
2018-10-15 06:33:32	Configuration Updated	RB25F		
2018-10-15 06:33:32	Configuration Updated	RB25F		
2018-10-15 06:30:44	Tables Initialized	RB25F		
2018-10-12 13:27:54	RFID Credential Read	RB25F-02BA96DECC2		
2018-10-12 12:34:54	Configuration Updated	RB25F-02BA96DECC2		
2018-10-12 12:34:54	Configuration Updated	RB25F-02BA96DECC2		
2018-10-12 12:34:54	Configuration Updated	RB25F-02BA96DECC2		
2018-10-12 12:33:22	Configuration Updated	RB25F-02BA96DECC2		

Appendix A

A Fingerprint enrollment guidelines

The iCLASS SE® RB25F Biometric Reader/Controller is capable of extracting quality features even from fingers with poor conditions. Nevertheless, correct placement of fingers on the sensor during enrollment helps consistency in fingerprint recognition. Adhere to the following general guidelines and RB25F specific guidelines to enroll optimal fingerprint images from a user's finger to improve recognition performance.

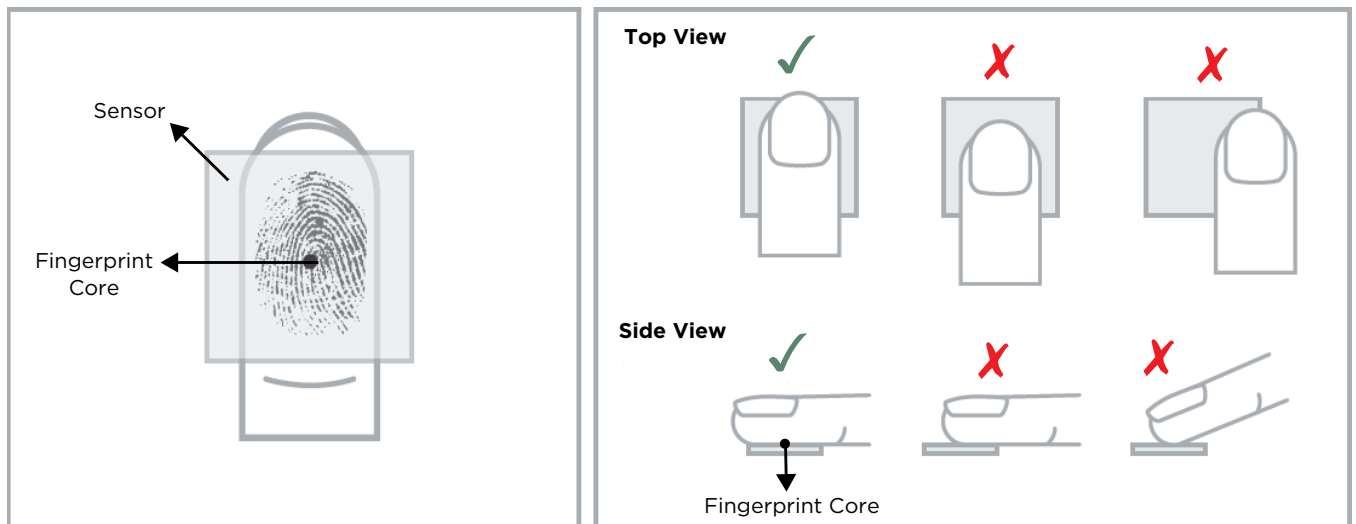
A.1 General guidelines

Choose the ideal fingers to enroll

For correct positioning of finger on the sensor, it is recommended to use index or middle fingers.

Correct positioning of finger on sensor

- **Maximum contact area:** Place your finger to completely cover the sensor with maximum contact surface.
- **Place on the center:** Position center of fingerprint (core) on the center of the sensor.
- **Hold your finger still:** Once you place your finger on the sensor, hold finger still until prompted to remove finger.



Sensor cleaning

The fingerprint sensor can become soiled by user’s fingers, dust, or other sources. This contamination may affect image quality, degrading authentication performance. It is therefore recommended that you periodically clean the RB25F sensor.

In order to avoid scratching the sensor surface use soft lint-free material (or a cotton swab), with gently movements to clean the capture area.



CAUTION

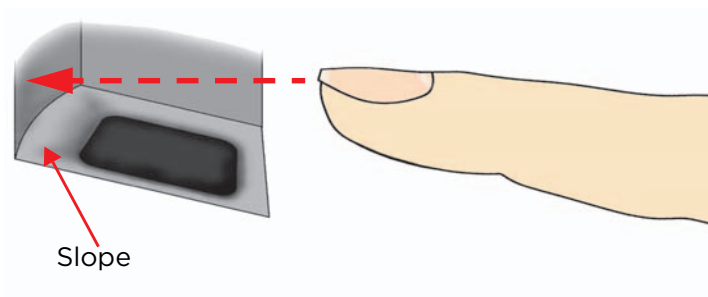
Do not use acidic liquids, alcohol or abrasive materials to clean the sensor.

Common reasons for enrollment failure

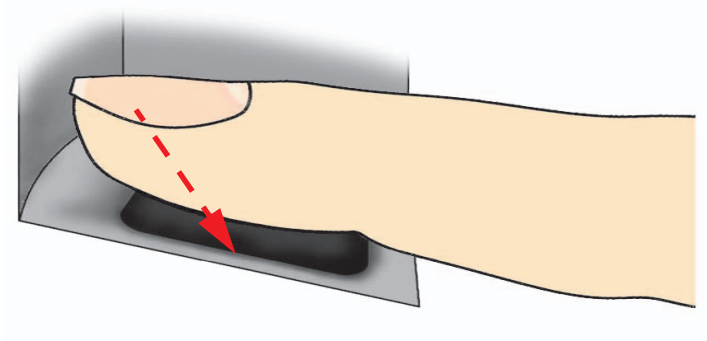
Problem	Solution
Finger is too dry or dirty	Rub the finger in the palm of your hand to moisten/clean it
Finger applied too lightly	Place finger firmly and flat onto the sensor surface
Finger positioned incorrectly	Your finger should cover most of the sensor window
Finger removed or moved during the scan process	Hold your finger still and do not slide it on the sensor window until the scanning process is complete
Injury or wear has changed the fingerprint pattern	Contact the administrator as you may need to enroll another finger

A.2 Fingerprint enrollment best practices for RB25F

1. Insert your finger into the RB25F sensor area so the finger tip touches the back wall and rest softly on the sensor slope.



2. Slide your finger down so that it completely covers the sensor window contact surface.



3. Apply gentle pressure on the sensor to slightly flatten your finger and expose a maximum usable area.
4. Keep your finger still until prompted to remove finger.



This page is intentionally left blank.

Appendix B

B Acronyms and terminology

Term	Definition
Authentication Mode (RB25F)	<p>Template on Card: The RB25F is waiting for a Credential (Card) to be presented. It retrieves all the biometric templates from the credential. If the presented finger matches the biometric templates retrieved from the credential a Grant Access is recommended. This is a 1:1 Verification match against Template on Card (ToC). The sensor is not armed (blue light off) until the Credential is presented.</p> <p>Card + Finger: The RB25F is waiting for a Credential (Card) to be presented. It looks up the user ID and all associated biometric templates in it's local device database. If the presented finger matches the biometric templates retreated from the local database a Grant Access is recommended. This is a 1:1 Verification match against Template on Device (ToD). The sensor is not armed (blue light off) until the Credential is presented.</p> <p>Finger Only: The RB25F is waiting for a finger to be presented that is stored in its local device database. If the presented finger matches one stored in the database a Grant Access is recommended. This is a 1:N Identification match against Template on Device (ToD). The sensor is always armed (blue light on).</p> <p>Card Only: The RB25F is waiting for a Credential (Card) to be presented. It reads the PACS data only and always recommends a Grant Access. The sensor is never armed (blue light off).</p>
Biometric spoofing	Biometric spoofing is a method of fooling a biometric identification management system. An artificial object (for example, a fingerprint mold made of silicon) is presented to the biometric scanner that imitates the unique biological properties of a person which the system is designed to measure.
BLE	Bluetooth Low Energy (formerly marketed as Bluetooth Smart) is a wireless personal area network technology.
ERR	The Equal Error Rate (EER) is the common value indicating that the proportion of false acceptances (FAR) is equal to the proportion of false rejections (FRR). The lower the EER value, the higher the accuracy of the biometric system.
False Accept Rate (FAR)	The False Accept Rate (FAR) is the measure of the likelihood that the biometric security system will incorrectly accept an access attempt by an unauthorized user.
False Reject Rate (FRR)	The False Reject Rate (FRR) is the instance of a security system failing to verify or identify an authorized person.
FTA	Failure To Acquire. The biometric system failure to extract usable identification data from a biometric sample.
Identification (of Identity)	Typically finding a matching template in a large database of templates. 1:N matching.

Term	Definition
LFD	Live Finger Detection. This is used in some markets instead of Spoof. It is also used to refer to insuring a severed finger is not being presented at the sensor.
MINEX	Minutia Interoperability Exchange. The MINEX program is dedicated to the evaluation and development of the capabilities of fingerprint minutia matchers running on ISO/IEC 7816 smart cards.
M-Series	Mercury Platform Series of Products.
MSI	Multi-Spectral Imaging.
OSDP	Open Supervised Device Protocol (OSDP) is an access control communications standard developed by the Security Industry Association (SIA) to improve interoperability among access control and security products.
PAD	Pressure Attack Detection.
PD	Presence Detection.
ROC	Receiver Operating Characteristic.
SDK	Software Development Kit.
SIA	Structure Image Acquisition.
System Mode (RB25F)	Reader: Reader mode allows the LED & Buzzer to be controlled over Wiegand. Controller: Controller mode is a demo mode that allows the demonstration of LED & Buzzer without the use of a third party controller.
Tap	The Tap gesture with a mobile device for door opening. The Tap operation is typically used when the mobile device is in close proximity to the reader. Approximately 0 inch to 4 inches (0 cm to 10 cm).
Twist and Go	The Twist gesture with mobile device for door opening. The Twist operation is typically used when the mobile device is at a longer distance from the reader. Approximately 1 ft to 10 ft (0.3 m to 3 m).
ToC	Template on Card. The PACS data is read from the card.
ToD	Template on Device. The PACS data is read from the device database.
vCOM	V-Series Command Protocol.
Verification (of Identity)	Typically a fingerprint template is stored on a card and checked against a finger presented to the finger print sensor. 1:1 matching.

This page is intentionally left blank.

