



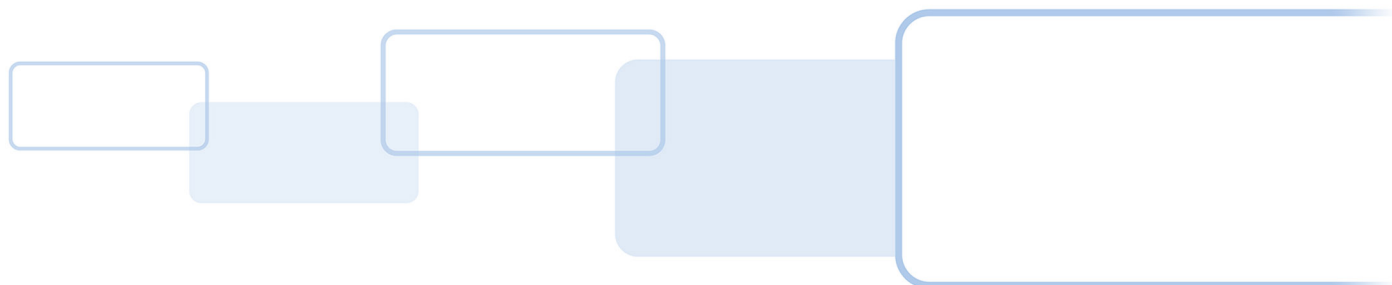
iCLASS SE® RB25F

Biometric Reader/Controller

ADMINISTRATION GUIDE

PLT-04029, Rev. A.2

August 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.

MIFARE is a registered trademark of NXP Semiconductors N.V. and is used under license.

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 Related material	5
1.4 Physical Access Control System overview	6
1.5 HID Biometric Manager	7
1.5.1 Credential Database	7
1.5.2 Data Import	7
1.5.3 Reader Service	7
1.6 Browser compatible device	7
1.7 RB25F	7
1.8 Panels and Door Controllers	8
1.9 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
2.3.4 Direct connection to PC	14
2.4 Hardware reset the RB25F	15
Section 3: HID Biometric Manager	17
3.1 HID Biometric Manager overview	17
3.1.1 System 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 Configure time zone setting	23

3.2.4 Configure software/firmware update settings	25
3.2.5 Create Biometric Manager operators	27
3.3 Device profiles	29
3.3.1 Edit a device profile	29
3.3.2 Create a device profile	32
3.3.3 Delete a device profile	34
3.4 Device installation and configuration	35
3.4.1 Configure device settings	37
3.4.2 Device firmware update	40
3.4.3 Reset a device	43
3.4.4 Uninstall a device	44
3.5 Enrollment	45
3.5.1 Enroll People	45
3.5.2 Enroll Cards	47
3.5.3 Enroll Biometrics	51
3.6 Write fingerprint templates to a card	54
3.7 System monitoring and Reports	56
3.7.1 View Biometric Manager events	56
3.7.2 Transaction Reports	57
Appendix A: Biometric Manager Mobile Access setup	59
A.1 Setup prerequisites	59
A.1.1 HID Mobile Identities setup	59
A.1.2 HID Reader Manager setup	59
A.1.3 Mobile Access user setup	59
A.2 Validate a Reader Manager account in HID Biometric Manager	60
A.3 Load a MOB key onto a device	62
A.4 Test MOB keys are working correctly	64
Appendix B: Fingerprint enrollment guidelines	65
B.1 General guidelines	65
B.2 Fingerprint enrollment best practices for RB25F	66
Appendix C: Acronyms and terminology	69



Section 1

1 Introduction

1.1 Document purpose

This document gives an overview of the iCLASS SE® RB25F Biometric Reader 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, 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 Related material

Refer to the documents listed in the following table for information related to the content of this guide:

Refer to this document:	For information on:
<i>HID Mobile Access Solution Overview</i> (PLT-02078)	The HID Mobile Access solution, how system components interact with each other, and how to get the best out of the solution.
<i>HID Mobile Access Frequently Asked Questions</i> (PLT-02085)	The Mobile Access solution, Mobile Access Portals, Mobile IDs, Mobile Access Apps, Mobile-enabled readers, onboarding process, and security
<i>HID Reader Manager Solution User Guide (iOS)</i> (PLT-03683)	The HID Reader Manager solution, HID Reader Manager App for iOS devices, and the HID Reader Manager Portal.
<i>HID Reader Manager Solution User Guide (Android)</i> (PLT-03858)	The HID Reader Manager solution, HID Reader Manager App for Android devices, and the HID Reader Manager Portal.
<i>HID Mobile Access SIS Portal User Guide</i> (PLT-03613)	Procedures for Mobile Access Administrators to manage mobile users and credentials through the HID Mobile Access SIS Portal.
<i>HID Mobile Access App User Guide</i> (PLT-02077)	Installation, configuration, and use of the HID Mobile Access App for iOS and Android devices.

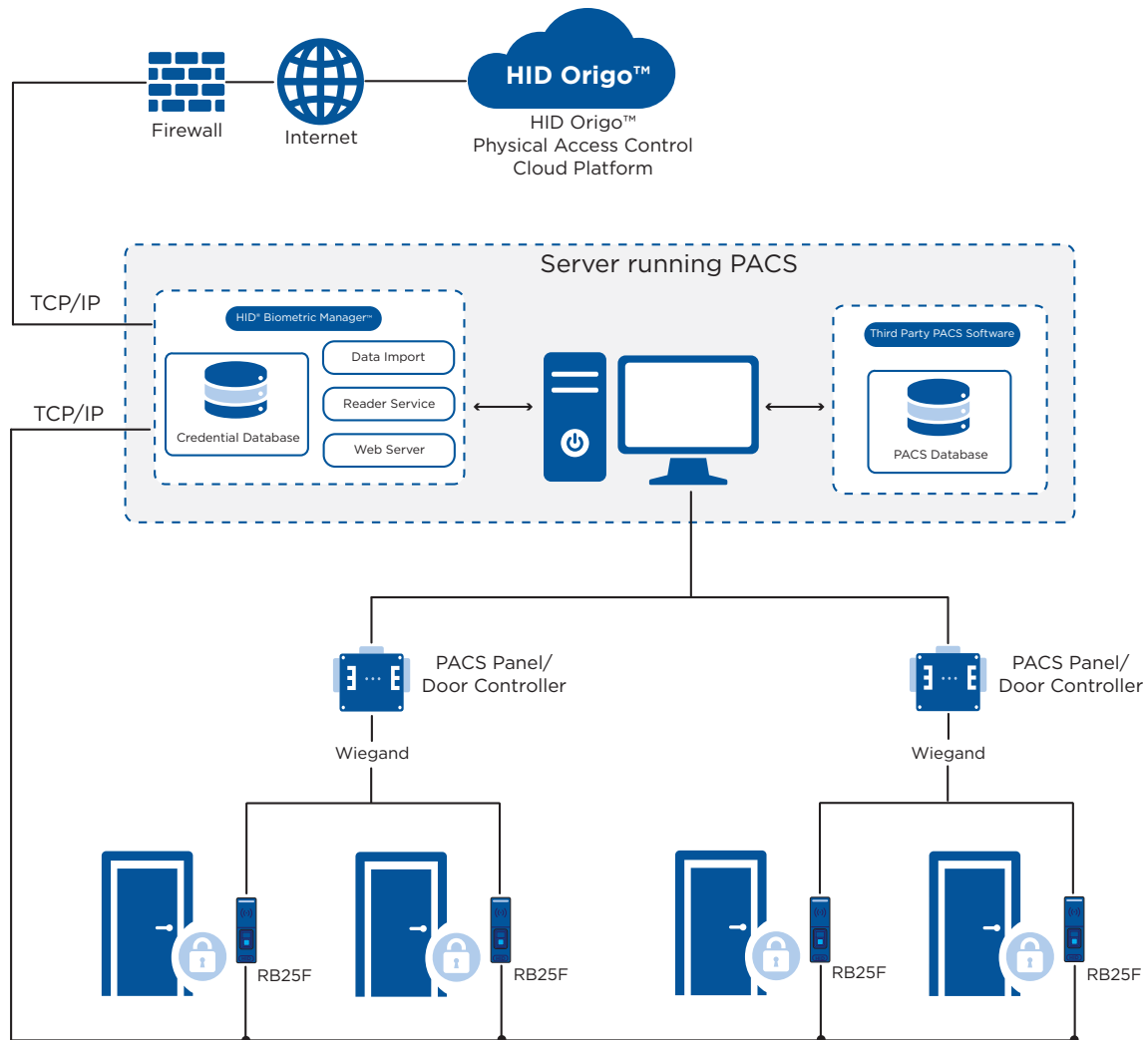
1.4 Physical Access Control System overview

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.



1.5 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.

1.5.1 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.

1.5.2 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.

1.5.3 Reader Service

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

1.6 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.

1.7 RB25F

The RB25F is a biometric card and fingerprint reader. It authenticates users according to one of five modes (see *Appendix C - Acronyms and terminology*) 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.

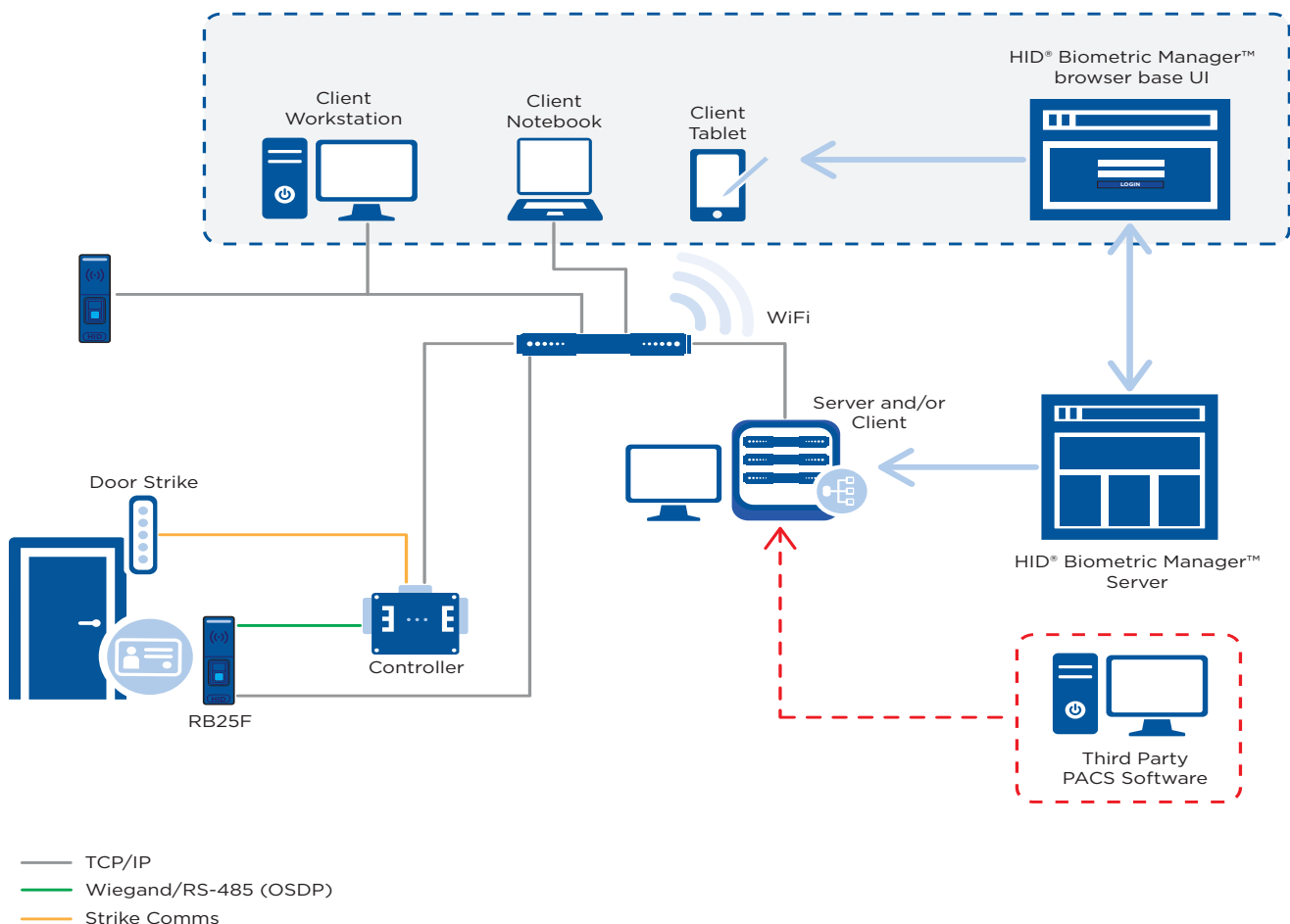
1.8 Panels and Door Controllers

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 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.



1.9 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

The HID Biometric Manager install wizard carries out setup and assigns a hostname.

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.

Note: Device controller functionality will be introduced in a future release through an API.

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

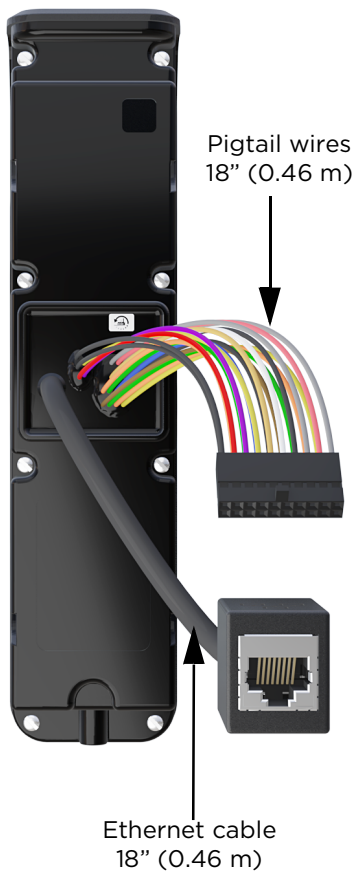
The following shows RB25F wiring functions and color codes.

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		
	Black	Ground		
DC Power	Red	Power +12 V		
	Black	Power Ground		

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

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

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

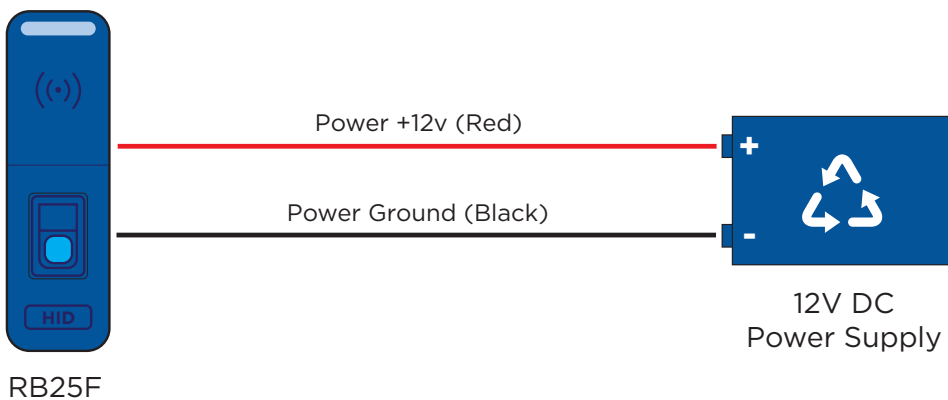
Relay/Inputs: Reserved for future device controller functionality through an API

2.3 System connections

2.3.1 Power supply connection

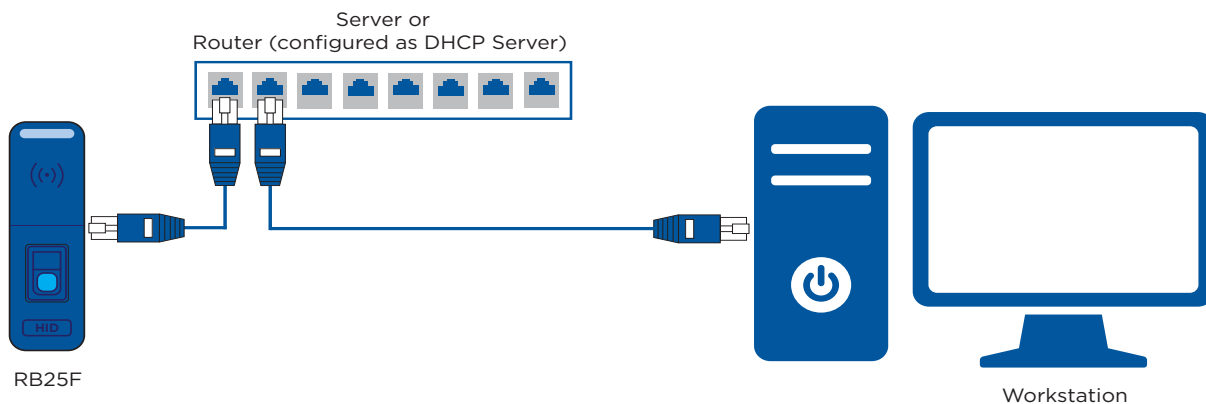
For the RB25F power supply use a 12V DC power supply adapter capable of at least 2A, with IEC/EN 60950-1 approval. If additional power consuming devices are included, make sure to use a power adapter that is able to supply the total current needed.

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



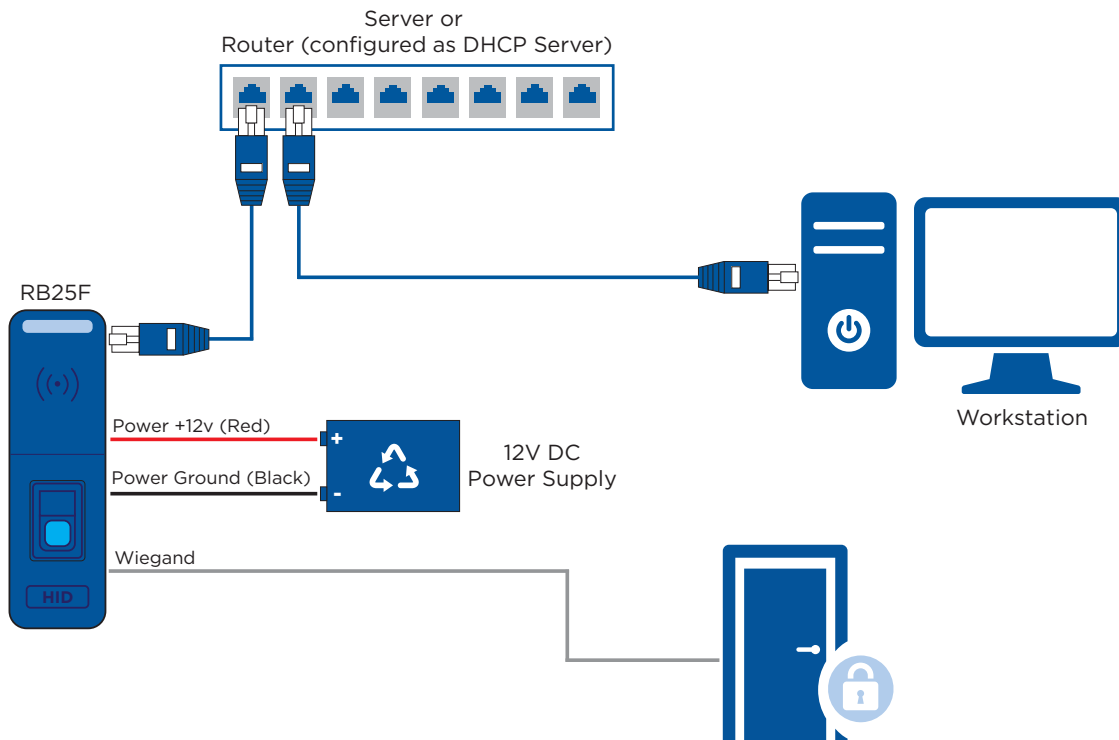
2.3.2 Network connection

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



2.3.3 Standalone operating mode connections

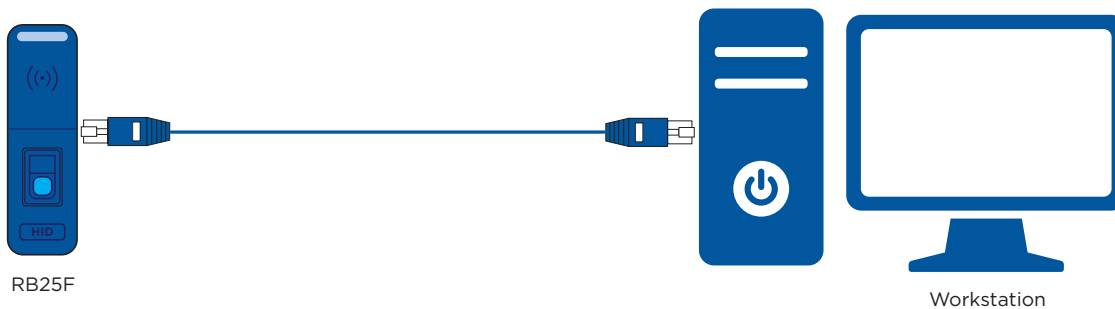
RB25F devices can be used in standalone operating mode.



2.3.4 Direct connection to PC

Direct connection to PC using an auto assigned IP address or a static IP address.

Note: It can take up to five minutes for this connection type to configure.



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 3.4.3 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 mounting bracket.
2. Slide the RB25F upwards and remove from the mounting bracket.
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 device settings 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*) and enroll people in the system, add credentials, collect and store associated biometric data (see *Section 3.5 Enrollment*).
- **Device Administrator:** This operator role is intended for HID partner technicians involved in the setup and maintenance of the Biometric Management environment as well as configuration and update of the RB25F. This operator role has limited access to user information.
- **Enrollment:** 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 System requirements

HID Biometric Manager system 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

HID Biometric Manager TCP port usage:

- 1883 Communication (MQTT Broker)
- 8883 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:

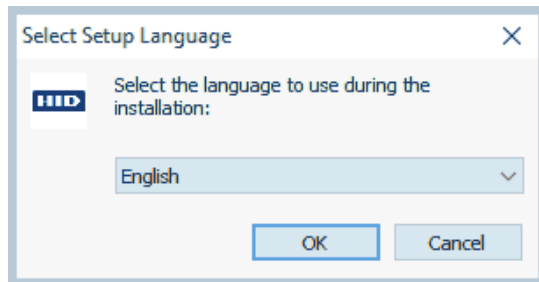
<https://www.hidglobal.com/rb25f>

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

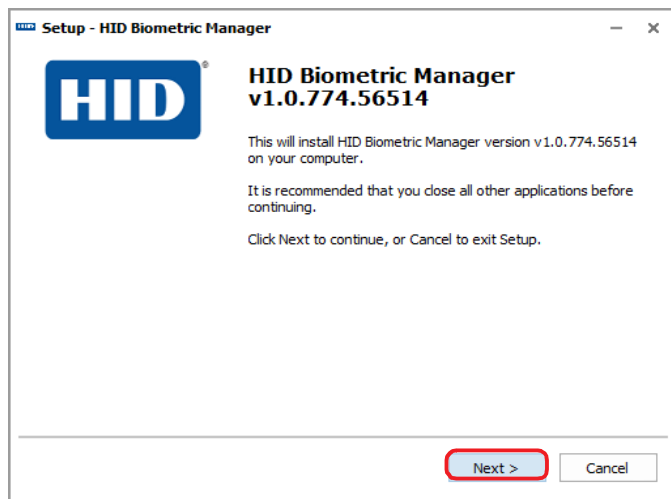
Note: If the server system language is configured to one of the supported languages then the install wizard instructions and Biometric Manager will automatically default to the server system language. Supported languages:

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

3. Select the HID Biometric language.

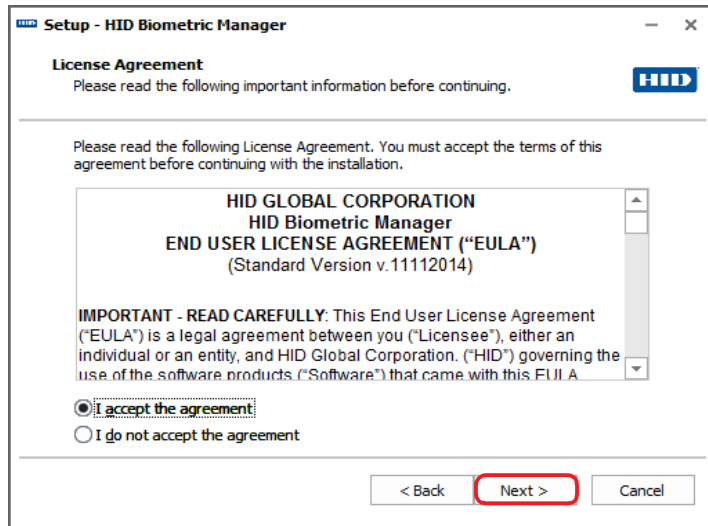


4. On the initial installation wizard screen, click **Next**.

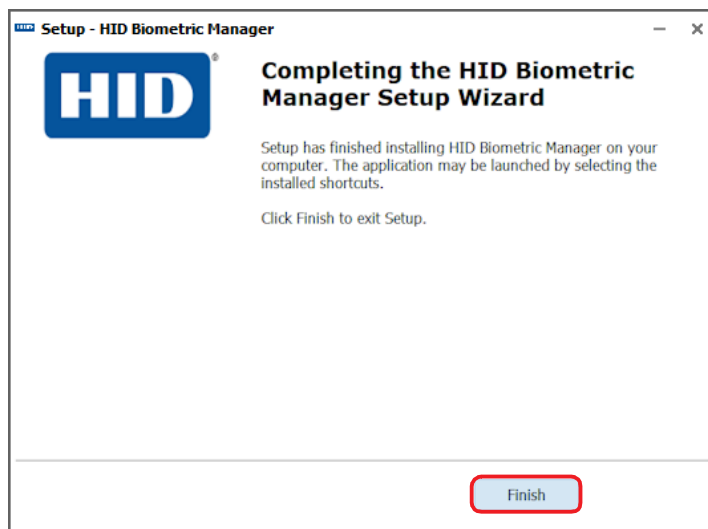


5. Read the License Agreement. Select **I accept the agreement**, and click **Next**.

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:

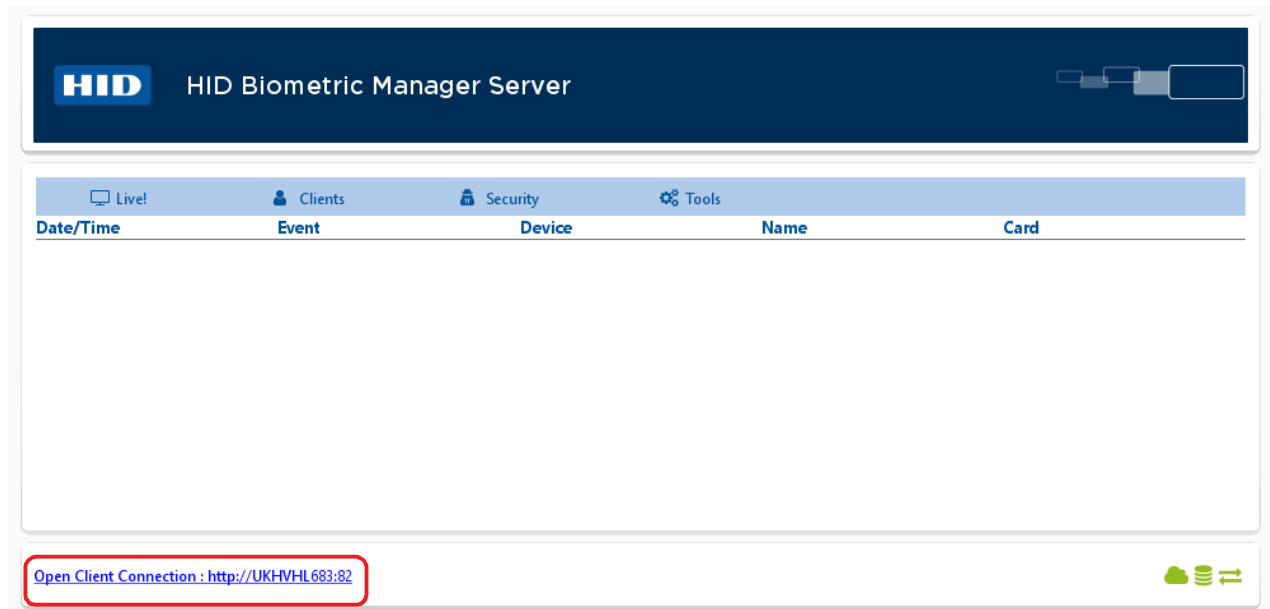
1. Double-click on the HID Biometric Manager desktop shortcut or navigate to the installation folder (usually, **C:\Program Files (x86)\HID Global\Biometric Manager\bin**) and double-click on the **HID Biometric Manager.exe** file.

Note: The size of the database may impact how long it takes the Biometric Manager application to launch. Start up feedback is indicated with an on screen progress bar.

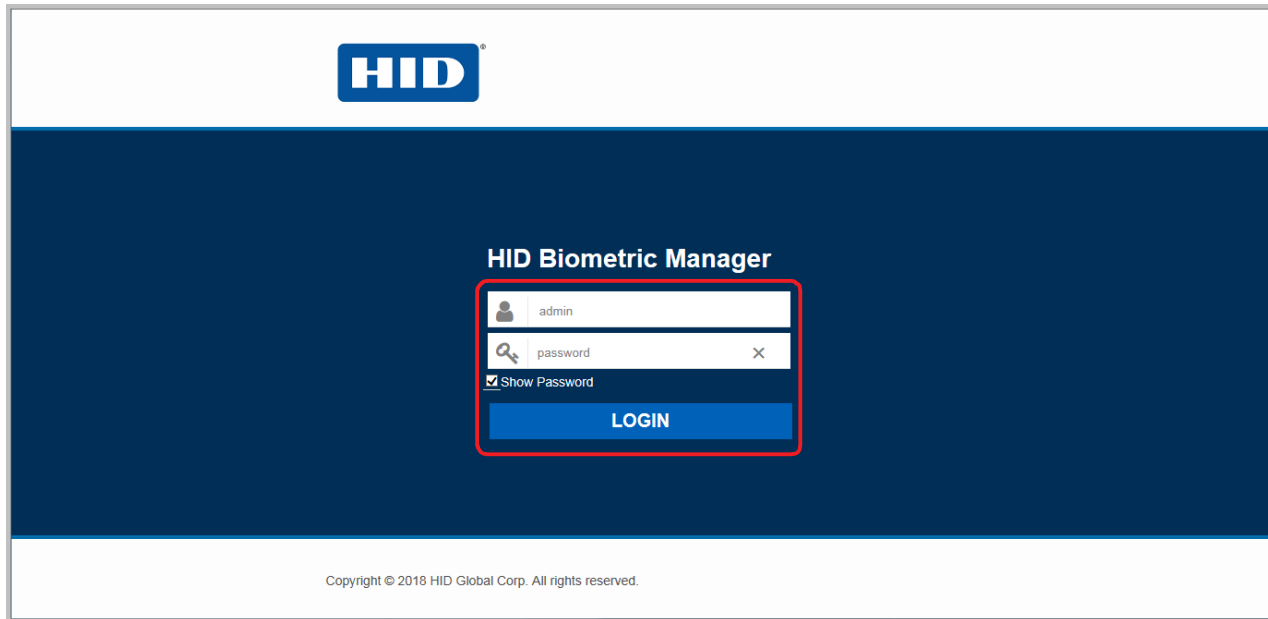
2. On the HID Biometric Manager Server application screen, click on the **Open Client Connection** link to access the HID Biometric Manager application login screen. Record the **Client Connection** link url as this can be distributed and used to access the HID Biometric Manager application from a client 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>

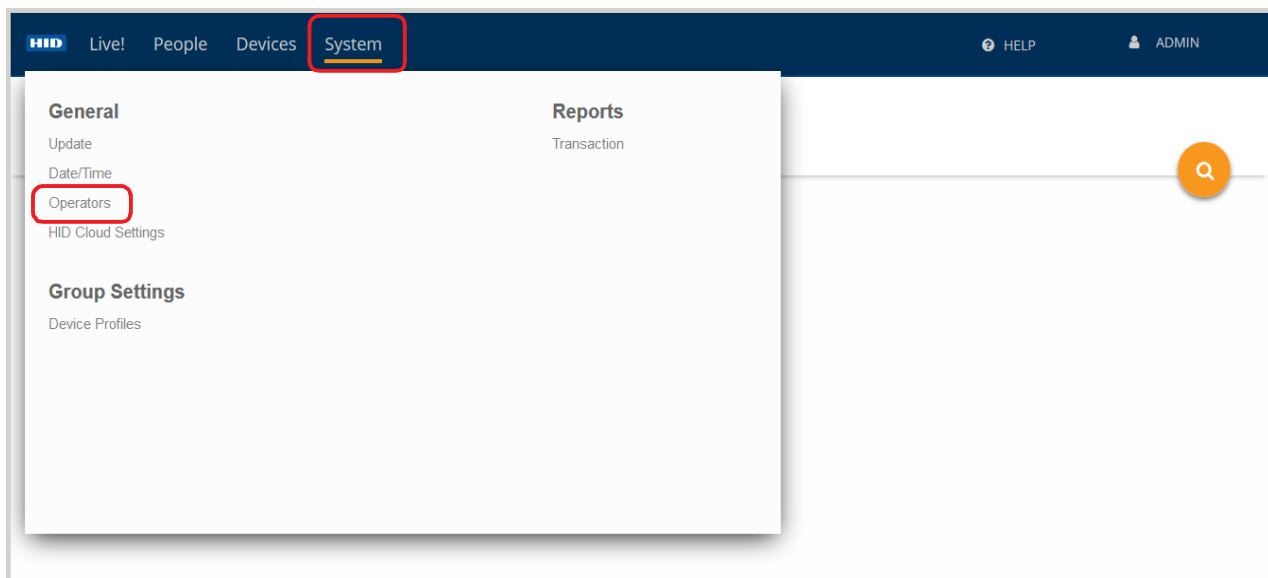


3. Enter the initial default admin User Name (**admin**) and Password (**password**) and click **LOGIN**.

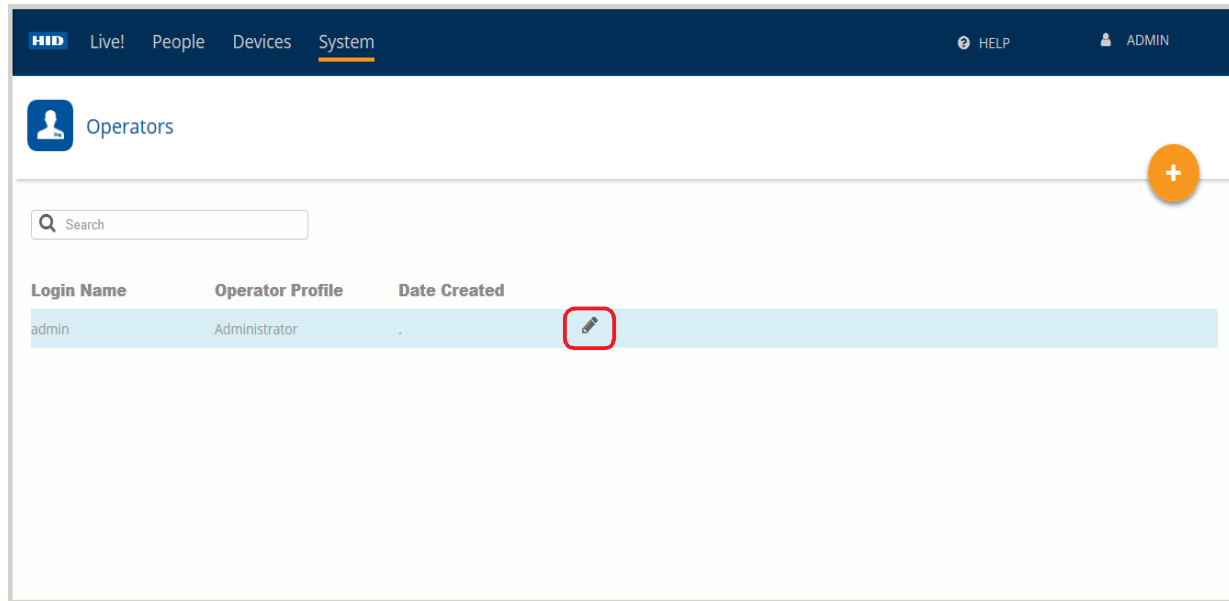


The screenshot shows the HID Biometric Manager login interface. At the top is the HID logo. Below it, the title "HID Biometric Manager" is centered. A login form is highlighted with a red border, containing a username field with "admin", a password field with "password", a "Show Password" checkbox, and a blue "LOGIN" button. At the bottom of the page, a copyright notice reads: "Copyright © 2018 HID Global Corp. All rights reserved."

4. For security reasons it is recommended that the default admin login credentials are immediately changed. Click on the **System** option and select **Operators**.



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

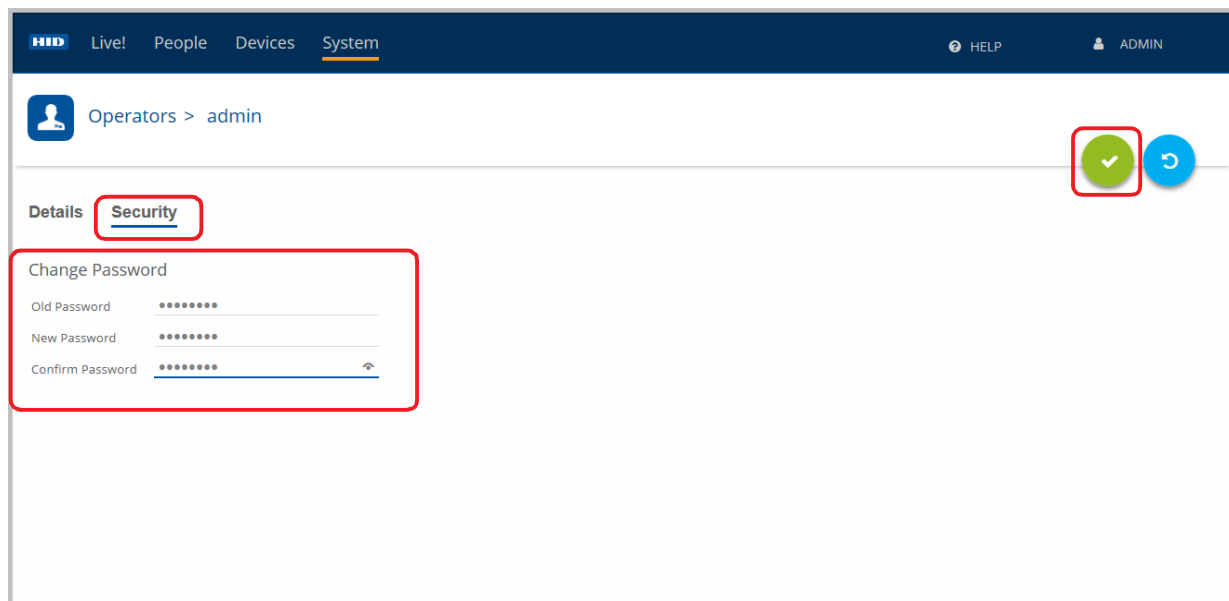


6. Select the **Security** option and under **Change Password**:

- 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.

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

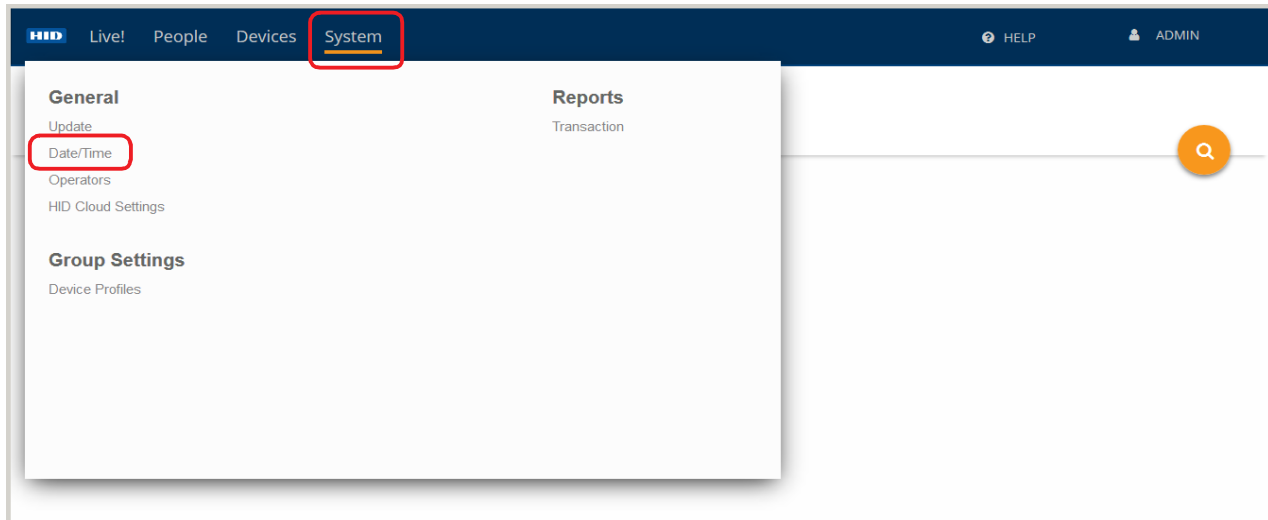


8. Exit HID Biometric Manager and login again using the default username (**admin**) and new password.

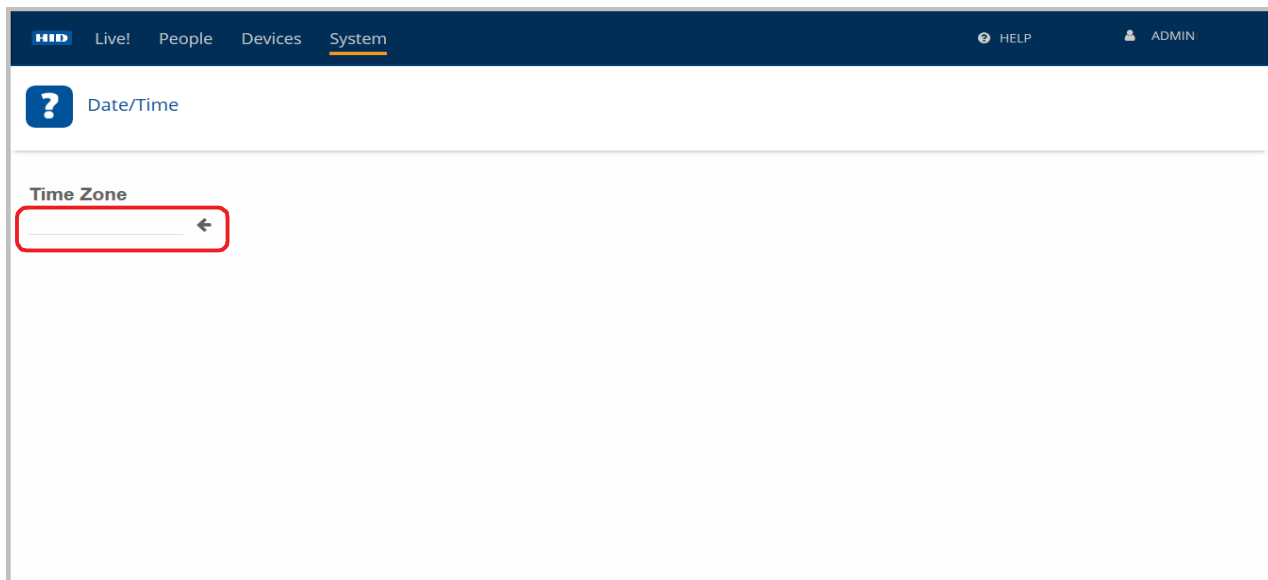
3.2.3 Configure time zone setting

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.

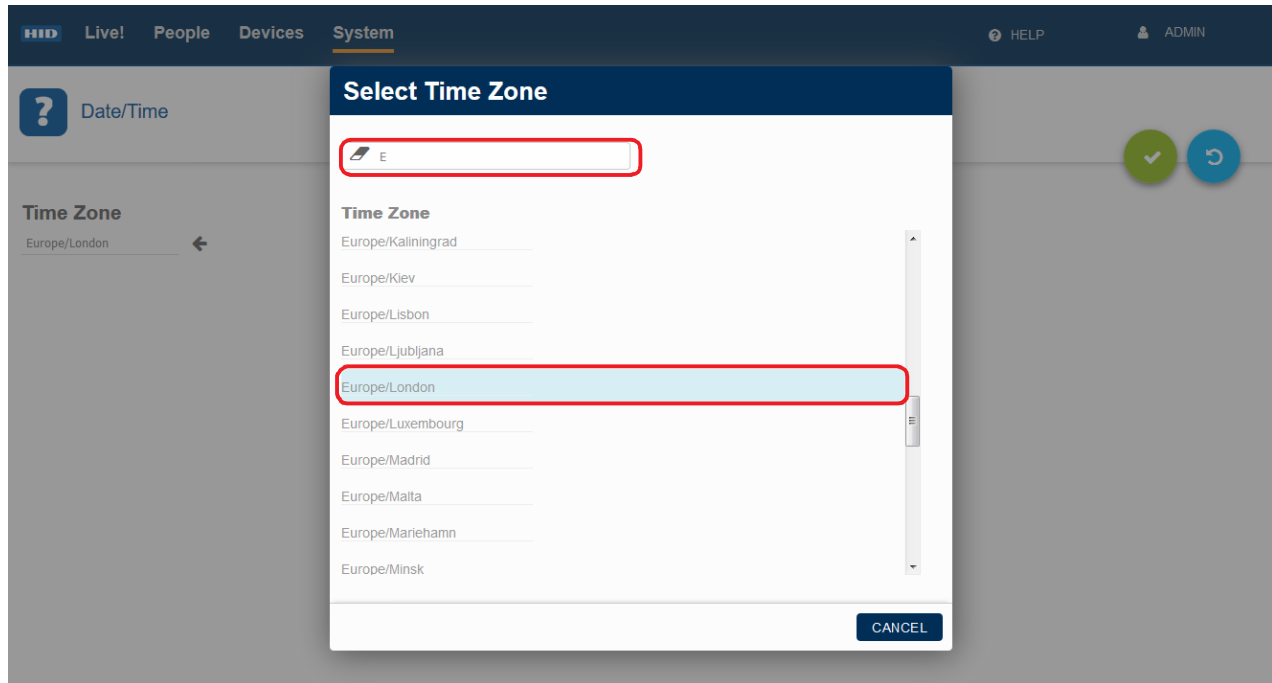


3. Select the **Time Zone** arrow icon to access a list of selectable time zones.

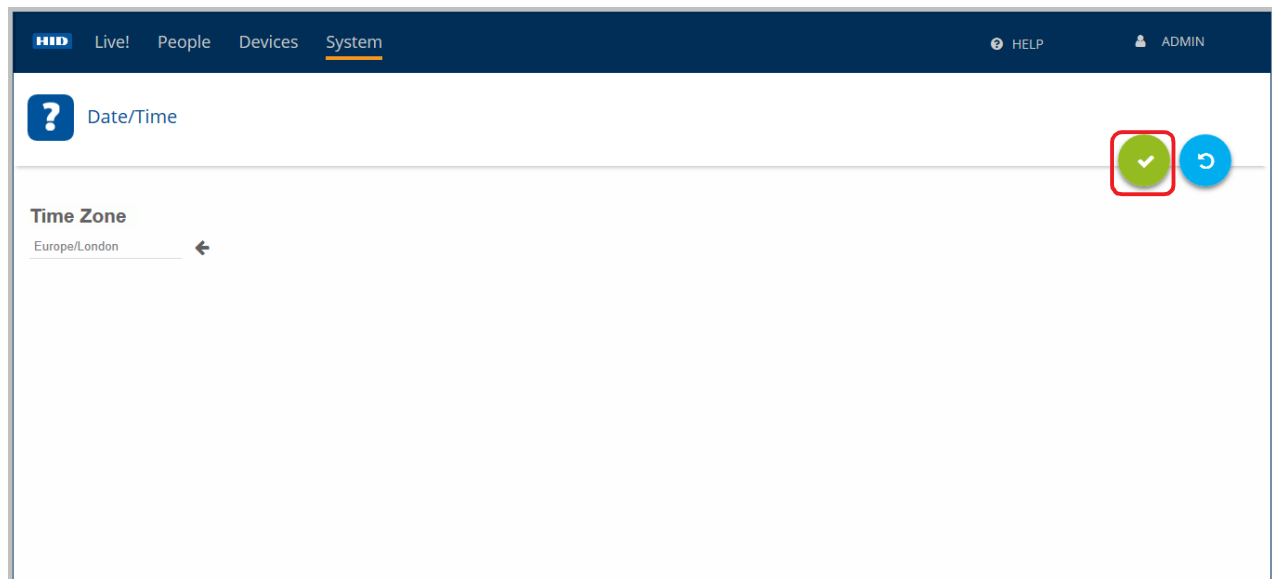


- Select the desired Time Zone from the displayed list.

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



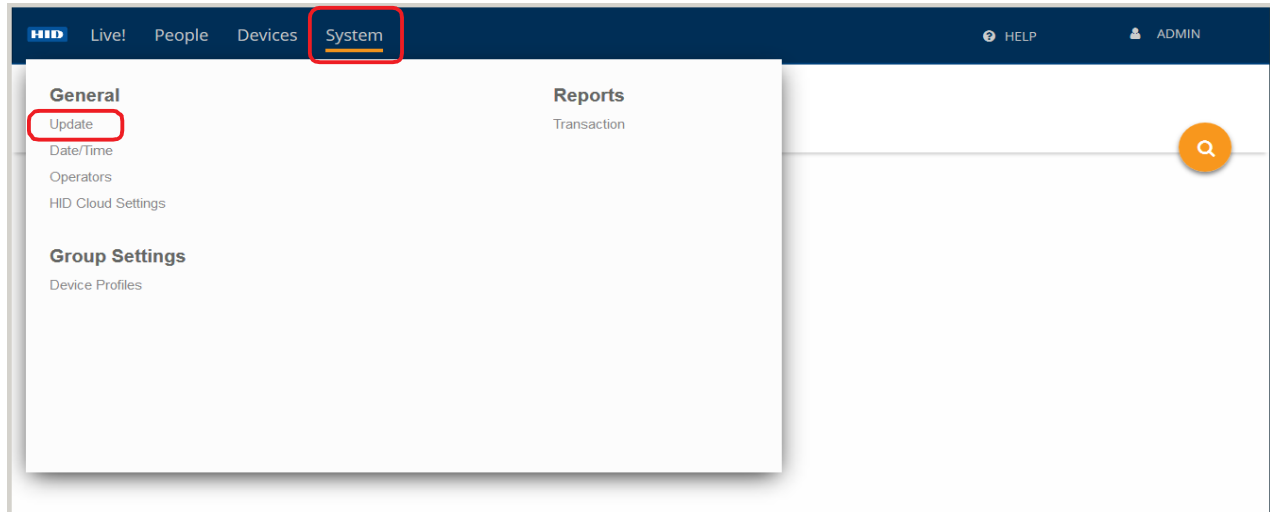
- On the **Date/Time** screen click the **Save** icon to save your time zone setting.



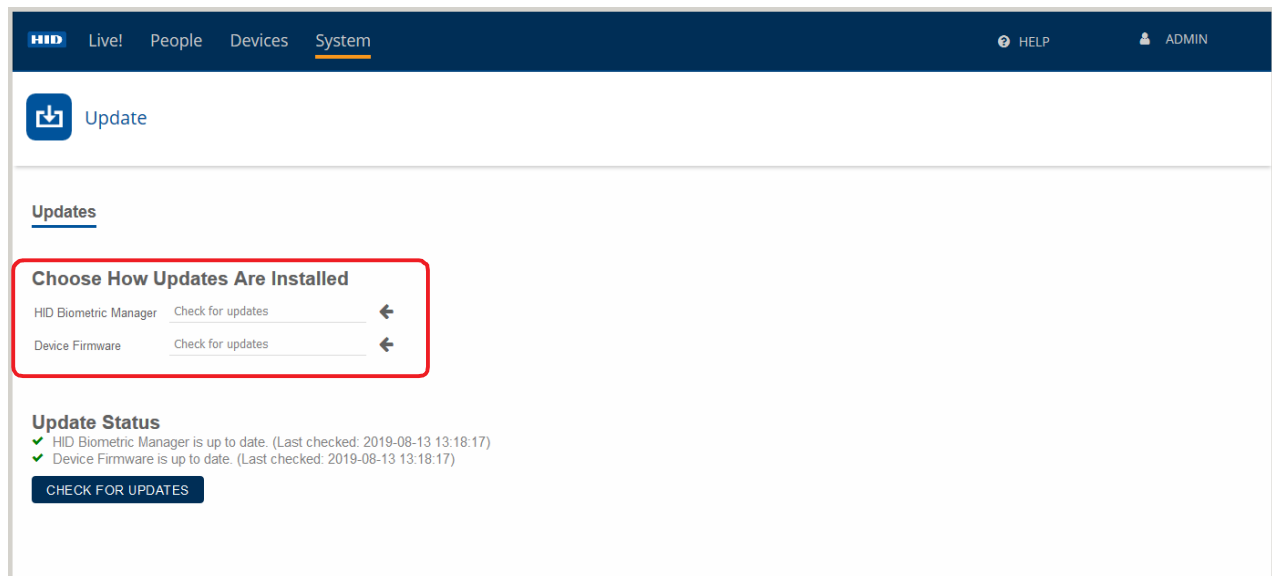
3.2.4 Configure software/firmware update settings

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

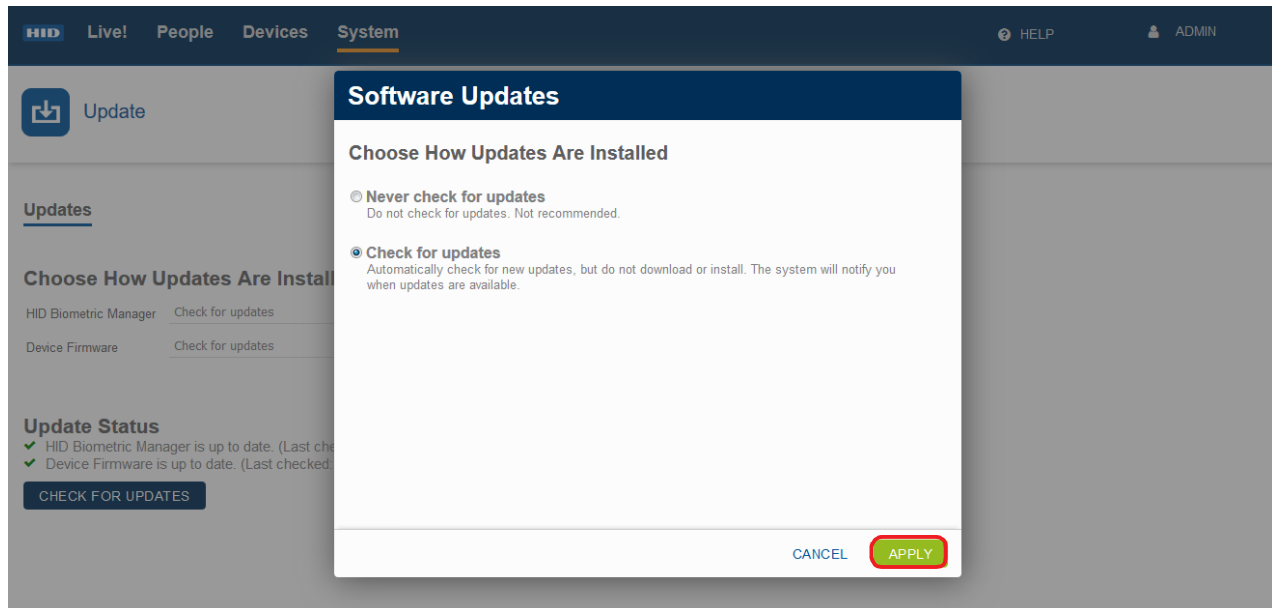
1. Click on the **System** option.
2. Select the **Update** option to access software and firmware update settings.



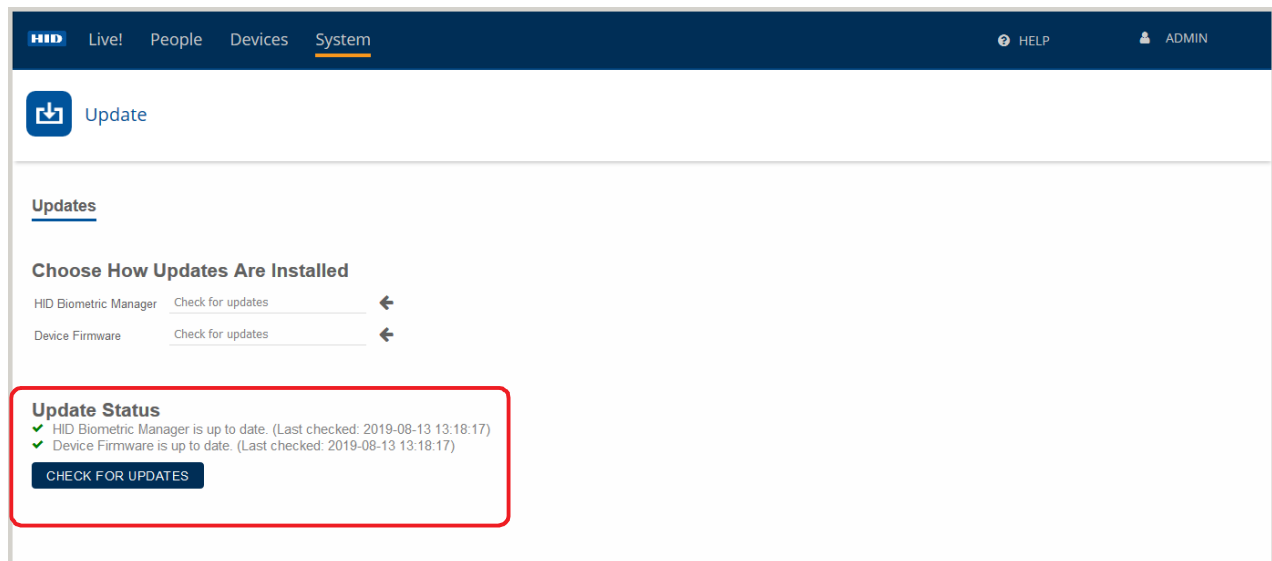
3. Select the arrow icon associated with:
 - **HID Biometric Manager:** To access options to configure how Biometric Manager software updates are installed.
 - **Device Firmware:** To access options to configure how device firmware updates are installed.



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



5. Click **CHECK FOR UPDATES** to check if software/firmware updates are available. **Update Status** information is displayed on the screen.
 - If new HID Biometric Manager 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. You will be prompted to log back into the HID Biometric Manager.
 - If new device firmware is available, see *Section 3.4.2 Device firmware update*.



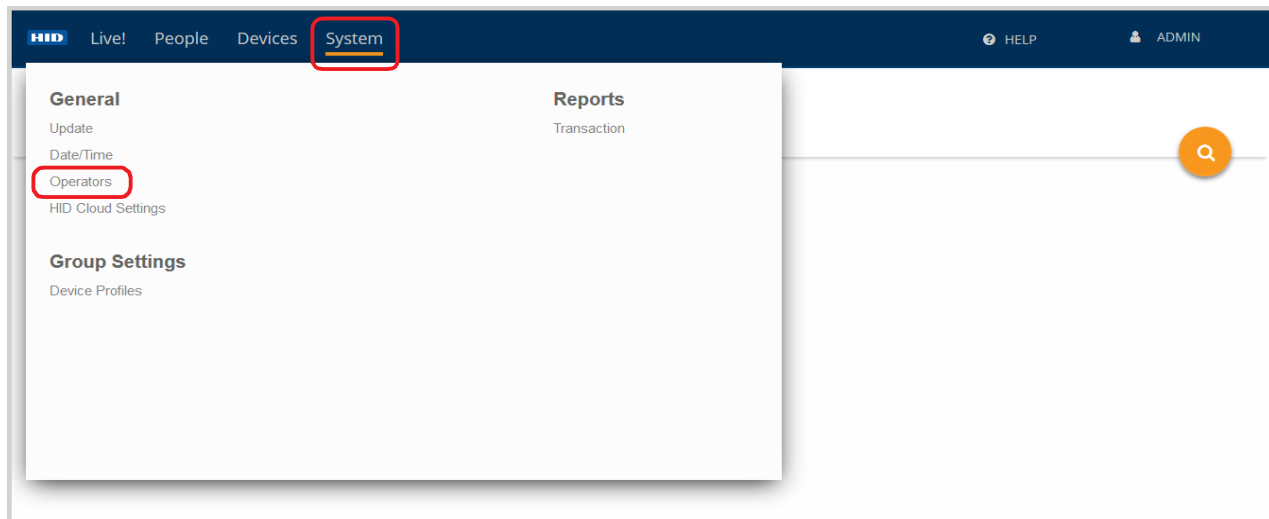
3.2.5 Create Biometric Manager operators

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

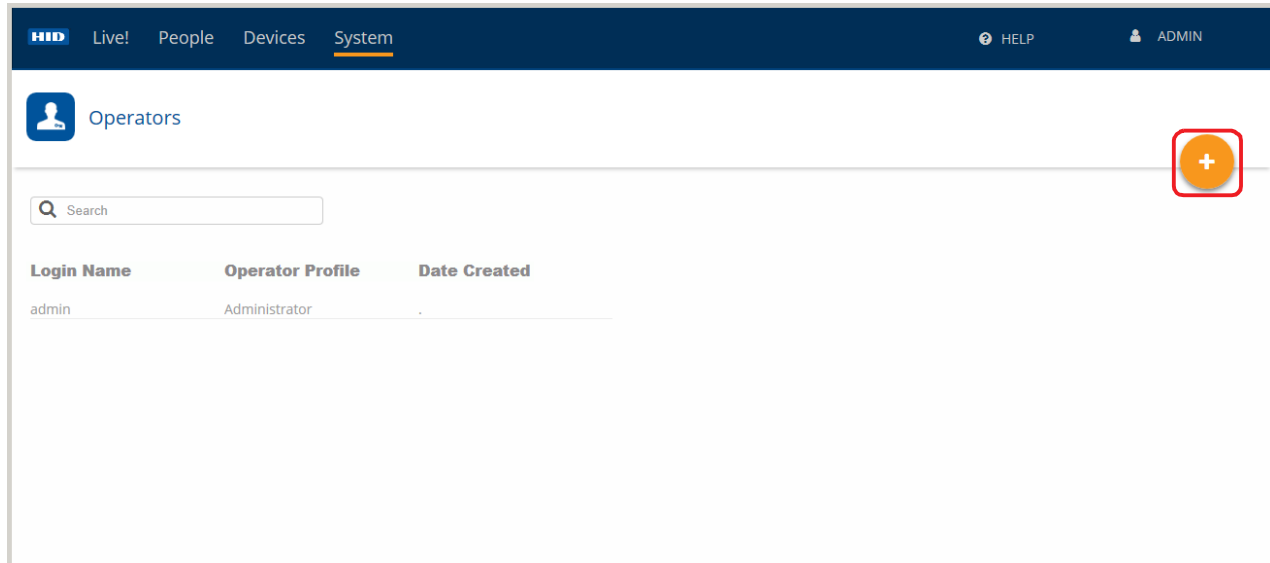
- **Administrator:** This operator role has full access to Biometric Manager web application with functions to install and manage RB25F devices, enroll people in the system, add credentials, and collect and store associated biometric data.
- **Device Administrator:** This operator role is intended for HID partner technicians involved in the setup and maintenance of the Biometric Management environment as well as configuration and update of the RB25F. This operator role has limited access to user information.
- **Enrollment:** 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:

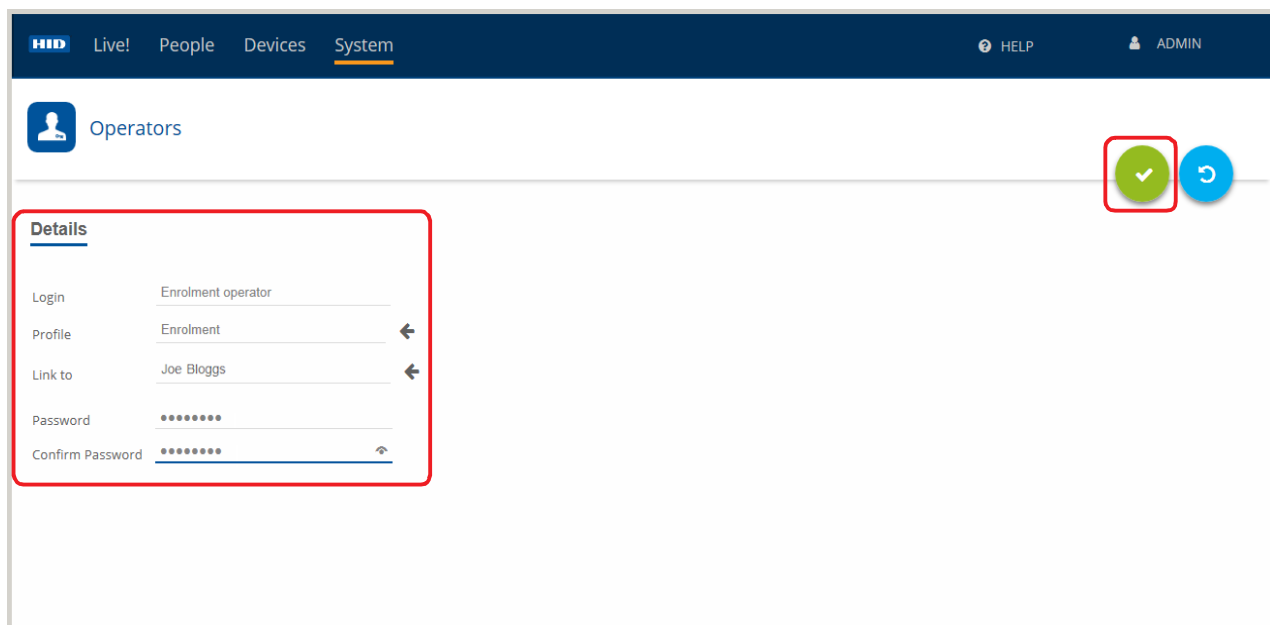
1. Click on the **System** option.
2. Select the **Operators** option to access software and firmware update settings.



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



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




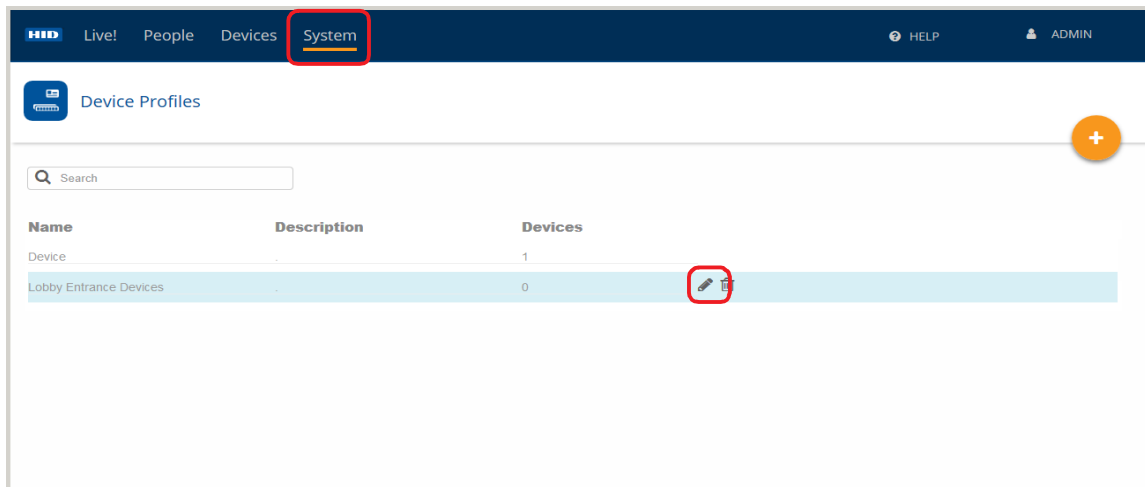
3.3 Device profiles

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

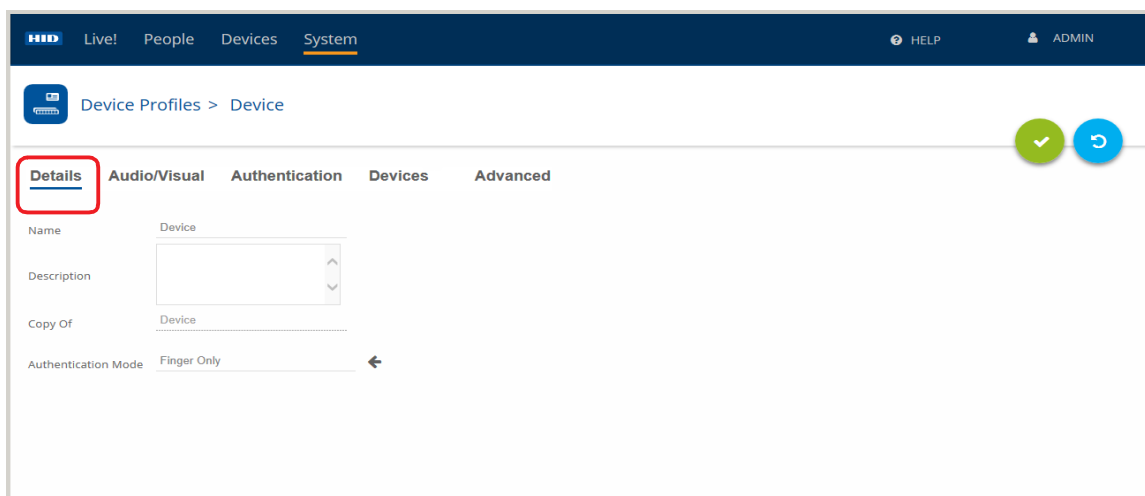
To edit the attributes of device profile:

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.



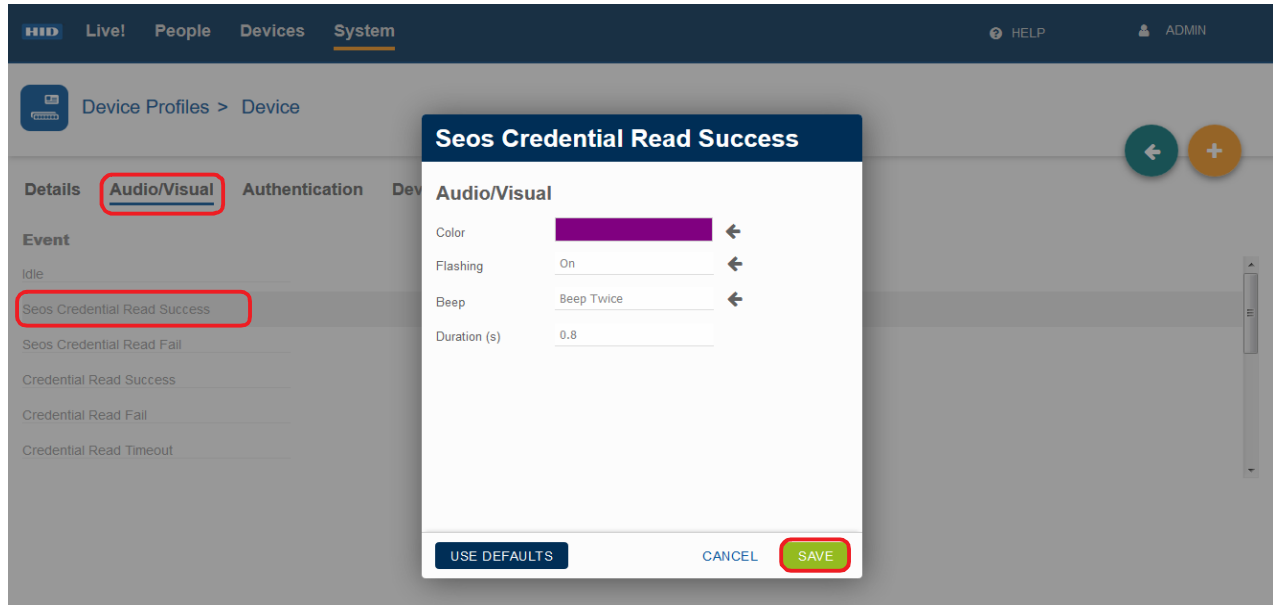
3. On the **Device** screen, if not already displayed, select **Details**. On the **Details** screen you can edit the device profile **Name** and **Description** and select the **Authentication Mode** (for a definition of the **Authentication Modes**, see *Appendix C - Acronyms and terminology*).

Note: The authentication mode set here is the default when no authentication mode schedule has been configured.



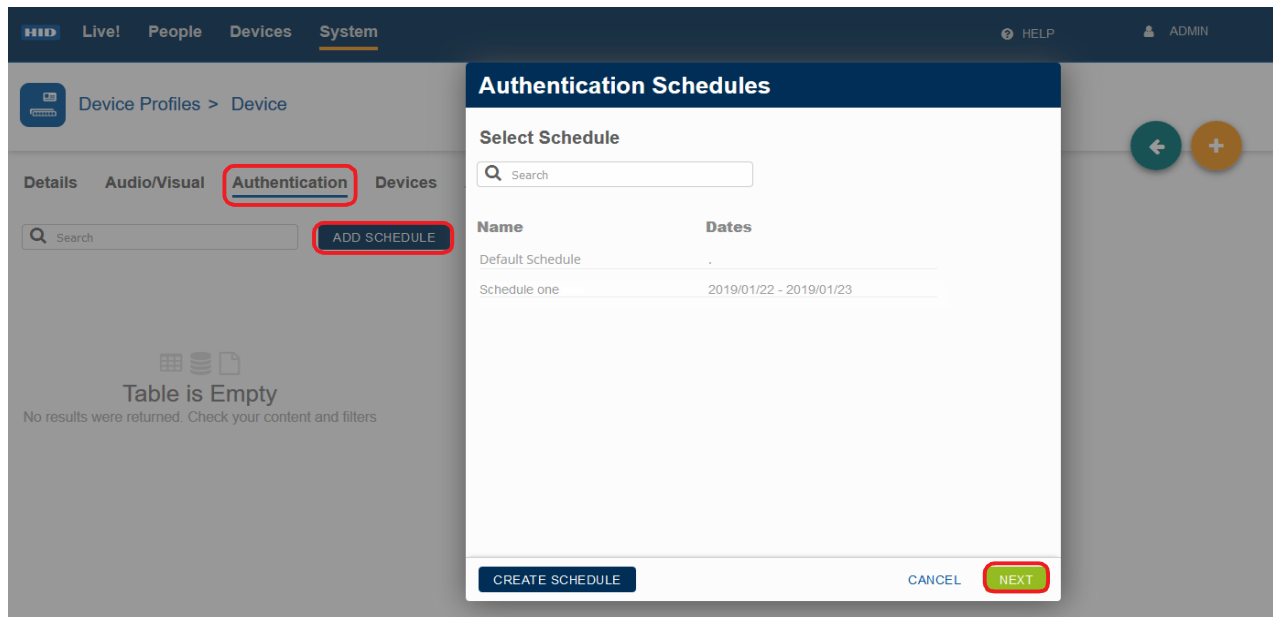
4. On the **Device** screen, select **Audio/Visual**.
5. Click on an **Event** type from the displayed list to edit the attributes for the selected event.
6. Click **SAVE** to save the selected settings.


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

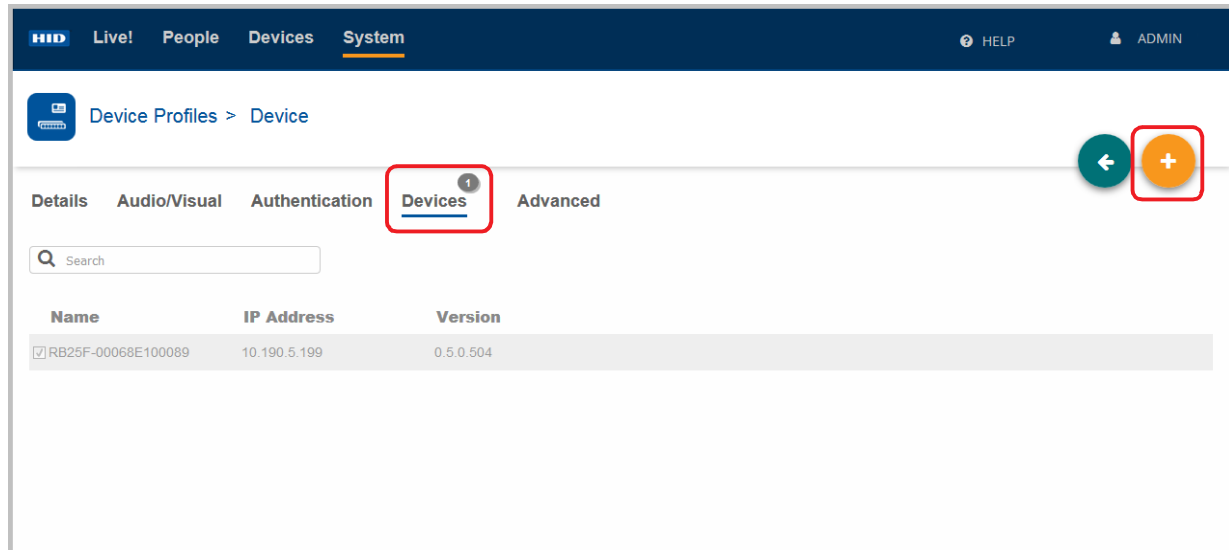


7. On the **Device** screen, select **Authentication**.
8. Click **ADD SCHEDULE** to schedule when a device will operate in a specified Authentication Mode. Select a schedule from the list and click **Next**.

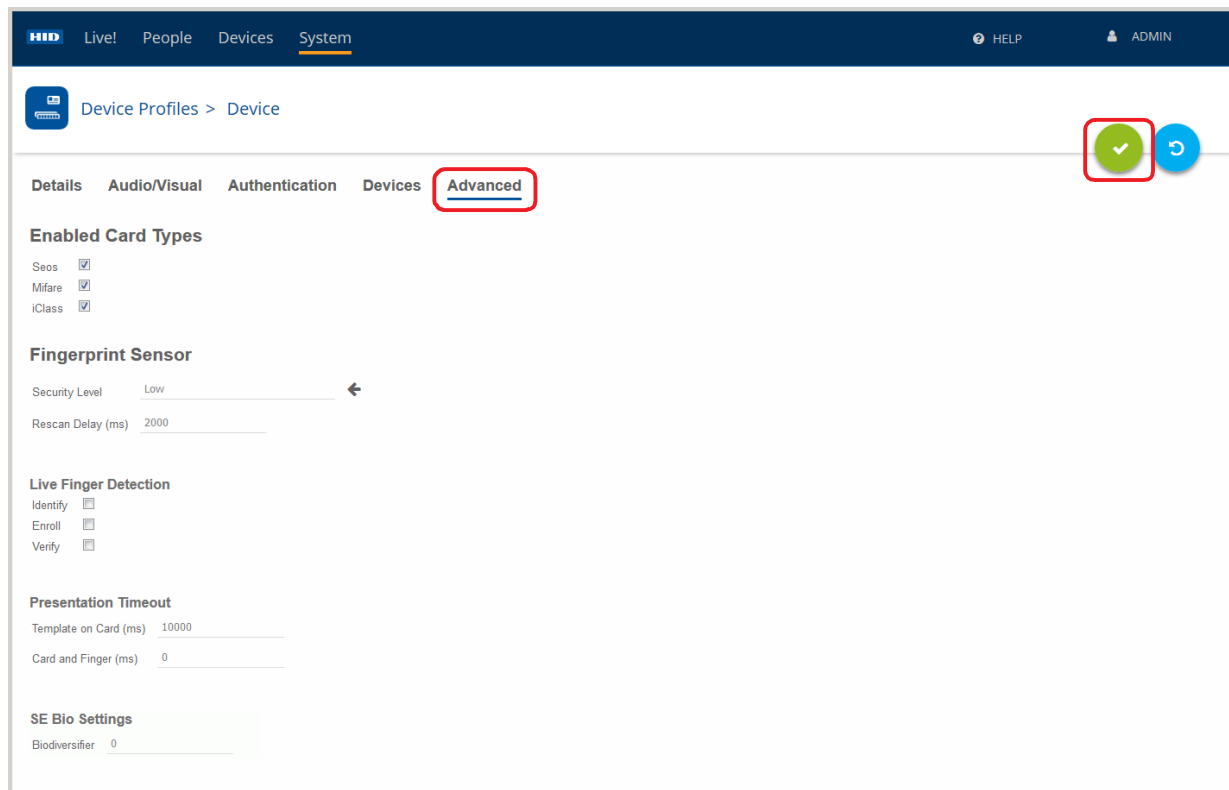
Note: Click **CREATE SCHEDULE** to create a new authentication schedule.



9. 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.
10. Click the **Add** icon [] to add a device to this device profile.



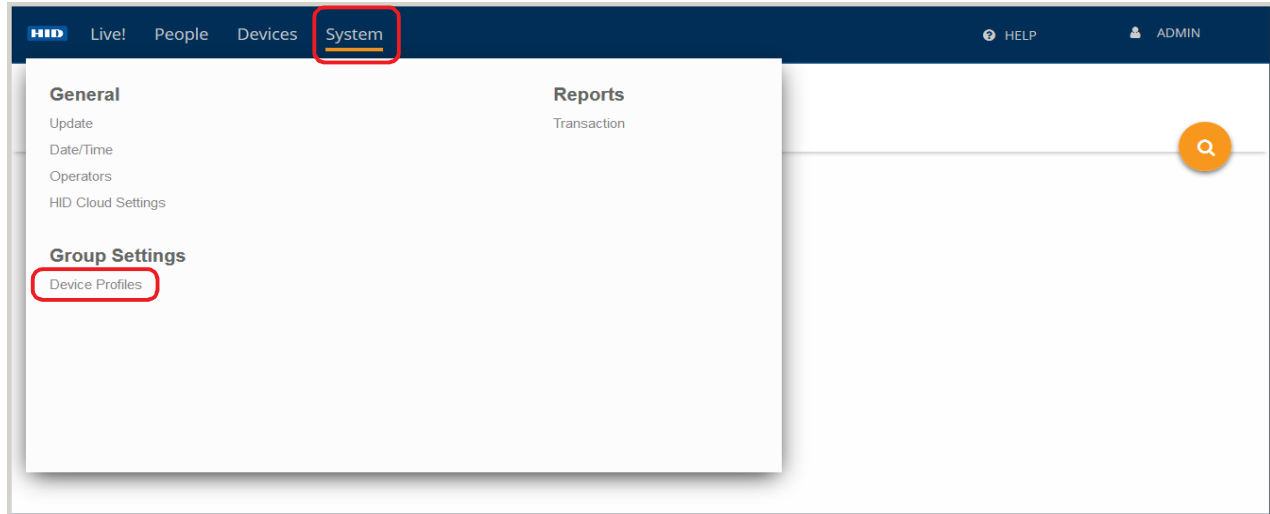
11. On the **Device** screen, select **Advanced**.
12. Select the card types which the device should support and the fingerprint sensor settings.
13. Click **SAVE** to save the selected settings.



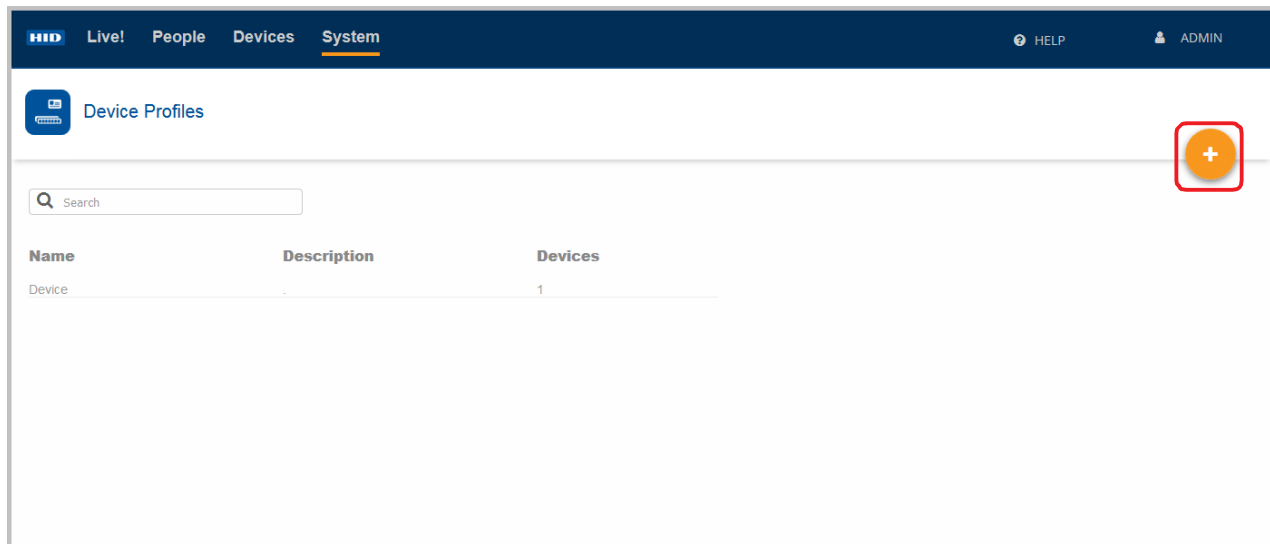
3.3.2 Create a device profile

To create a new device profile:

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

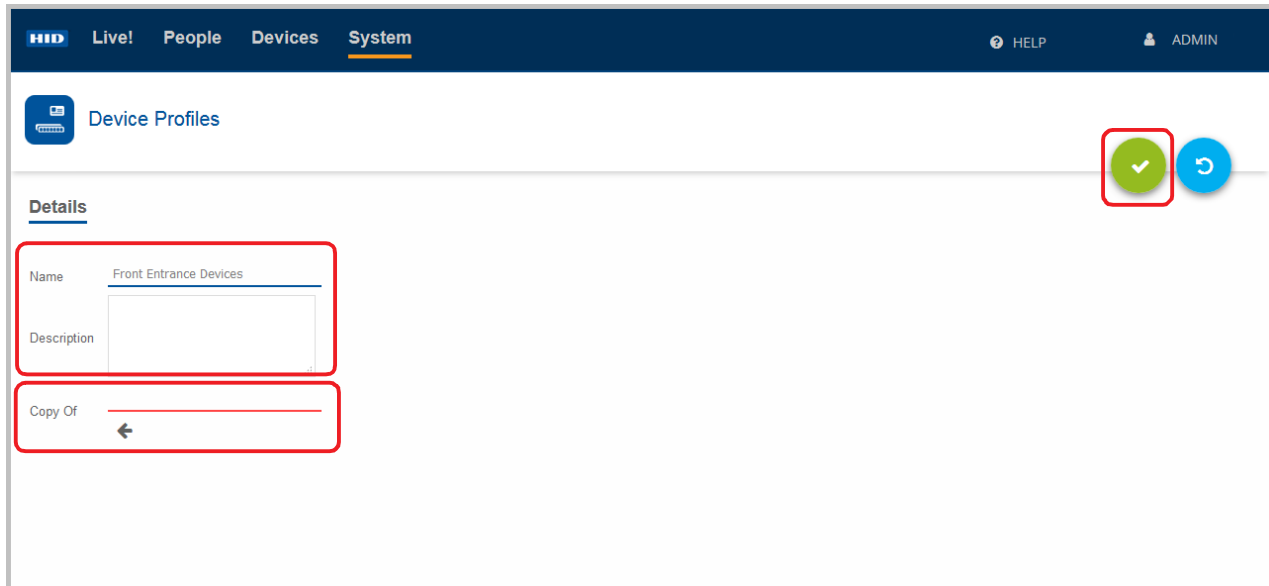


2. Click the **Add** icon [+].

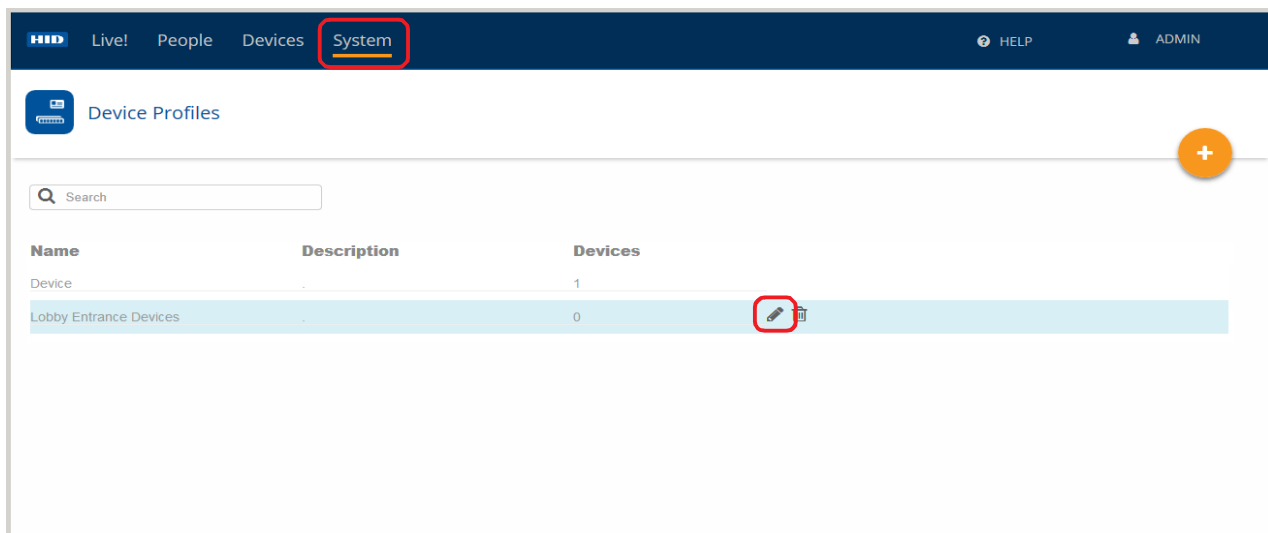



- Enter a **Name** and optional **Description** for the new device profile, then click the **Save** icon [✓].

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*.




- 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.
- Click on the **Edit** icon [✎] associated with the device profile to access the profile attributes. See *Section 3.3.1 Edit a device profile*.

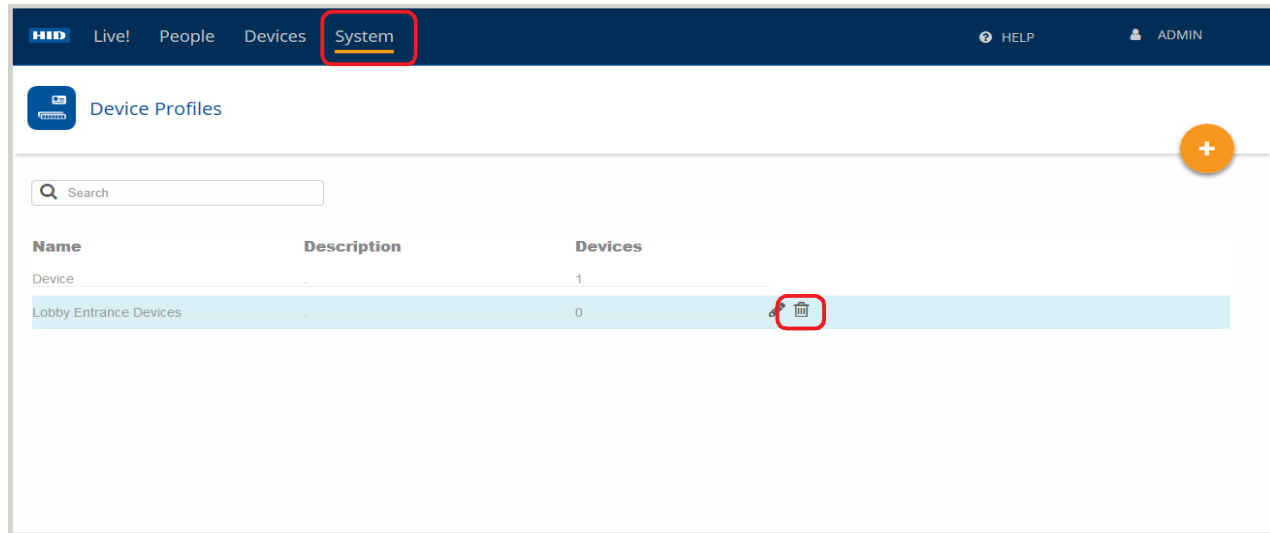


Name	Description	Devices	
Device		1	
Lobby Entrance Devices		0	

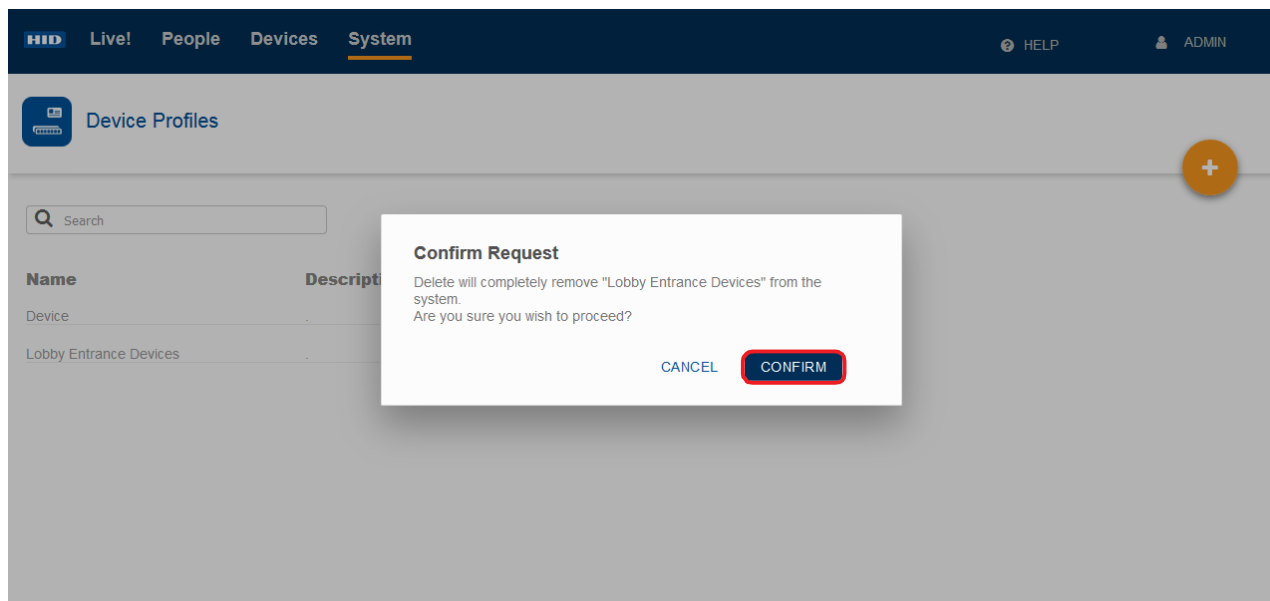
3.3.3 Delete a device profile

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.

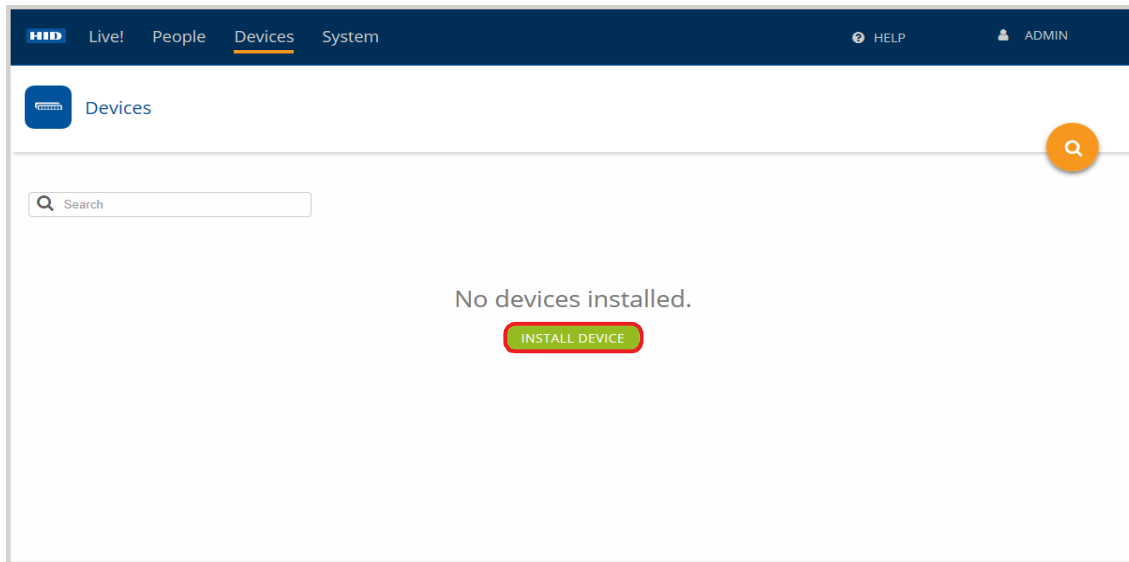


3.4 Device installation and configuration

Device installation and configuration with HID Biometric Manager can only be carried out by the **Administrator** or **Device Administrator** 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*.

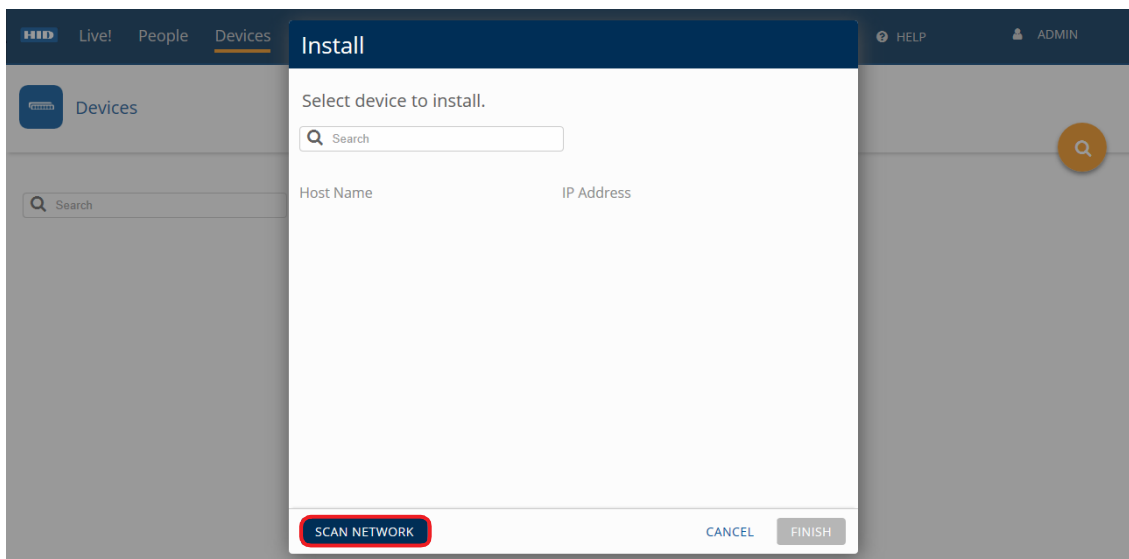
1. Launch HID Biometric Manager and login as an **Administrator** or **Device Administrator** operator.
2. To initially install a device, on the **Devices** screen, click **INSTALL DEVICE**.

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

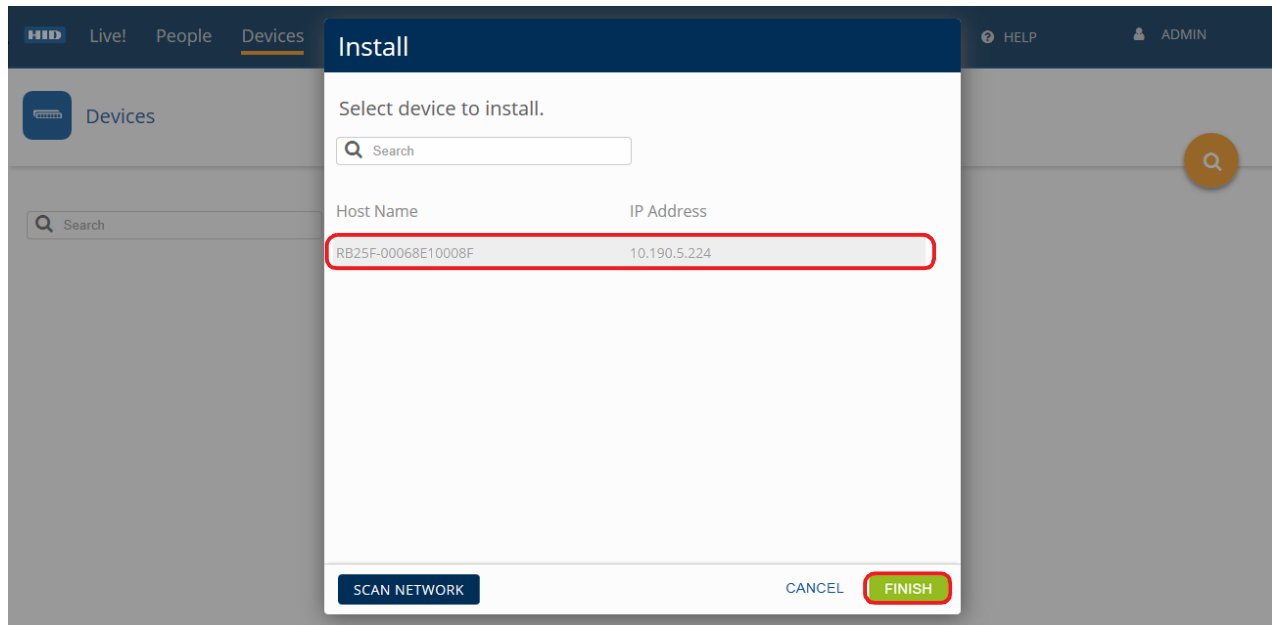


3. In the **Install** dialog, click **SCAN NETWORK** to ensure the complete list of available devices are shown.

Note: If no devices are found check the ports listed in *Section 3.1.2 TCP Port usage* are open. The **Search** function can be used to search the list of displayed devices.

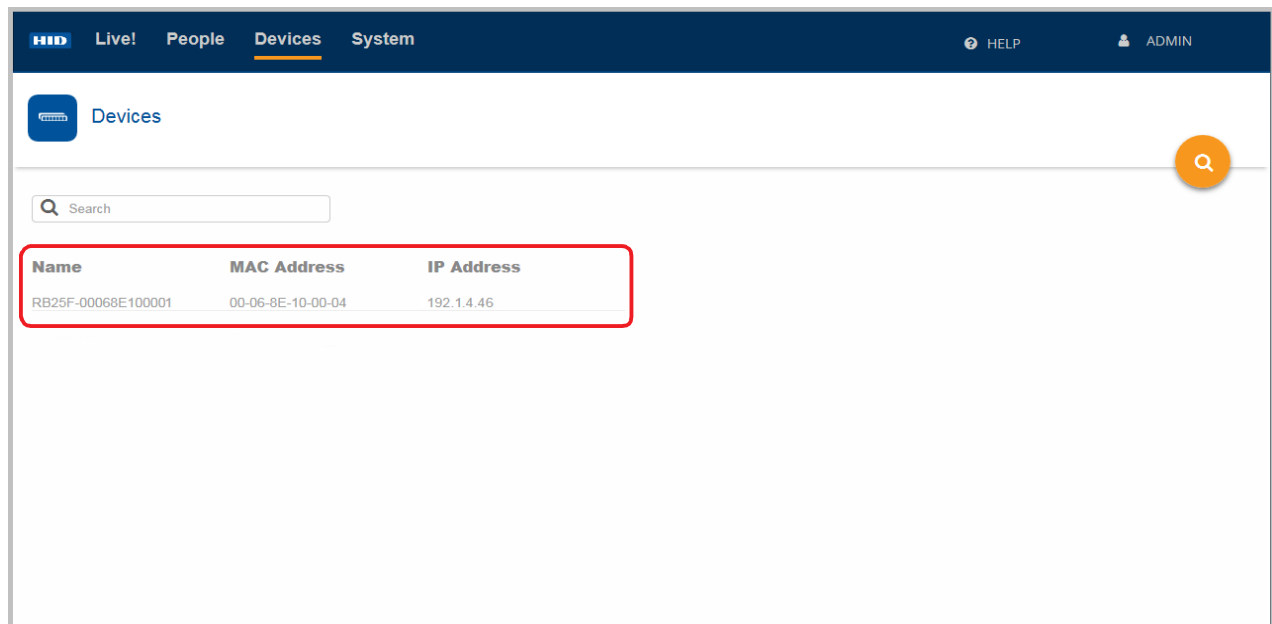


4. Select a device from the displayed list and click **FINISH**.



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.

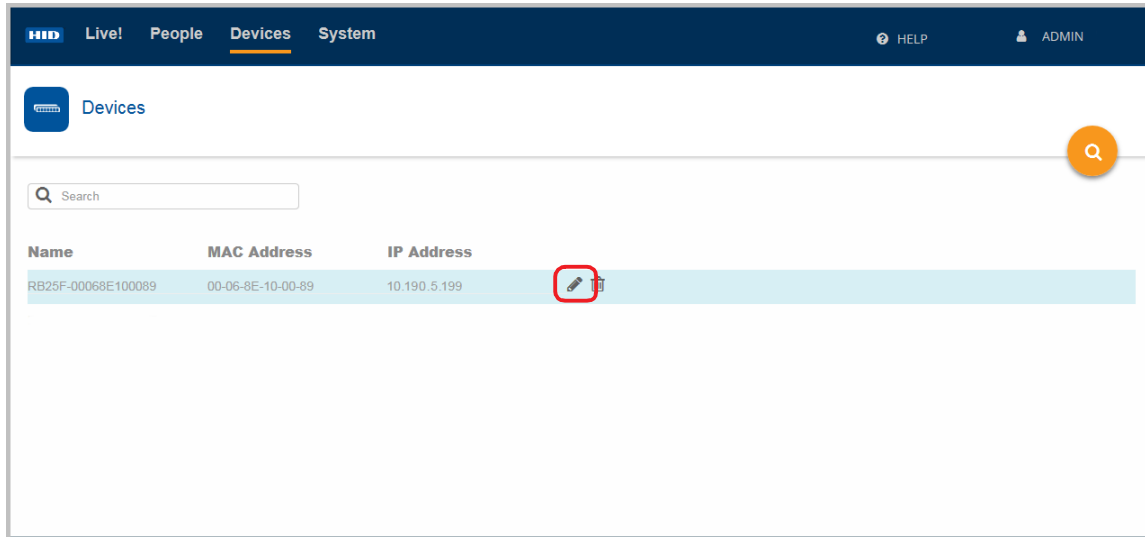


Note: To uninstall a device, see *Section 3.4.4 Uninstall a device*.

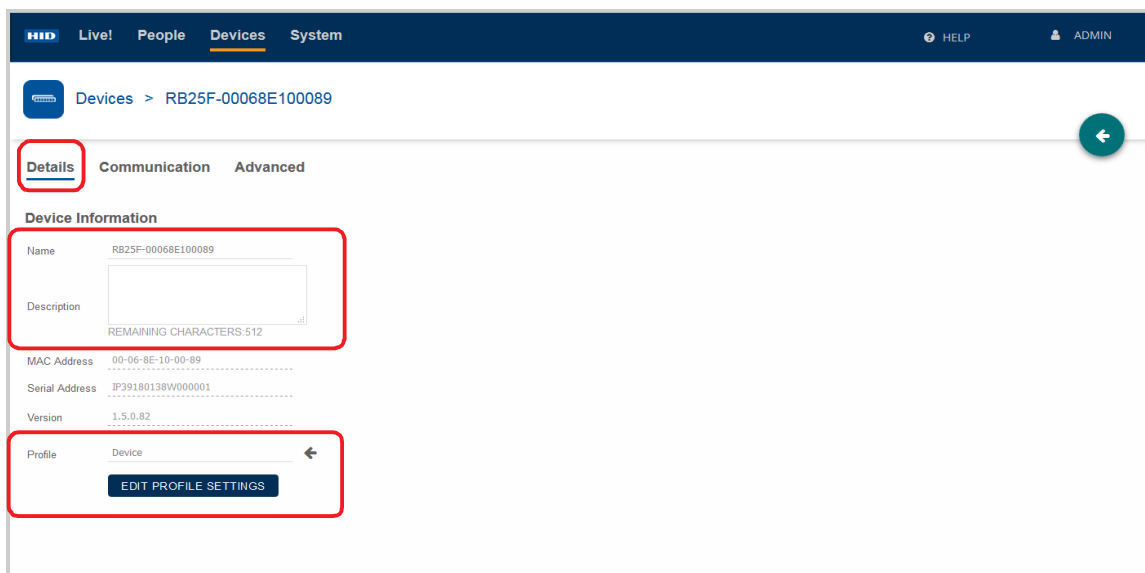
3.4.1 Configure device settings


To access and configure settings associated with an installed device:

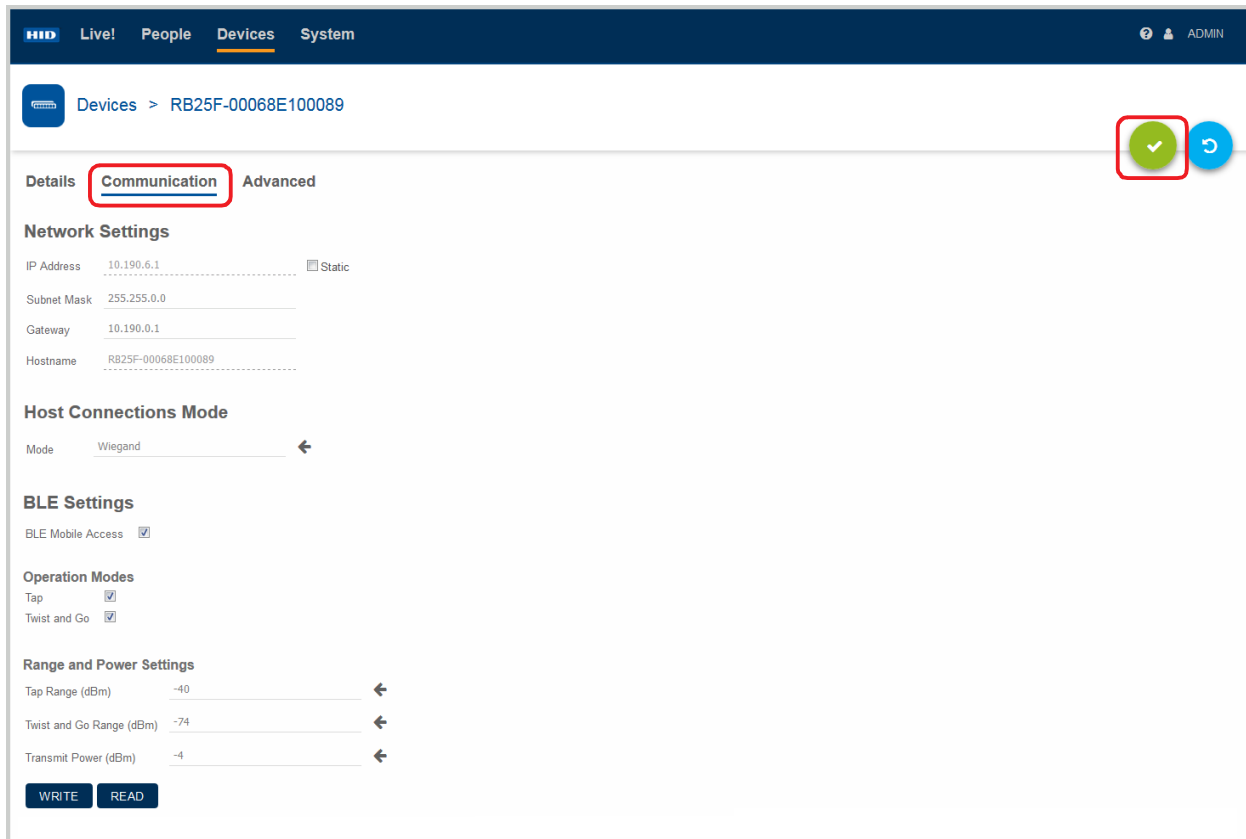
1. On the **Devices** screen, highlight a device entry from the displayed list. The **Edit/Delete** icons appear on the screen for the highlighted device.
2. Click on the **Edit** icon [] associated with the device to access the device settings screen.



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 **EDIT PROFILE SETTINGS** to configure the settings for the displayed device profile, see *Section 3.3.1 Edit a device profile*.



5. On the **Devices** screen, select **Communication**.
6. On the Communication screen you can configure:
 - **Network Settings:** To use a static IP address select the **Static** option. Enter a static IP address (IPv4) and also the Subnet Mask and Gateway.
 - **Host Connections Mode:** Set as **Wiegand** (default).
Note: OSDP is currently not supported.
 - **BLE Settings:** Enable/disable **BLE Mobile Access**.
 - **Operation Modes:** Select the desired operation mode to enable/disable the **Tap** or **Twist and Go** gesture operation.
 - **Range and Power Settings:** Set the read range for **Tap** and **Twist and Go** and the setting for **Transmit Power**.
Note: The default range settings for **Tap**, **Twist and Go** and **Transmit Power** are displayed in HID Biometric Manager. It is recommended that the default **Transmit Power** setting (-4 dBm) is not exceeded unless absolutely necessary as range and transmit power settings work in tandem to increase/decrease effective read range.
7. When the communication settings have been selected click the **Save** icon [].

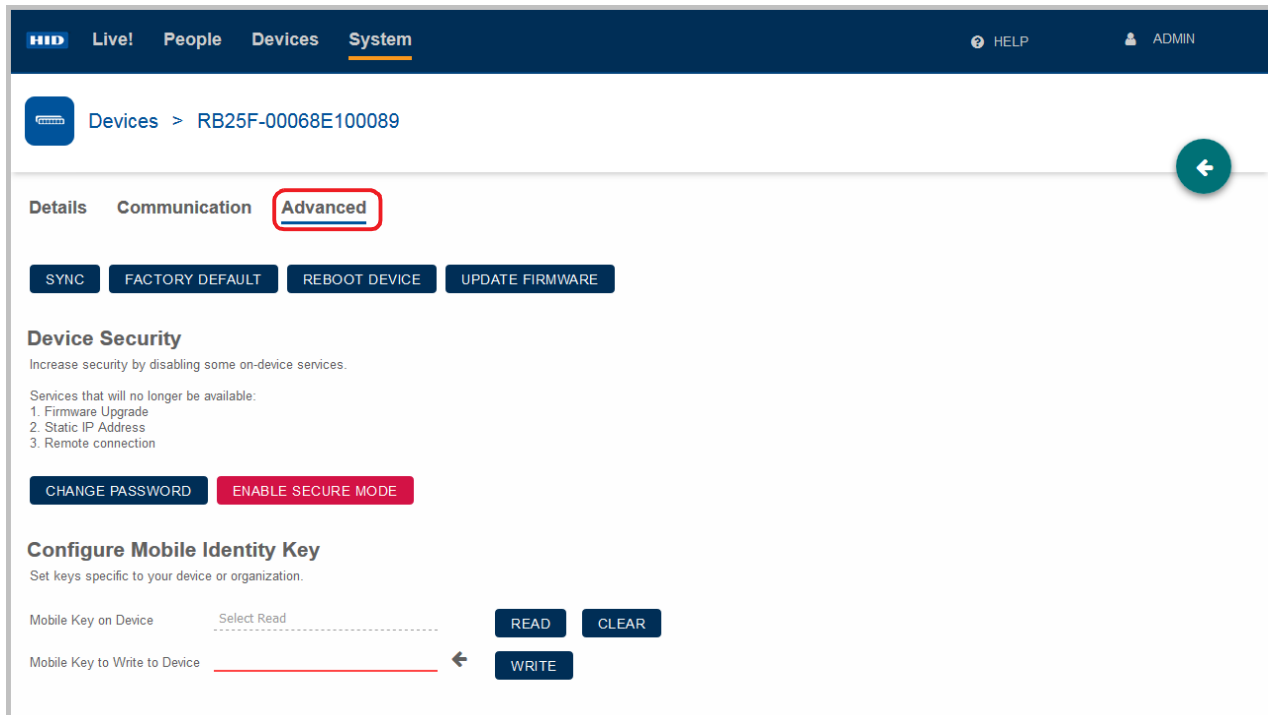


The screenshot shows the HID Biometric Manager web interface. The top navigation bar includes 'Live!', 'People', 'Devices' (selected), and 'System'. The user is logged in as 'ADMIN'. The breadcrumb trail shows 'Devices > RB25F-00068E100089'. The 'Communication' tab is selected and highlighted with a red box. The settings are as follows:

- Network Settings:** IP Address: 10.190.6.1, Subnet Mask: 255.255.0.0, Gateway: 10.190.0.1, Hostname: RB25F-00068E100089. The 'Static' checkbox is checked.
- Host Connections Mode:** Mode: Wiegand.
- BLE Settings:** BLE Mobile Access: ☒.
- Operation Modes:** Tap: ☒, Twist and Go: ☒.
- Range and Power Settings:** Tap Range (dBm): -40, Twist and Go Range (dBm): -74, Transmit Power (dBm): -4.

At the bottom, there are 'WRITE' and 'READ' buttons. A green checkmark icon in a red box is visible in the top right corner of the settings area, indicating the settings are saved.

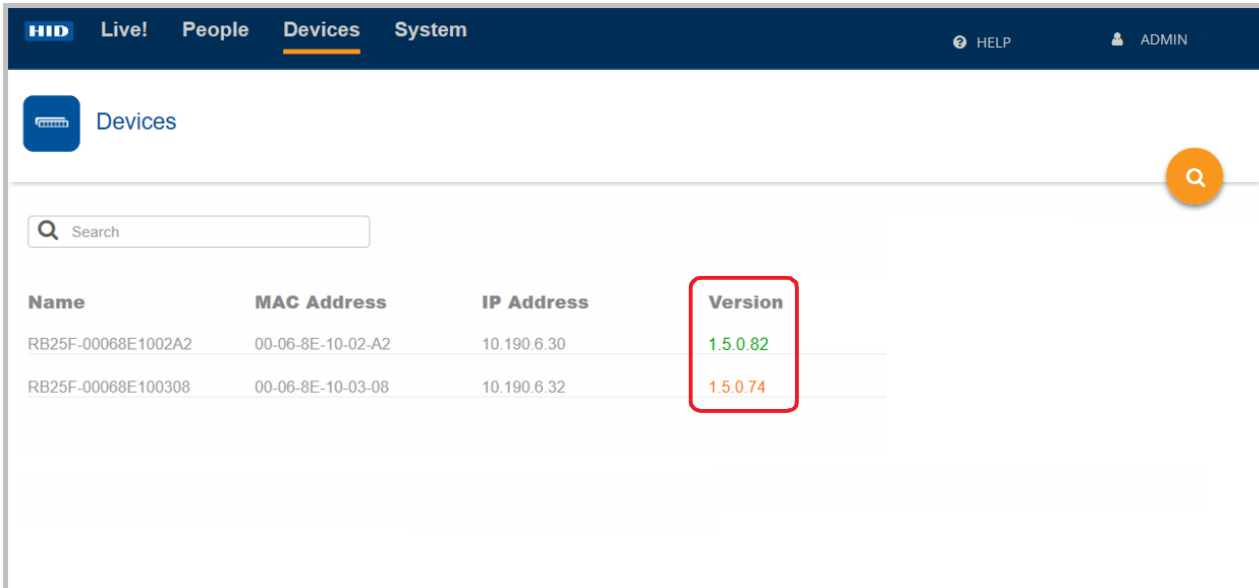
8. On the **Devices** screen select **Advanced**. On the **Advanced** screen you have options to:
- **SYNC:** Syncs all device settings in HID Biometric Manager to the device.
 - **FACTORY DEFAULT:** Restores all device settings to the original factory defaults, see *Section 3.4.3 Reset a device*.
 - **REBOOT DEVICE:** Reboots the device.
 - **UPDATE FIRMWARE:** Updates device firmware.
 - **CHANGE PASSWORD:** Change the device password. The device password provides device security on the LAN if secure mode is not enabled.
 - **ENABLE SECURE MODE/DISABLE SECURE MODE:** Enable/disable the device secure mode.
 - **READ:** Read mobile keys from the device.
 - **CLEAR:** Remove mobile keys read from the device.
 - **WRITE:** Write mobile keys to the device. Before Mobile keys can be written to the device, keys have to be loaded onto HID Biometric Manager, see *Appendix A - Biometric Manager Mobile Access setup*.
9. Click **SYNC** option. For the selected device all settings are copied from HID Biometric Manager to the RB25F.



The screenshot shows the HID Biometric Manager interface. At the top, there's a navigation bar with 'HID', 'Live!', 'People', 'Devices', and 'System' (selected). To the right are 'HELP' and 'ADMIN' links. Below the navigation bar, the breadcrumb 'Devices > RB25F-00068E100089' is shown. The main content area has three tabs: 'Details', 'Communication', and 'Advanced' (selected and highlighted with a red box). Under the 'Advanced' tab, there are four buttons: 'SYNC', 'FACTORY DEFAULT', 'REBOOT DEVICE', and 'UPDATE FIRMWARE'. Below these is the 'Device Security' section, which includes a warning: 'Increase security by disabling some on-device services. Services that will no longer be available: 1. Firmware Upgrade, 2. Static IP Address, 3. Remote connection'. There are two buttons: 'CHANGE PASSWORD' and 'ENABLE SECURE MODE'. The bottom section is 'Configure Mobile Identity Key', which includes the instruction 'Set keys specific to your device or organization.' It has two input fields: 'Mobile Key on Device' with a 'Select Read' dropdown and 'Mobile Key to Write to Device' with a red underline. There are three buttons: 'READ', 'CLEAR', and 'WRITE'.

3.4.2 Device firmware update

An indication that a firmware update is available for a device is provided on the **Devices** screen. If the displayed version number for a device is not green then this indicates that a firmware update is available for that device.



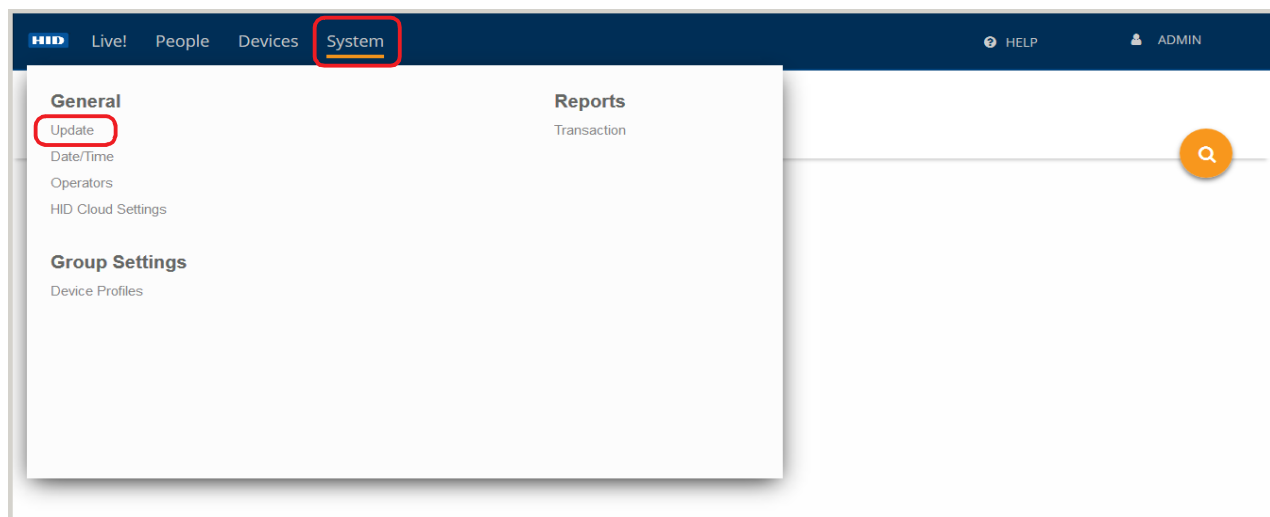
Name	MAC Address	IP Address	Version
RB25F-00068E1002A2	00-06-8E-10-02-A2	10.190.6.30	1.5.0.82
RB25F-00068E100308	00-06-8E-10-03-08	10.190.6.32	1.5.0.74

Device firmware updates can take up to approximately eight minutes per device, including updates of the reader board. Updates may complete faster depending on the HID Mobile Access Portal connection and the number of uninterrupted updates.

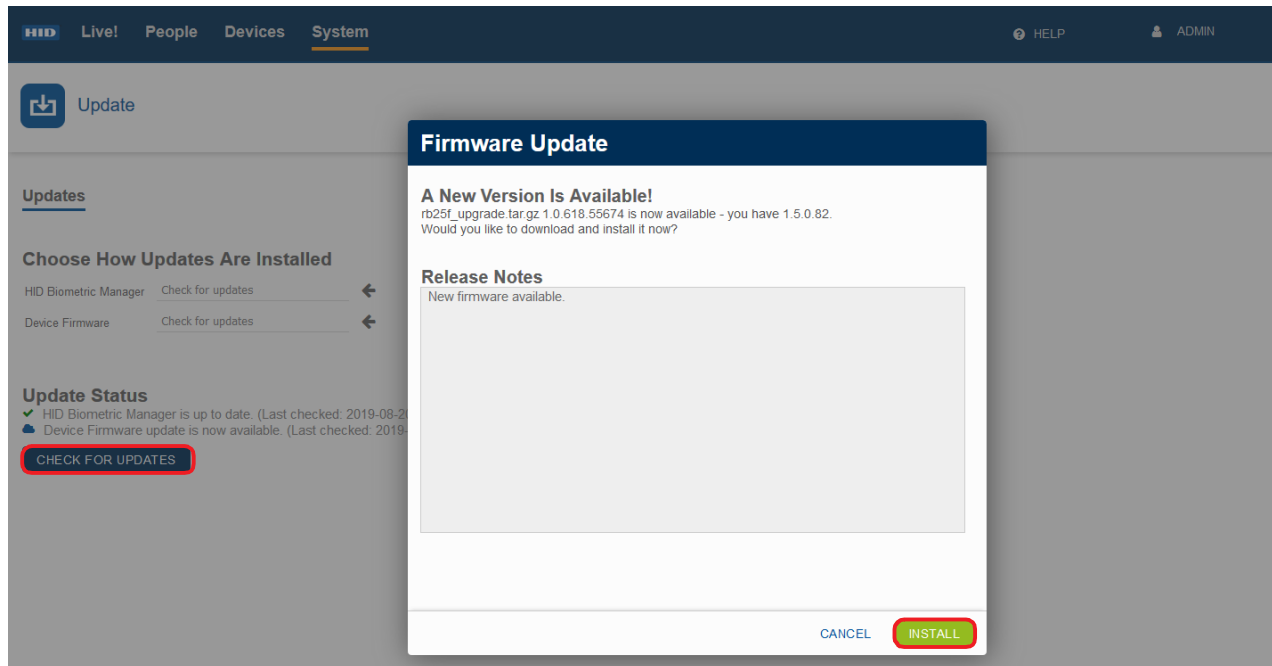
IMPORTANT: It is recommended that device firmware updates should be carefully scheduled as all devices are updated and will be unavailable for use during the firmware update period.

To update device firmware:

1. Select the **System** option and click **Update**.

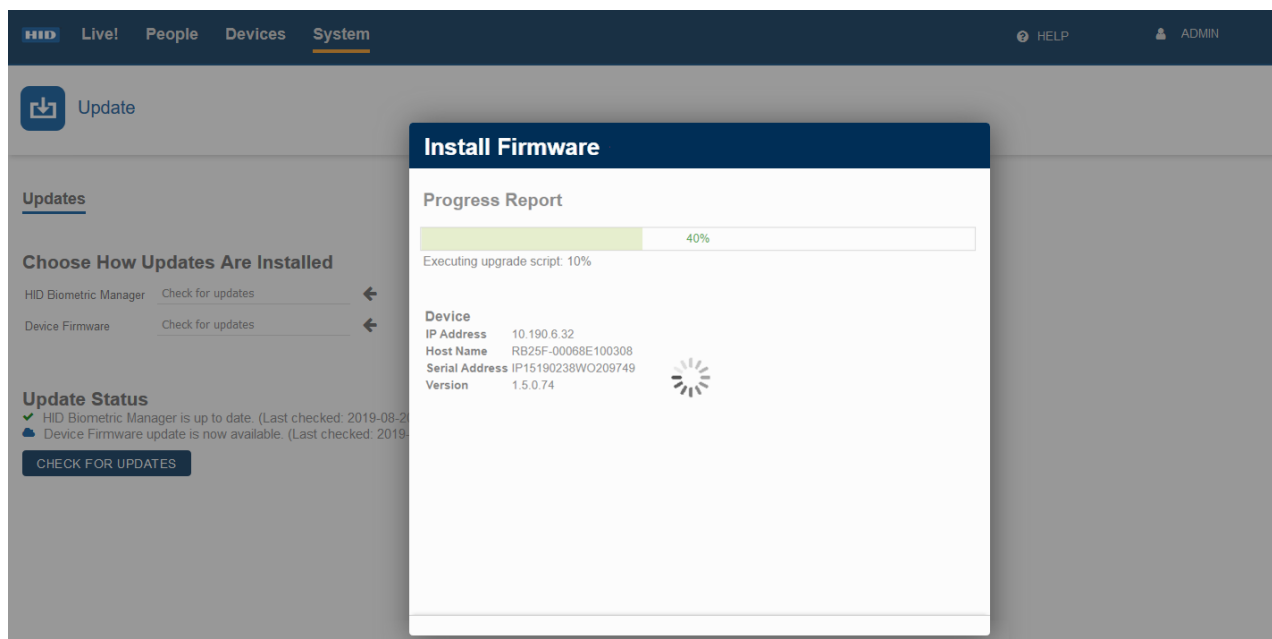


- Click **CHECK FOR UPDATES**. Review the displayed firmware update information and click **Install** to trigger the firmware update process.



An indication of the firmware update progress is displayed.

Note: The **Progress Report** bar indicates firmware update progress against total devices. For example, if two devices are being updated then 50% progress indicates one device updated out of two devices. Devices are updated in series with information displayed on the current device being updated.

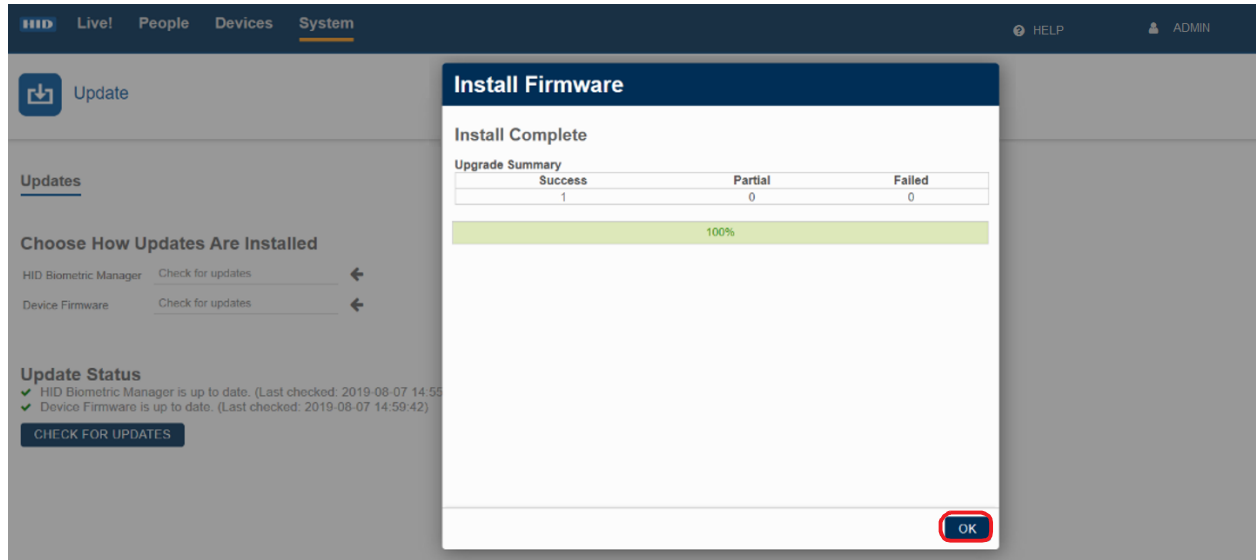


- When the firmware update is indicated as complete, click **OK**.

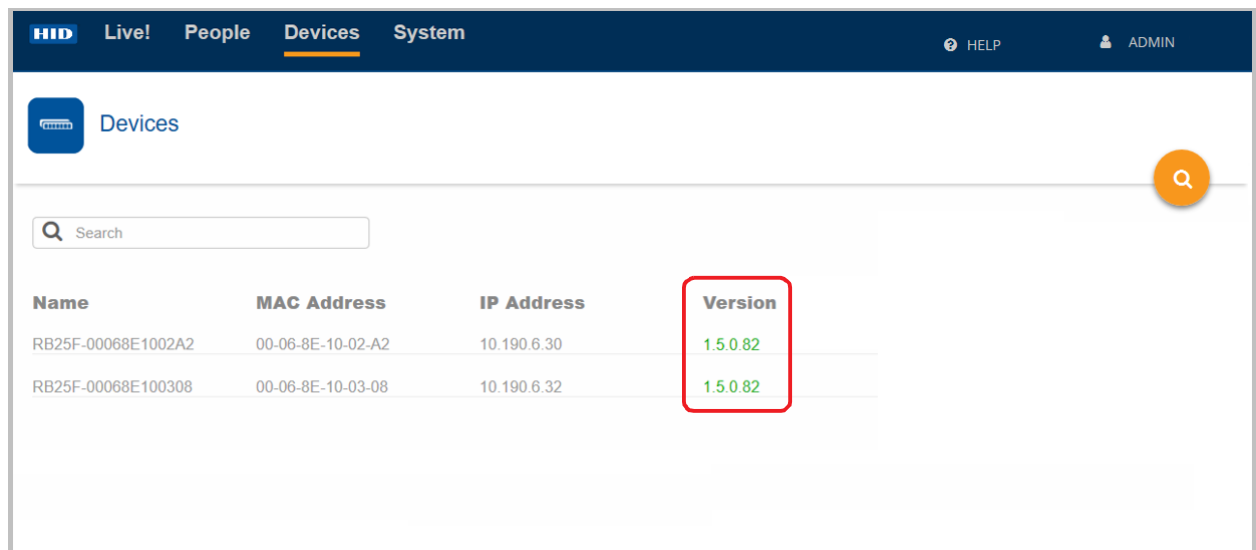
Note: Any partial or failed firmware updates are indicated in the **Upgrade Summary** table.

A partial update means that the system was not able to complete the secondary step of applying advanced updates, for example, as a result of the connection to the HID Mobile Access Portal not being setup (see *Appendix A - Biometric Manager Mobile Access setup*) or being interrupted.

A partially updated device will run the installed level of firmware however features, such as mobile access, and firmware fixes will not be available.




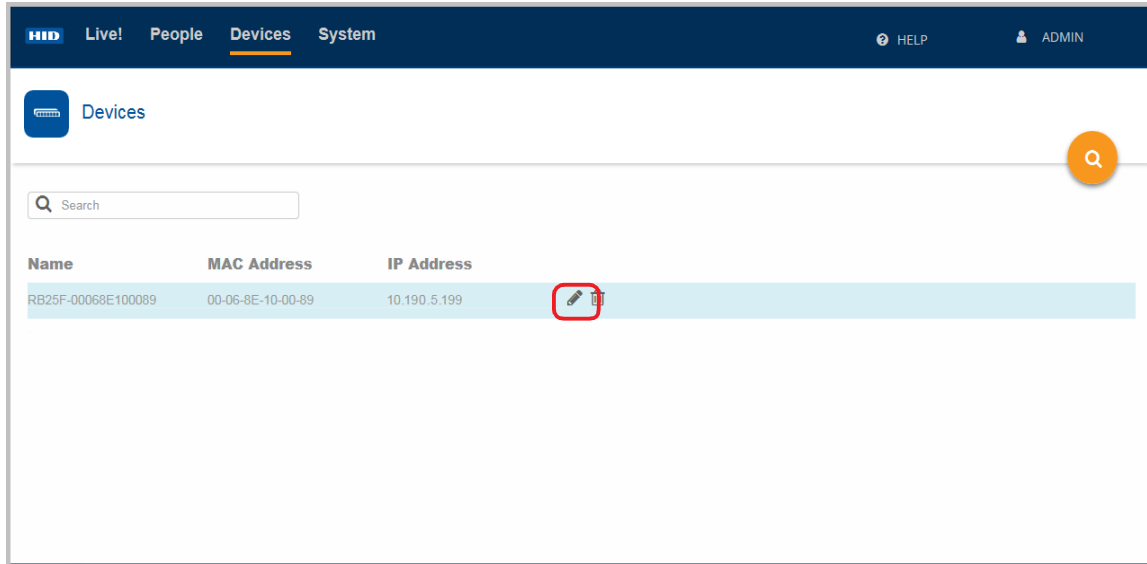
- Check the **Devices** screen to verify device firmware versions.



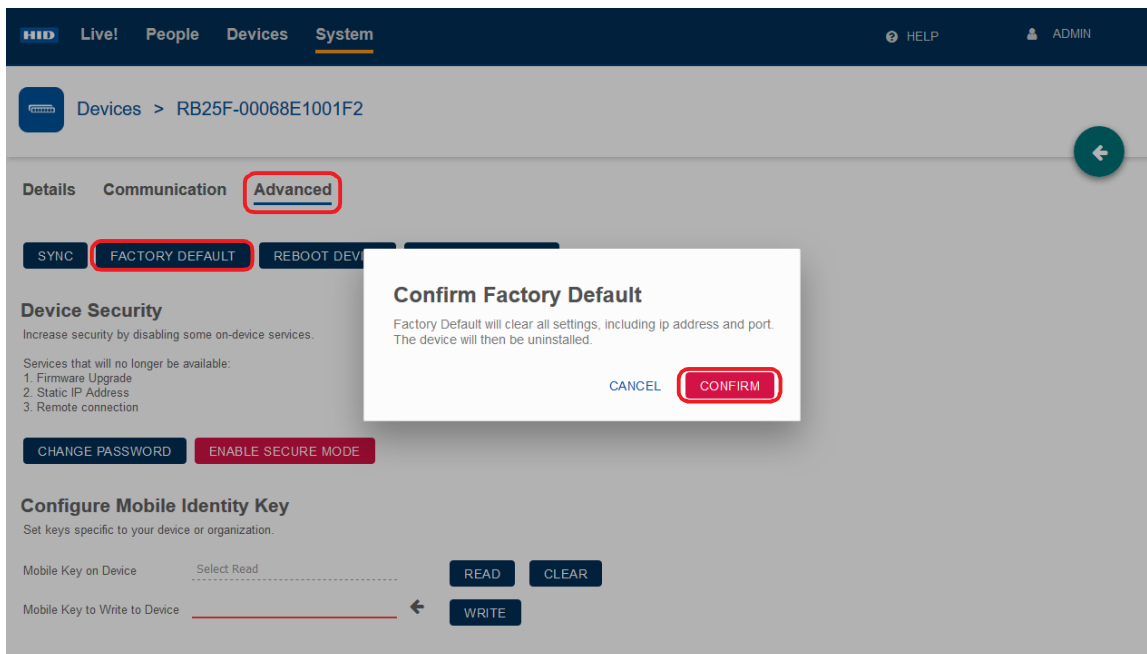
3.4.3 Reset a device

To clear all device settings, including IP address and port:

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.

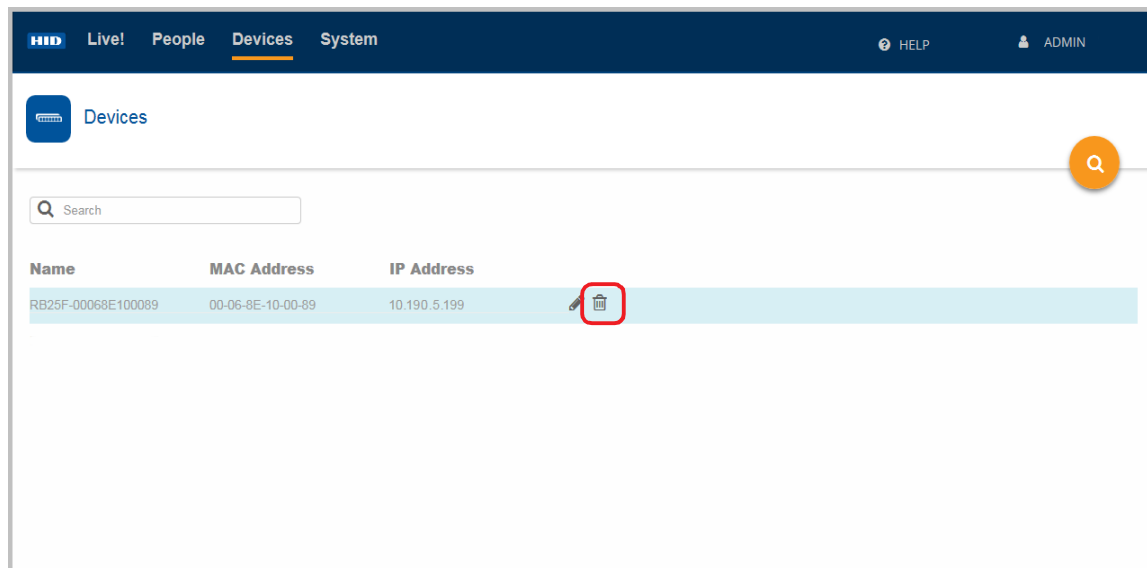


Note: Where communication between HID Biometric Manager and the RB25F is not possible, factory default reset can be carried out at the reader, see *Section 2.4 Hardware reset the RB25F*.

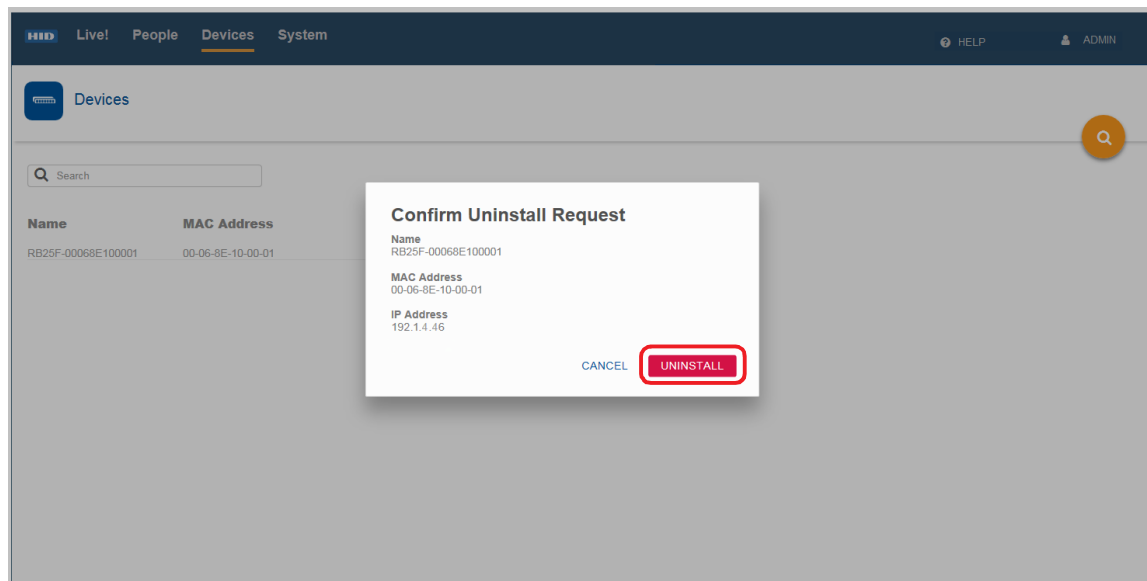
3.4.4 Uninstall a device

To uninstall a device (possibly as a means to resolving issues by removing the device from the database, power cycling, then re-installing the 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*.

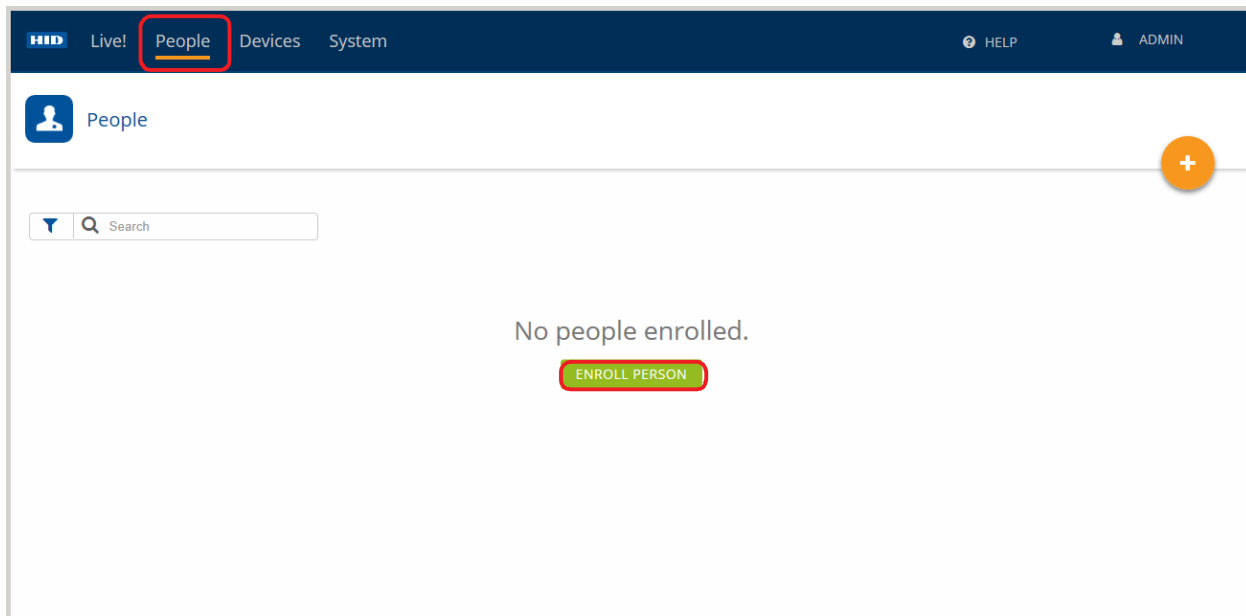
3.5 Enrollment


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

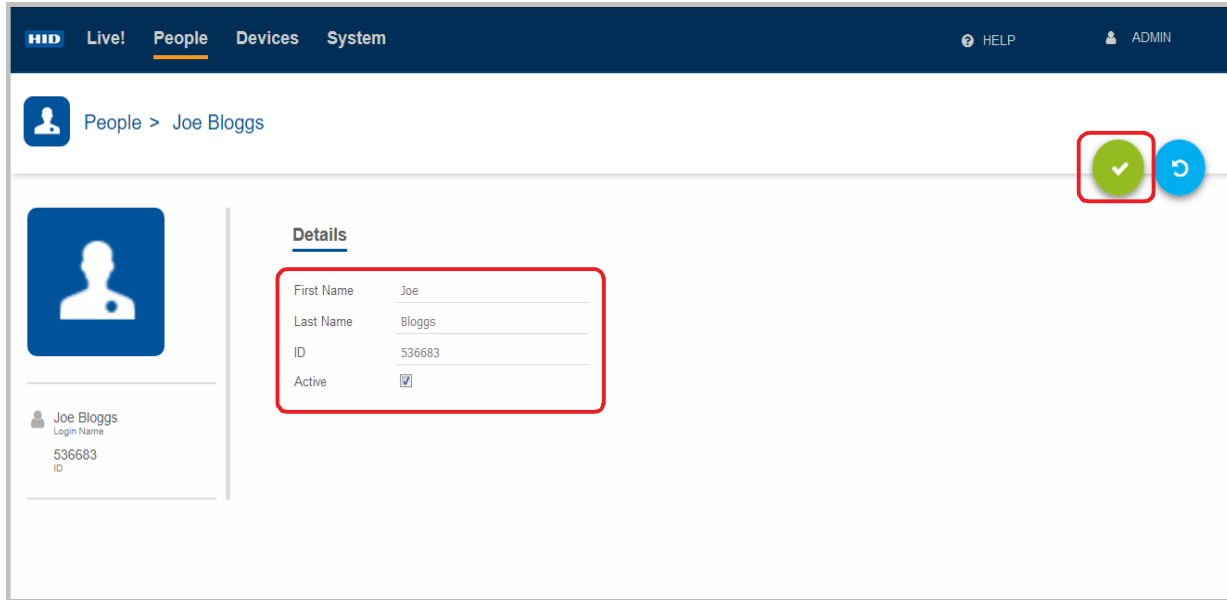
3.5.1 Enroll People

1. Launch HID Biometric Manager and login as either **Administrator** operator or **Enrollment** 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 **ENROLL PERSON**.

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



3. Enter the persons details (**First Name/Last Name**) and a **ID** number.
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 [].





People > Joe Bloggs

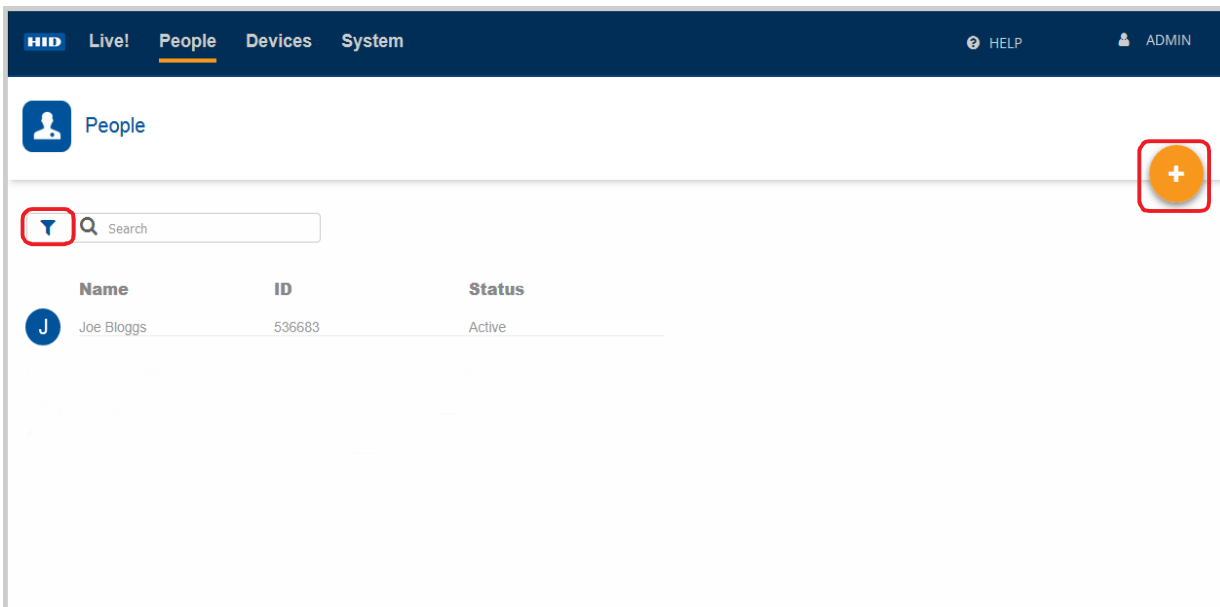
Details

First Name	Joe
Last Name	Bloggs
ID	536683
Active	<input checked="" type="checkbox"/>


Joe Bloggs
Login Name
536683
ID

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.



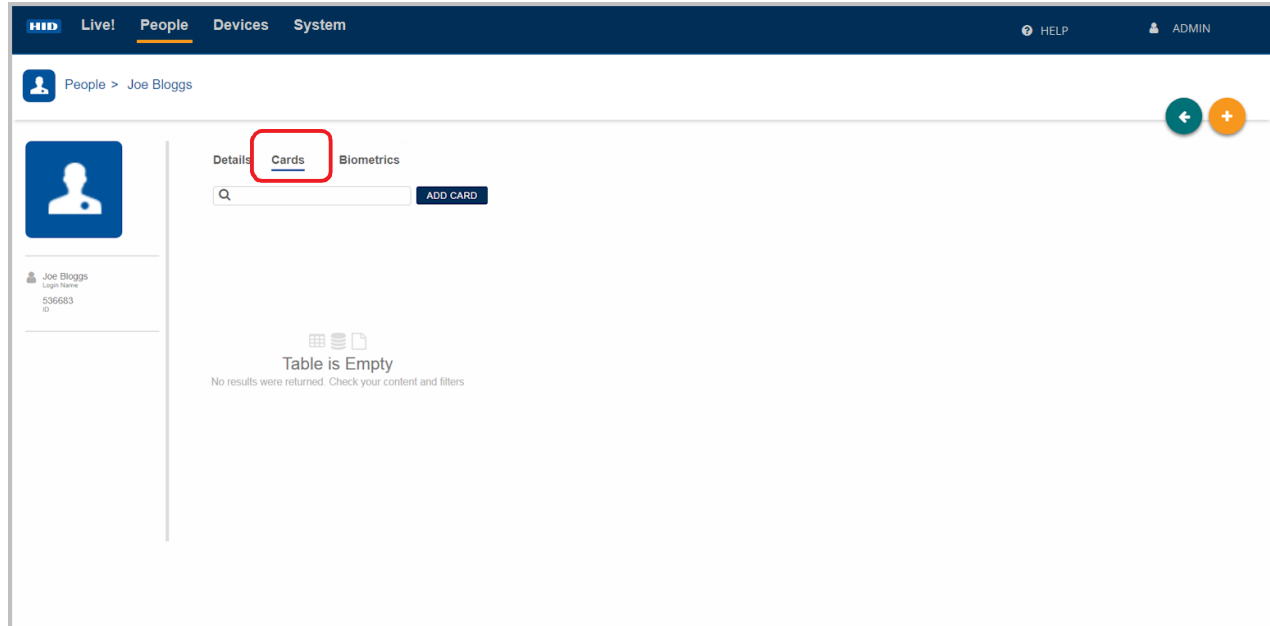
People

 Search

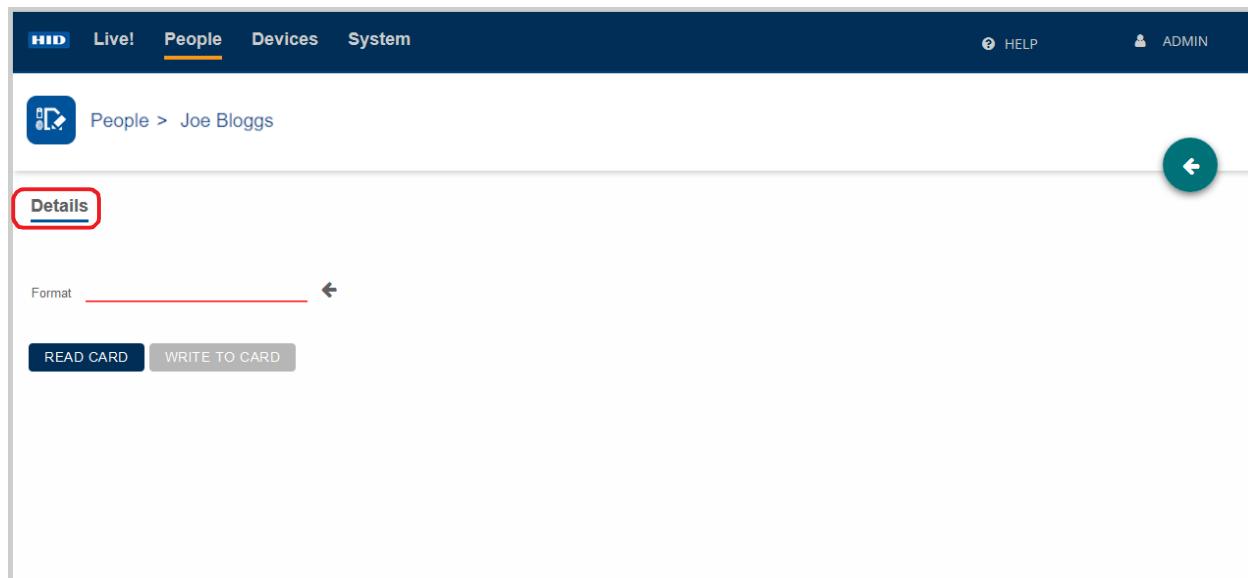
Name	ID	Status
J Joe Bloggs	536683	Active

3.5.2 Enroll Cards

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



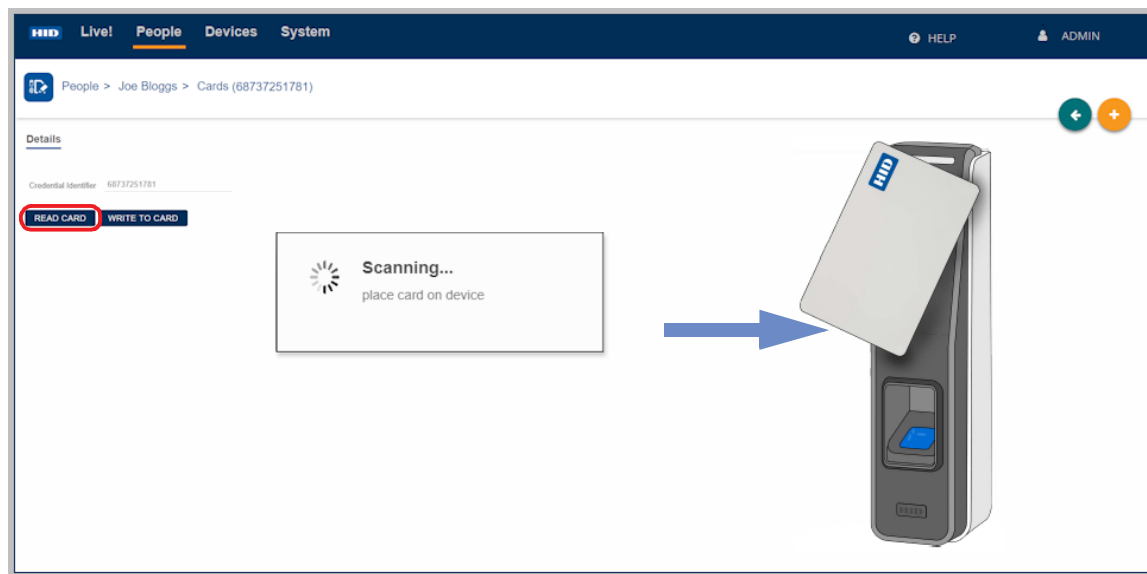
3. At this point on the **Details** screen you can either scan a card to obtain the card details or, if no card is available, manually enter card details.
 - Scan card for card details.
 - Manually enter card details.



Scan card for card details

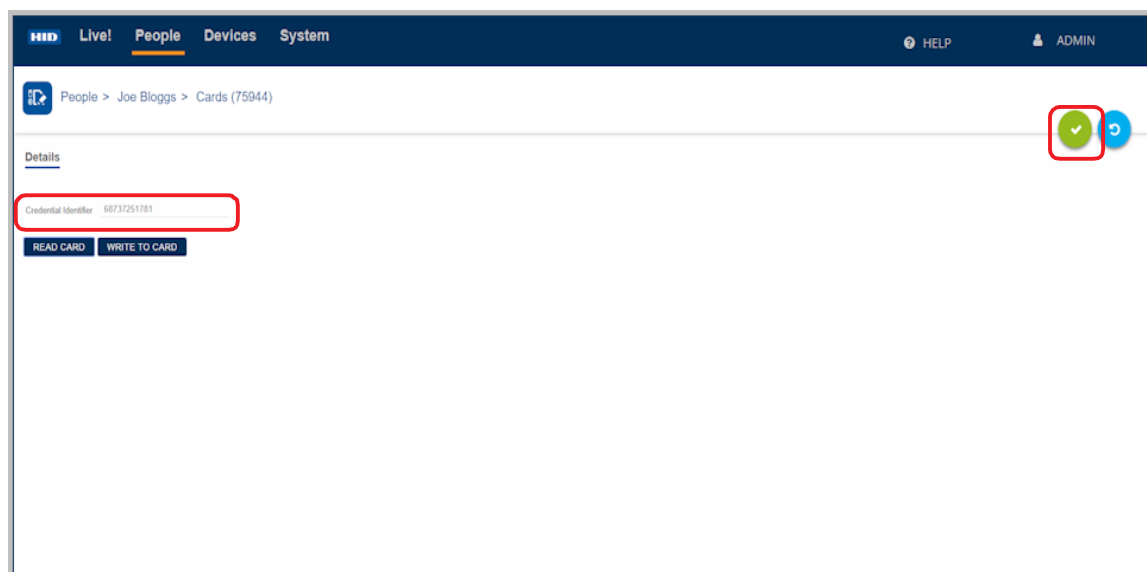
1. On the **Details** screen, click **READ CARD**. If more than one reader is installed, select a device from the displayed list.
2. Within five seconds, present a card to the RB25F device.

Note: The card type supported by the device is configured in the device profile settings, see *Section 3.3.1 Edit a device profile*.



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

Note: The credential recorded in HID Biometric Manager must also be present in the third party PACS software running on the PACS Server.

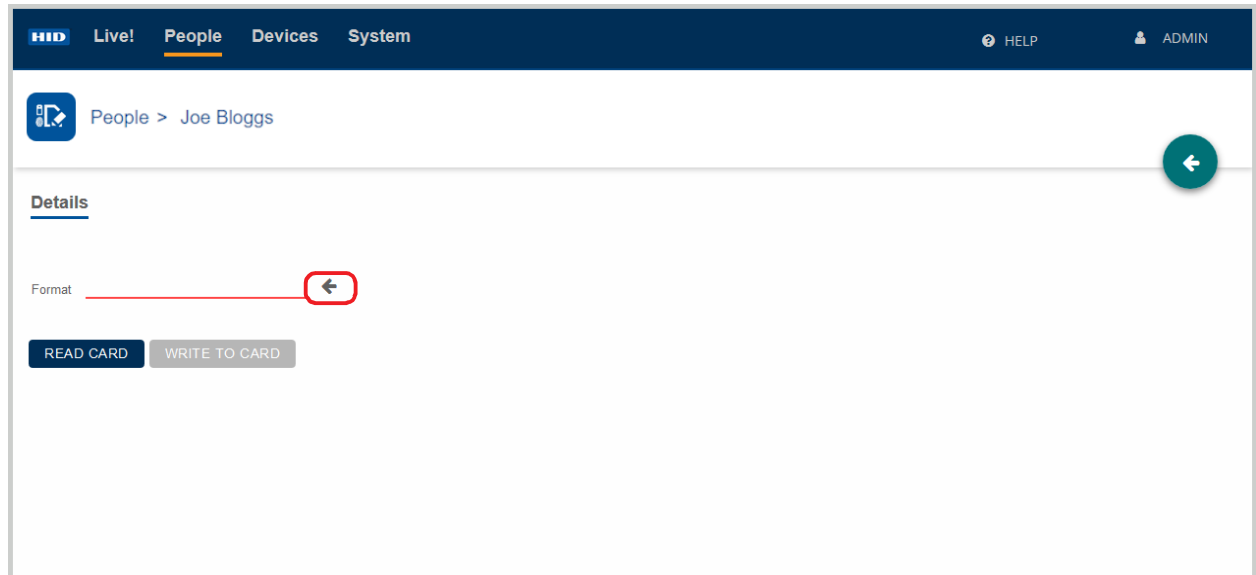


The operator can now collect and add biometric data associated with this enrolled person, see *Section 3.5.3 Enroll Biometrics*.

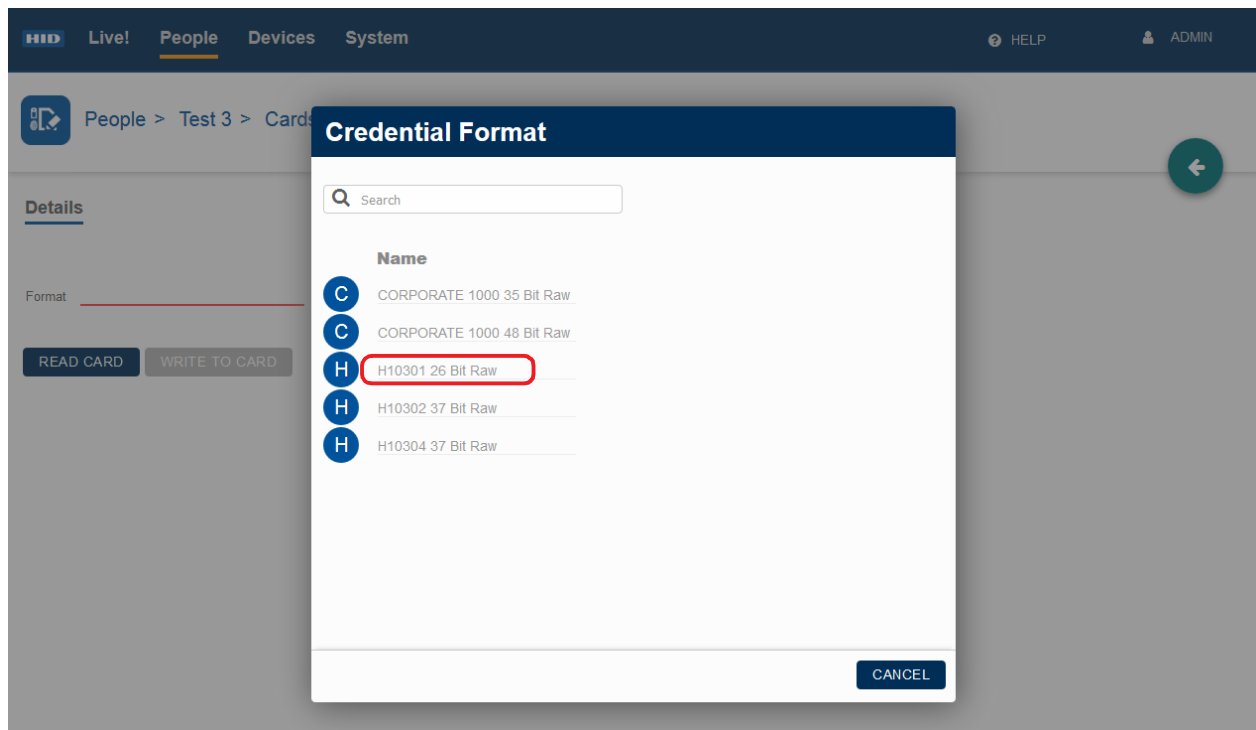
Manually enter card details

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

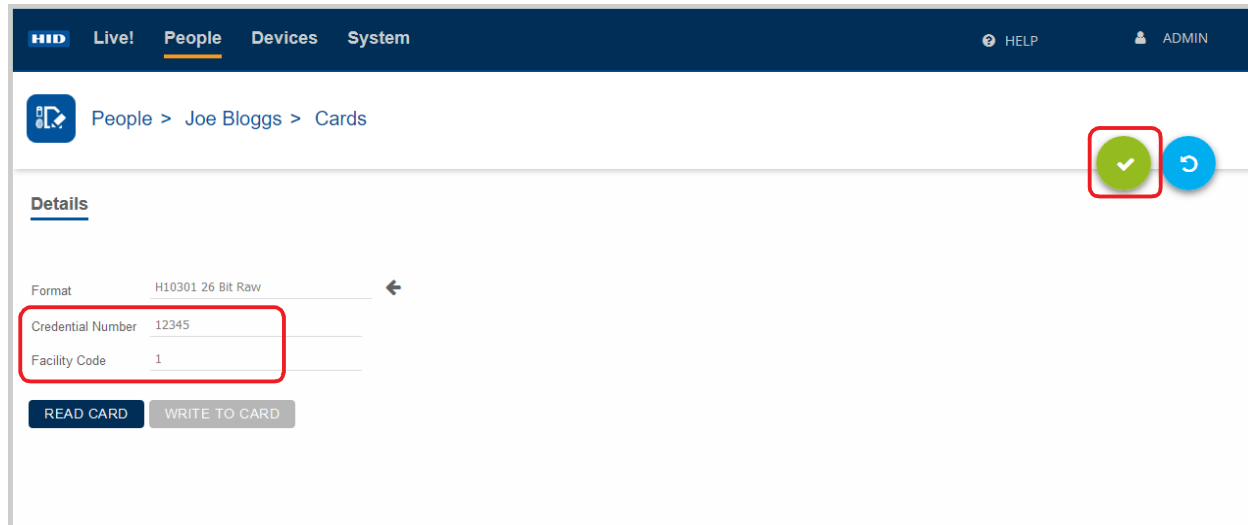
1. On the **Details** screen, select the arrow icon [] associated with the **Format** field.



2. Select the **Credential Format** appropriate for the card in use.



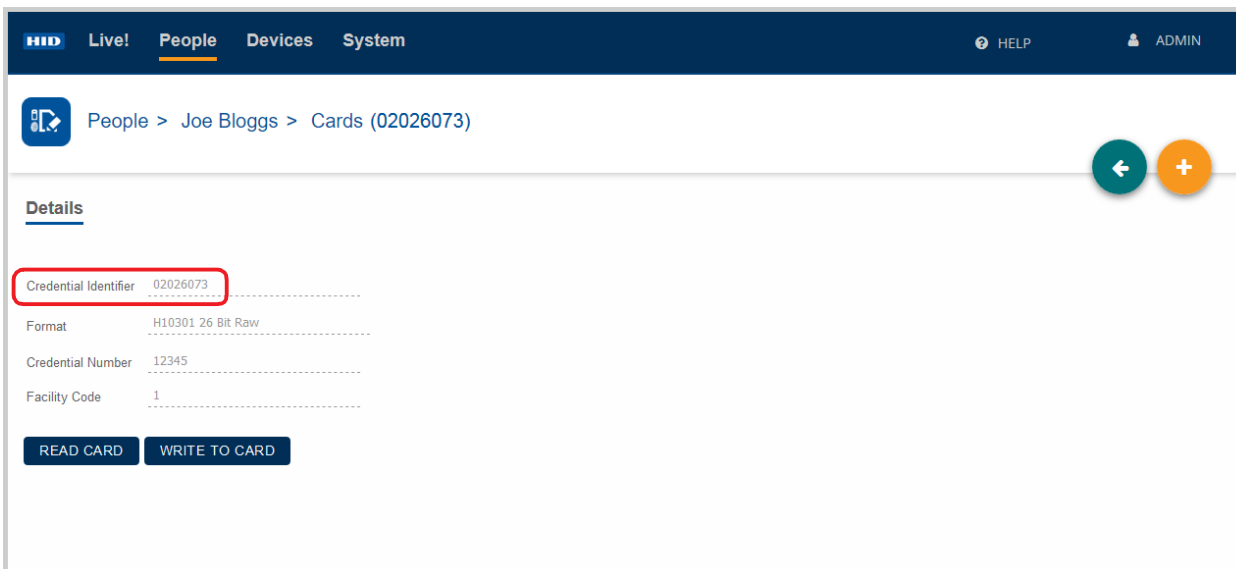
3. Enter a Credential Number (decimal) and Facility Code.
4. Click the **Save** icon [✓] to save these card details.



The screenshot shows the HID Biometric Manager interface. The top navigation bar includes 'HID', 'Live!', 'People', 'Devices', and 'System'. The 'People' tab is selected. The breadcrumb trail is 'People > Joe Bloggs > Cards'. In the 'Details' section, the 'Format' is 'H10301 26 Bit Raw'. The 'Credential Number' is '12345' and the 'Facility Code' is '1'. These two fields are enclosed in a red rectangular box. Below them are buttons for 'READ CARD' and 'WRITE TO CARD'. In the top right corner, there is a green circular icon with a white checkmark, which is also enclosed in a red rectangular box, indicating the save action.

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

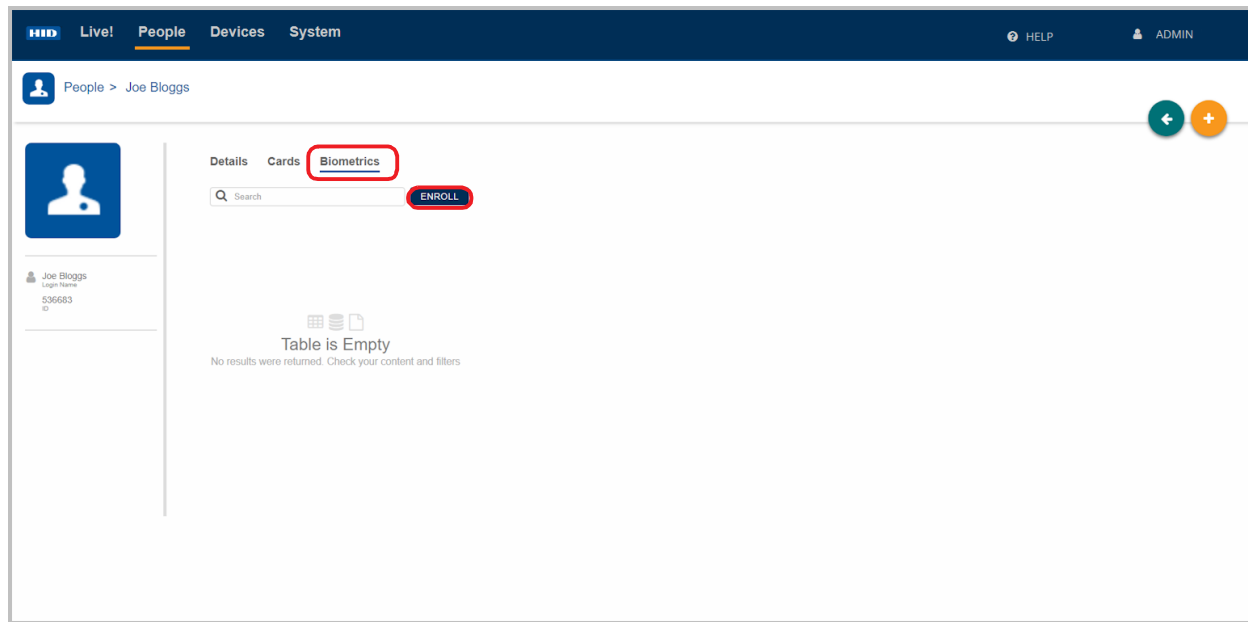
Note: The credential recorded in HID Biometric Manager must also be present in the third party PACS software running on the PACS Server.



The screenshot shows the HID Biometric Manager interface. The top navigation bar includes 'HID', 'Live!', 'People', 'Devices', and 'System'. The 'People' tab is selected. The breadcrumb trail is 'People > Joe Bloggs > Cards (02026073)'. In the 'Details' section, the 'Credential Identifier' is '02026073', which is highlighted with a red rectangular box. Below it, the 'Format' is 'H10301 26 Bit Raw', the 'Credential Number' is '12345', and the 'Facility Code' is '1'. At the bottom are buttons for 'READ CARD' and 'WRITE TO CARD'. In the top right corner, there are two circular icons: a green one with a white left arrow and an orange one with a white plus sign.

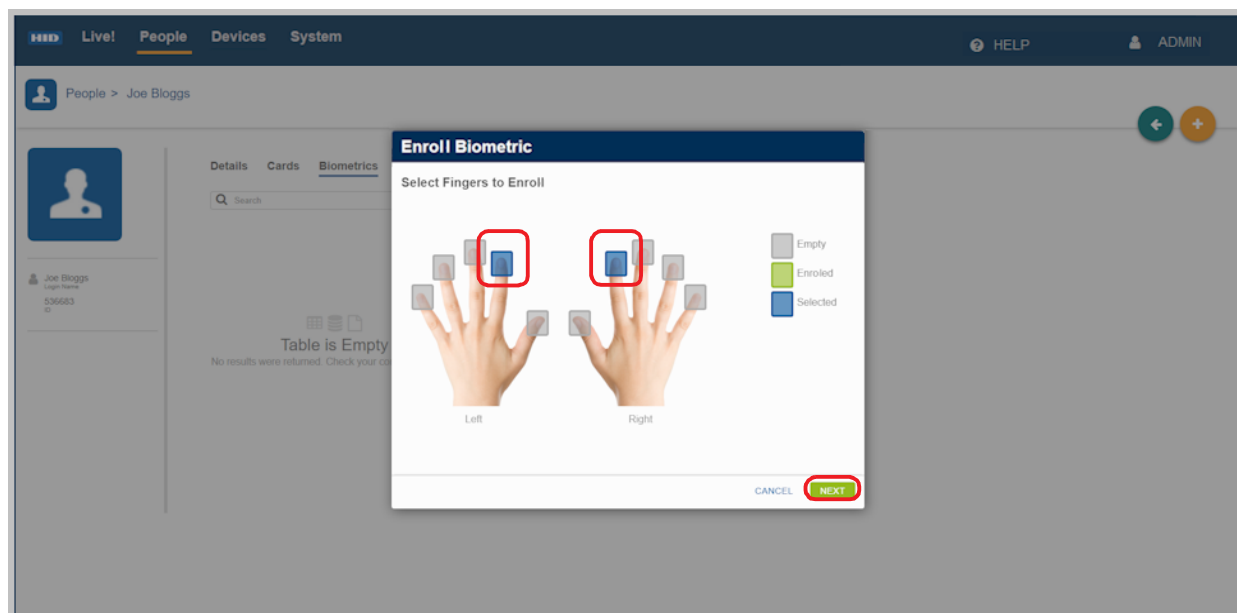
3.5.3 Enroll Biometrics

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



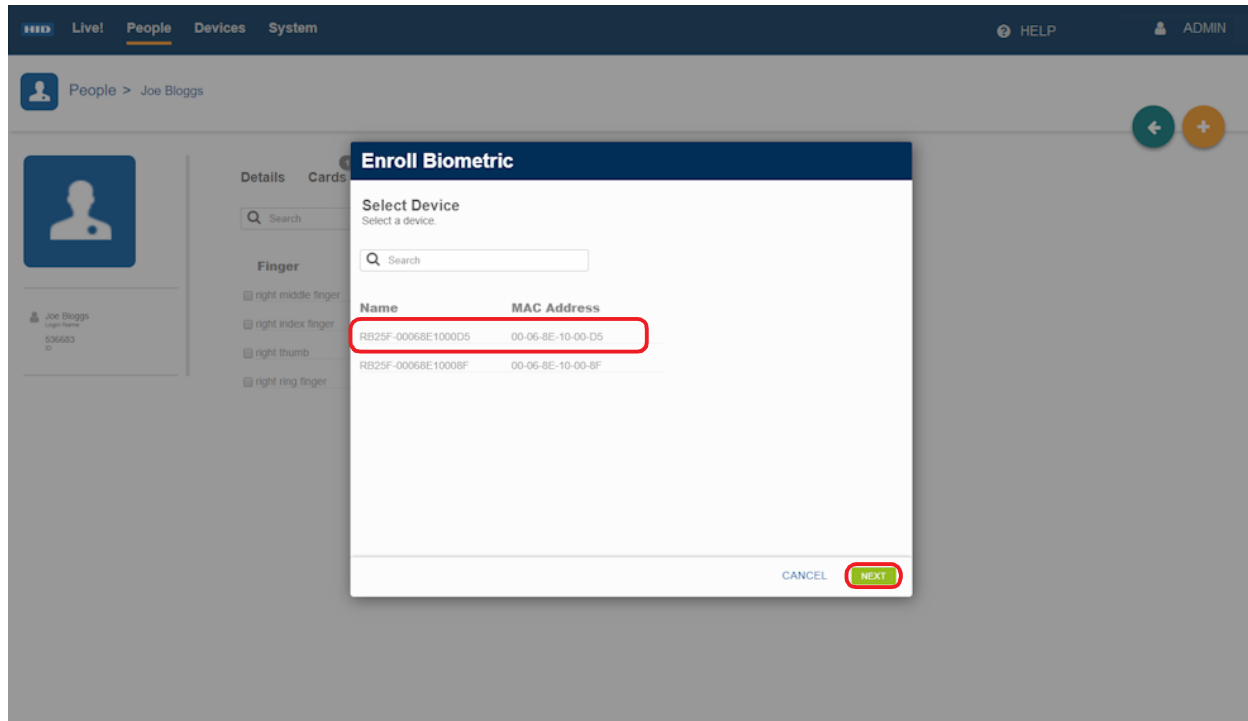
4. In the **Enroll Biometric** dialog select the fingers you wish to enroll and click **Next**.

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.



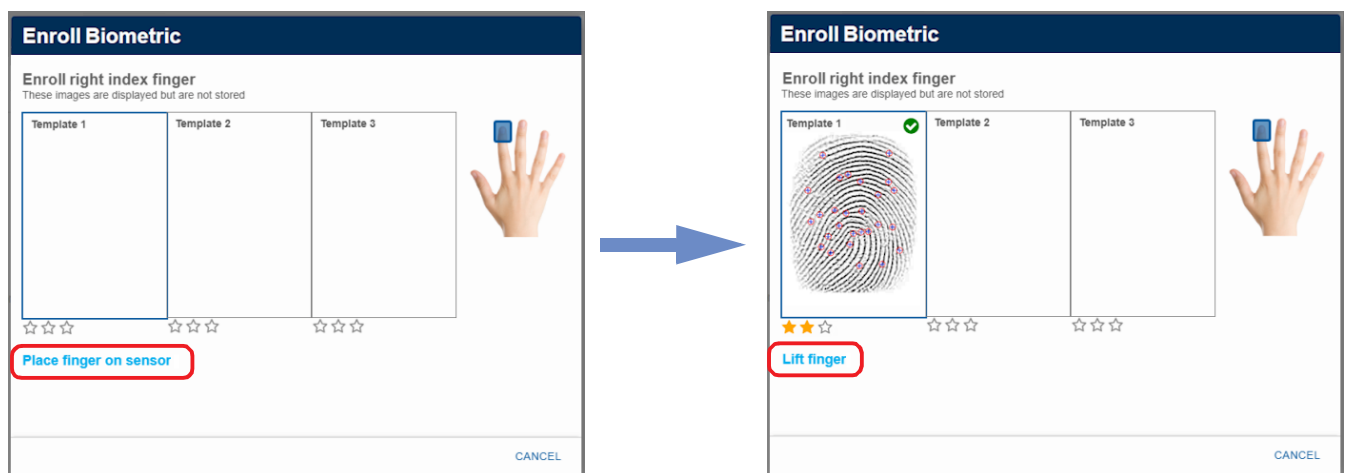
- Select a device from the displayed list and click **Next**.

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



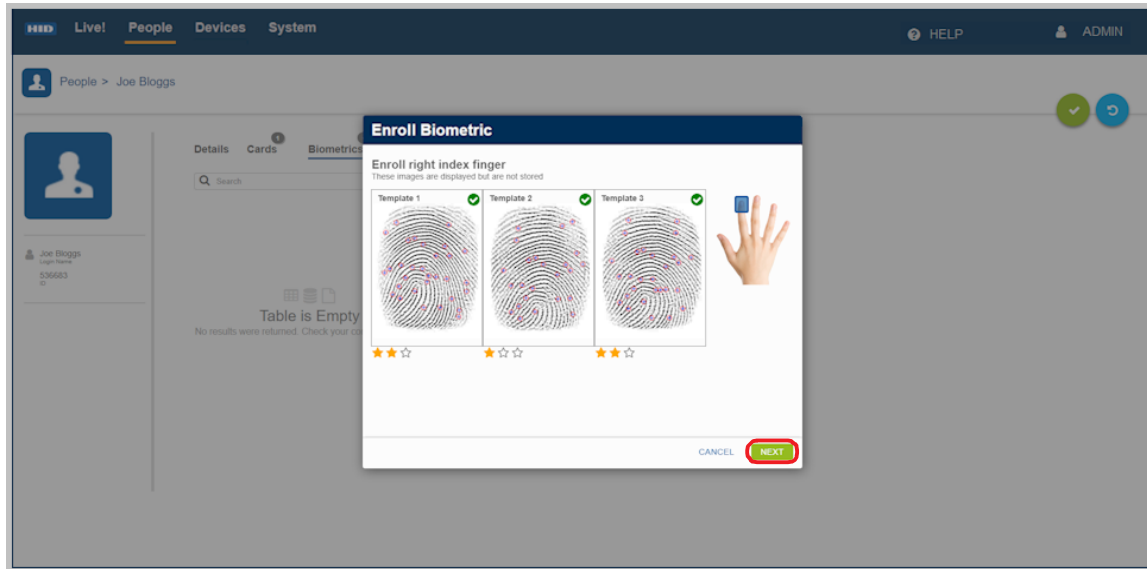
- For the highlighted finger you will be prompted to **<Place finger on sensor>** followed by **<Lift finger>**. It is recommended that you follow the on-screen prompts, in the correct sequence, to ensure a successful finger scan.

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



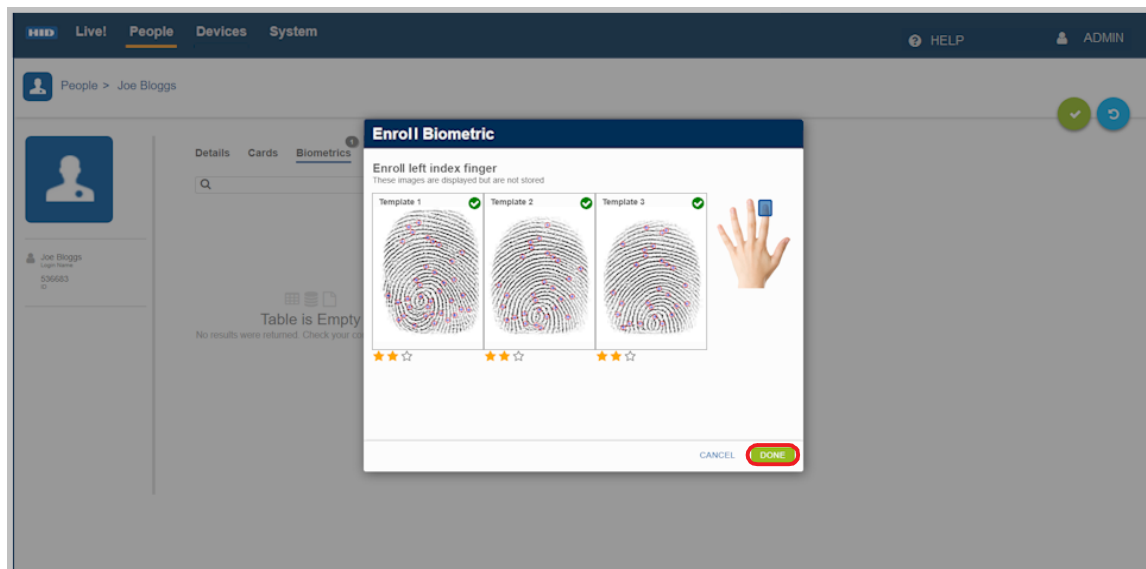
- Continue to follow the on-screen prompts until you have successfully scanned the first finger three times. Click **Next**.

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 fingerprints are associated with the top credential in the credential list.

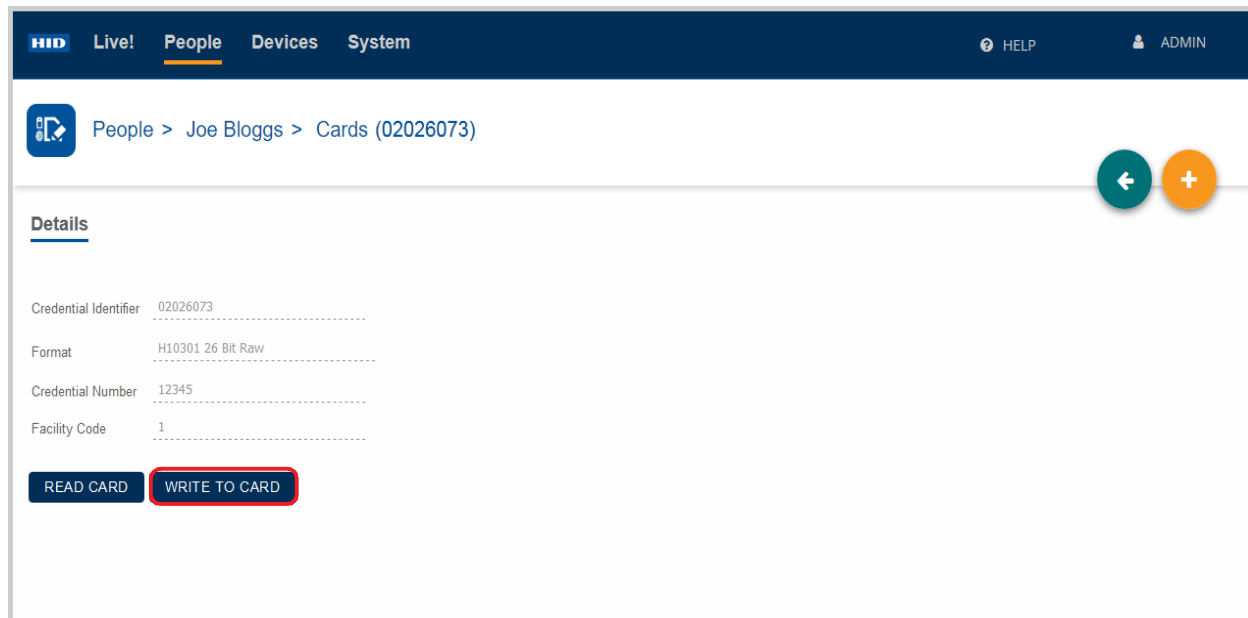
Note: If the top credential in the credential list is deleted then enrolled fingerprints are associated with the next credential in the list. If all credentials are deleted then the biometrics are also deleted.



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.

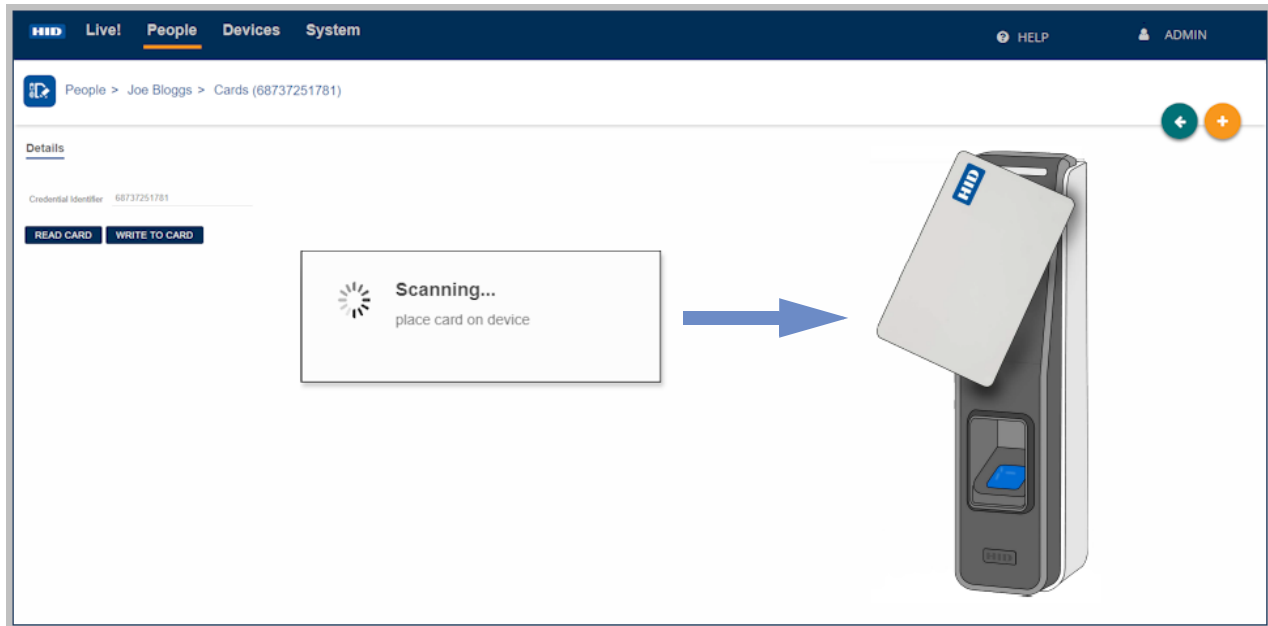
1. On the **People** screen select a displayed person record.
2. On the **Cards** screen select a displayed **Credential Identifier**.
3. Click **WRITE TO CARD** to copy the templates to the card.



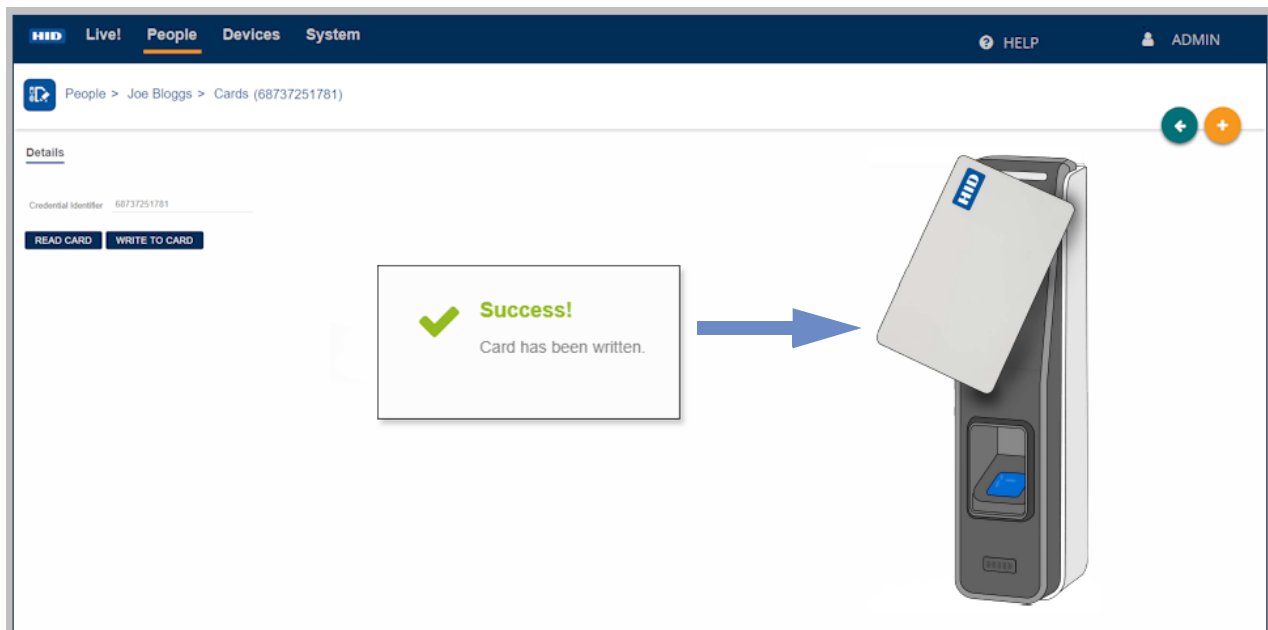
4. Select the fingers (maximum of two) you wish to be written to the card and click **WRITE TO CARD**.



5. You will have approximately five seconds to present the supported 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 System monitoring and Reports

3.7.1 View Biometric Manager events

Actions carried out in Biometric Manager are logged as events. To view a HID Biometric Manager events, click the **Live!** option. To examine individual entries when the network is busy click the pause icon [⏸] to pause real-time network monitoring.

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

Date/Time	Event	Device	Name	Card
2019-08-04 08:47:12	Configuration Updated	RB25F-00068E100001		
2019-08-04 08:13:10	Configuration Updated	RB25F-00068E100001		
2019-08-04 08:08:18	Unit Power Up	RB25F-00068E100001		
2019-08-04 08:06:35	RFID Credential Read	RB25F-00068E100001	Joe Bloggs	75944
2019-08-04 08:06:28	RFID Credential Read	RB25F-00068E100001	536683	75944
2019-08-04 08:04:15	Configuration Updated	RB25F-00068E100001		
2019-08-04 08:04:11	RFID Credential Read	RB25F-00068E100001		75944
2019-08-04 08:03:08	RFID Credential Read	RB25F-00068E100001		75944
2019-08-04 08:02:00	RFID Credential Read	RB25F-00068E100001		75944

To filter displayed events select the **Filters** option. Any current filters in use are displayed. Click **ADD FILTER** to create a new filter based on a **Name**, **Event**, or **Device**. Click the **Save** icon [✓] to save any added filters.

Note: If no filters are used then the default filter is applied. This displays events only for the calendar day.

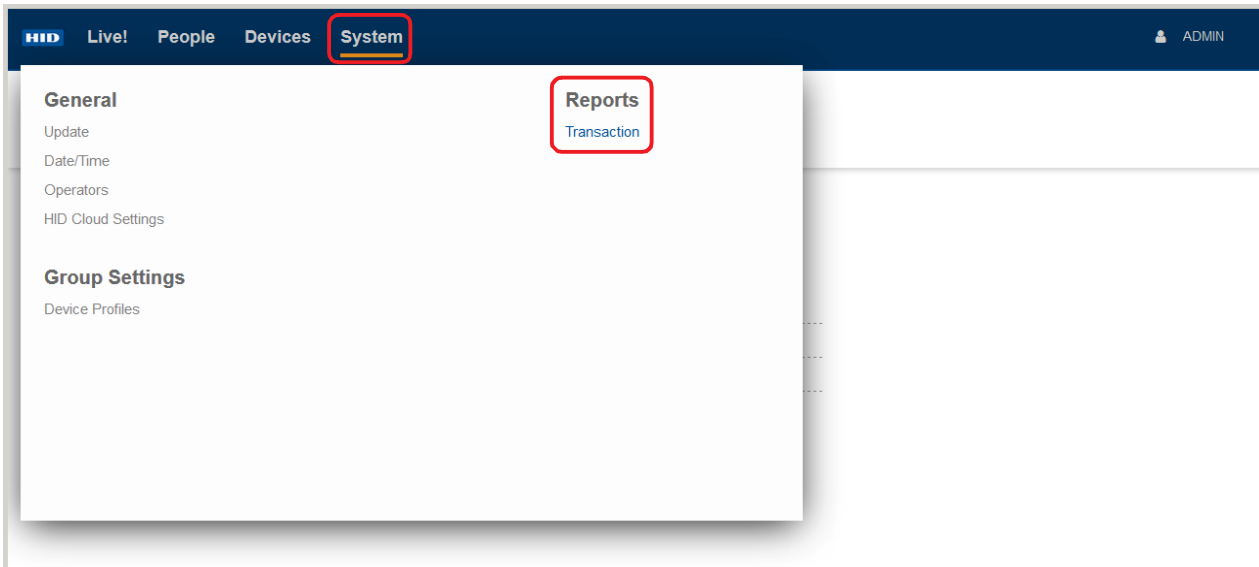
Filters In Use

✗ Event Anti Tamper ←

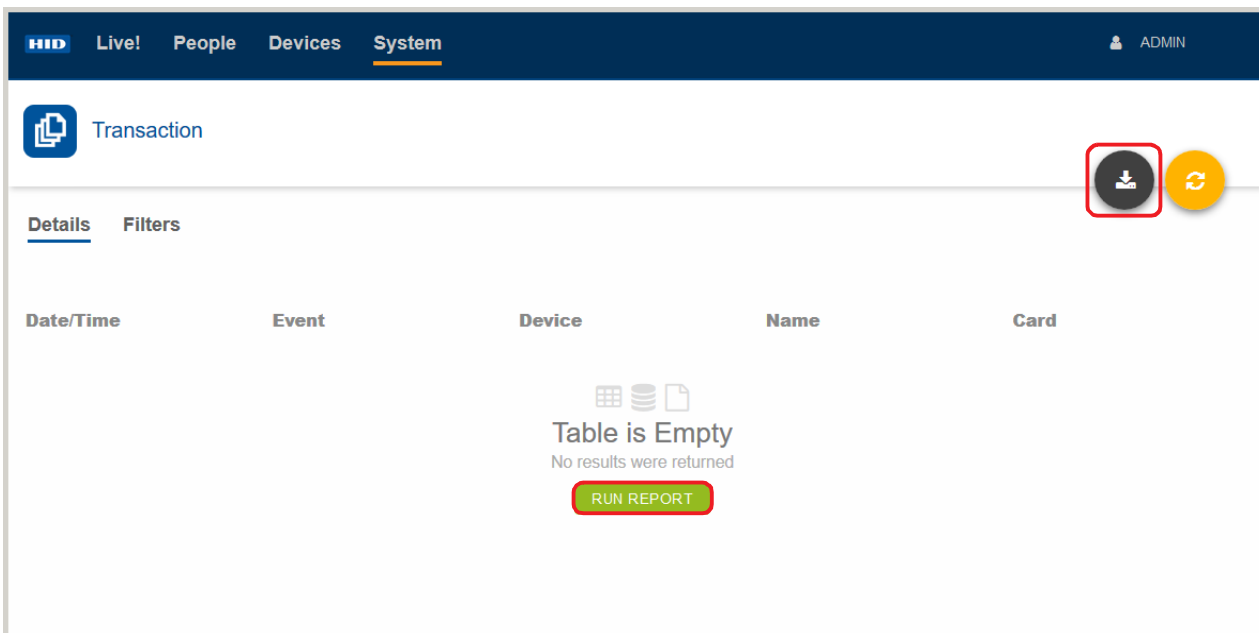
ADD FILTER

3.7.2 Transaction Reports

To create a report of HID Biometric Manager transactions click **System** and select **Transaction** option.

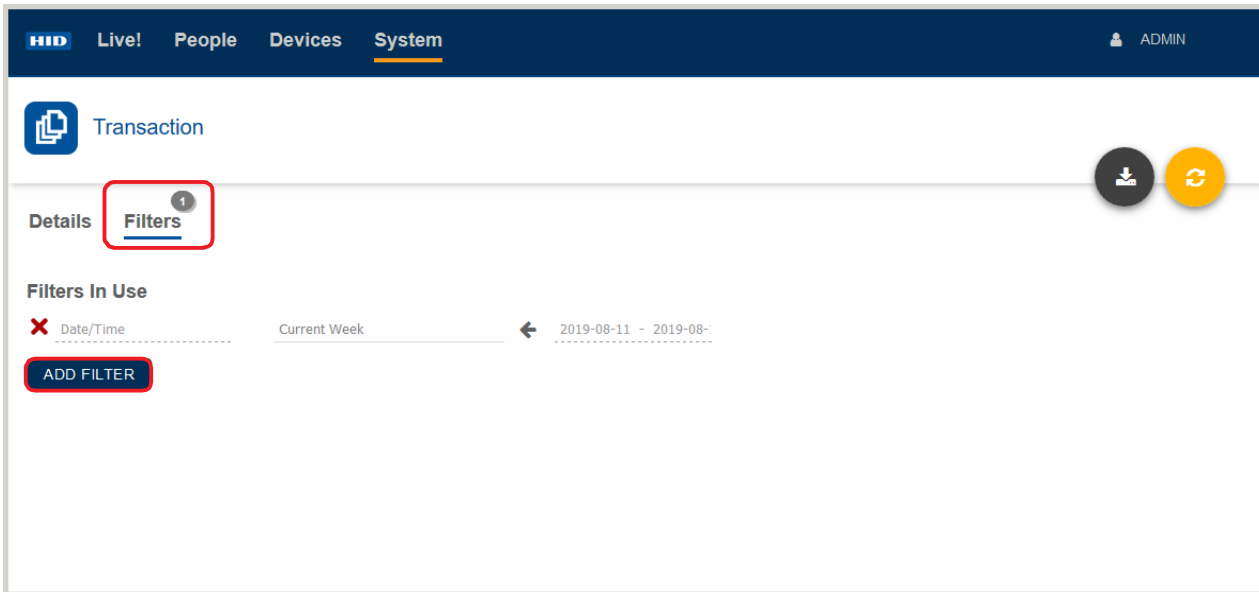


Click **RUN REPORT** to create a report of HID Biometric Manager transactions. Once the report is created click the save report icon [📄] to save the report to a PDF or CSV file.



To filter report content select the **Filters** option. Any current filters in use are displayed. Click **ADD FILTER** to create a new filter based on a **Controller**, **Date/Time**, **Event**, or **Person/Asset**. Click the **Save** icon [✓] to save any added filters.

Note: If no filters are used then the default filter is applied. This displays events only for the calendar day.





Appendix A

A Biometric Manager Mobile Access setup

This section provides details on the prerequisites that must be in place in order to setup a connection between HID Biometric Manager and the HID Mobile Access Portal. The section also details on how to verify HID Reader Manager Technician account details in Biometric Manager and how to load Mobile Access® (MOB) keys onto the RB25F.

A.1 Setup prerequisites

In order to setup a connection between HID Biometric Manager and HID Mobile Access for updates and to facilitate loading MOB keys onto the RB25F the following prerequisites must be in place.

A.1.1 HID Mobile Identities setup

The Organization must register for HID Mobile Identities via the onboarding process. The onboarding process will setup an Organizational account in the HID Mobile Access Portal and creates a primary account administrator. For detailed information on the onboarding process visit the onboarding site at:

<https://manageservices.hidglobal.com/faces/maUserOnBoardingStart>

For information relating to the HID Mobile Access solution, including the HID Mobile Access Portal, refer to the following:

- *HID Mobile Access Solution Overview* (PLT-02078).
- *HID Mobile Access Frequently Asked Questions* (PLT-02085).

A.1.2 HID Reader Manager setup

The Mobile Access Portal administrator creates a Reader Manager administrator in the Mobile Access Portal. A designated Reader Technician downloads, registers, and authenticates the HID® Reader Manager™ App on a mobile device. The Reader Manager Portal administrator enrolls the Reader Technician and issues Authorization Keys to the Reader Technician. For information relating to setup procedures for HID Reader Manager Portal Administrators and Reader Manager Technicians refer to:

- *HID Reader Manager Solution User Guide (iOS)* (PLT-03683).
- *HID Reader Manager Solution User Guide (Android)* (PLT-03858).

A.1.3 Mobile Access user setup

The Mobile Access Portal administrator enrolls mobile users in the system and issues Mobile IDs. End users download and install the HID Mobile Access App on their mobile devices. For detailed information refer to the following:

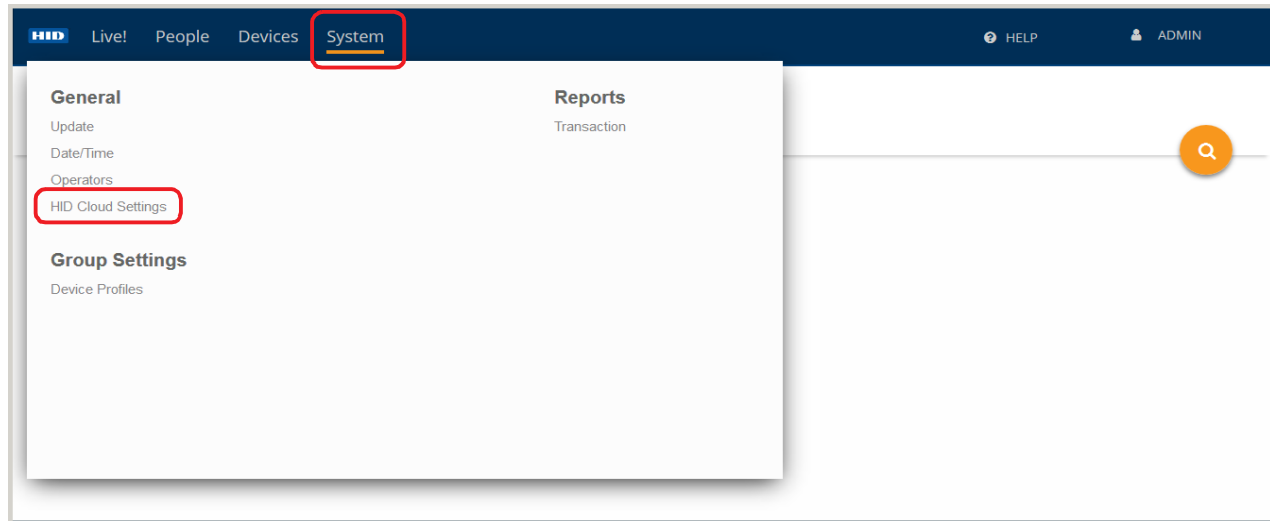
- *HID Mobile Access Frequently Asked Questions* (PLT-02085).
- *HID Mobile Access App User Guide* (PLT-02077).

A.2 Validate a Reader Manager account in HID Biometric Manager

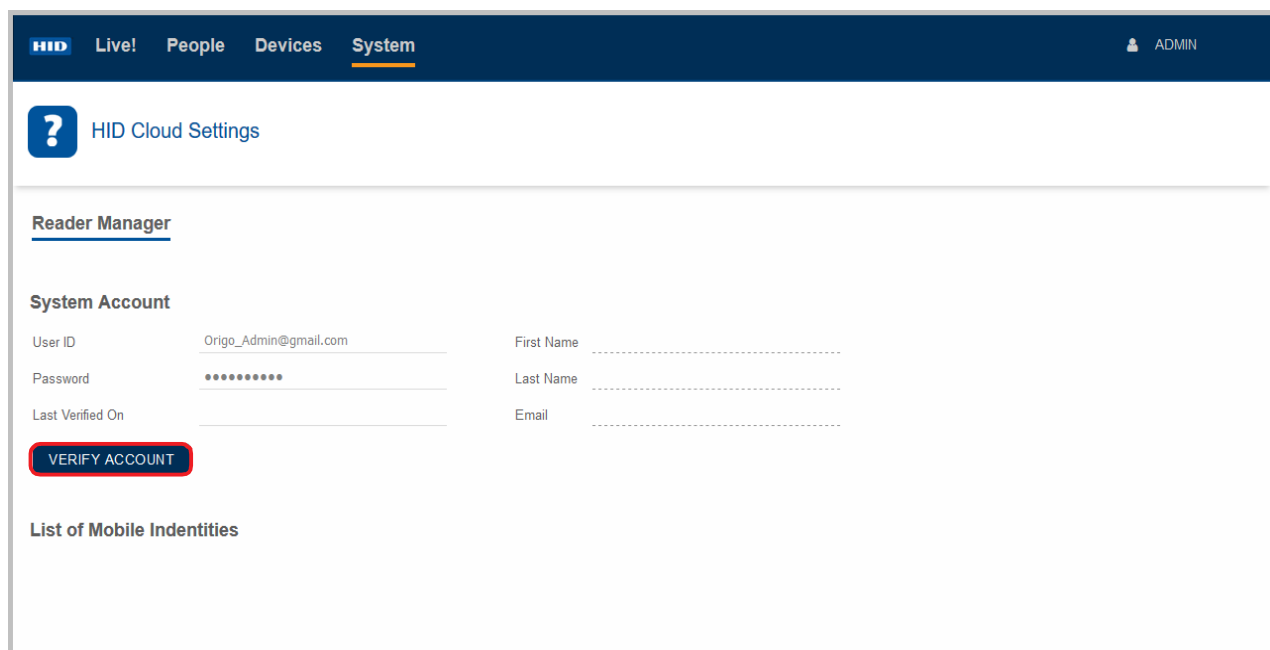
In order to validate a Reader Manager Technician account in HID Biometric Manager an active Reader Manager Technician account must be present, see *Appendix A - HID Reader Manager setup*.

To validate a Reader Manager Technician account (this should be the Portal admin or a company employee) in HID Biometric Manager:

1. Log into HID Biometric Manager.
2. Select **System** and under the **General** section click **HID Cloud Settings**.



3. On the **HID Cloud Settings** page enter the Reader Manager Technician (this should be the Portal admin or a company employee) account details (User ID/Password) and click **VERIFY ACCOUNT**.





If the Reader Technician account has not been authorized for any MOB keys then no keys are listed under **List of Mobile Identifiers**. If MOB keys have been assigned to the account then these will be listed in.

HID Live! People Devices System ADMIN

? HID Cloud Settings

Reader Manager

System Account

User ID: Origo_Admin@gmail.com First Name: Biometric
Password: Password field Last Name: Manager
Last Verified On: Last Verified On field Email: Origo_Admin@gmail.com

VERIFY ACCOUNT


List of Mobile Identities

MobileKey : MOBA233
CustomerName : Eureka Demo Org
IssuedOn : 2019-07-12T14:47:59+01:00
ExpiresOn : 2024-07-12T14:47:59+01:00
EndPoint : 908071513

ICLASS[®] Seos[®]

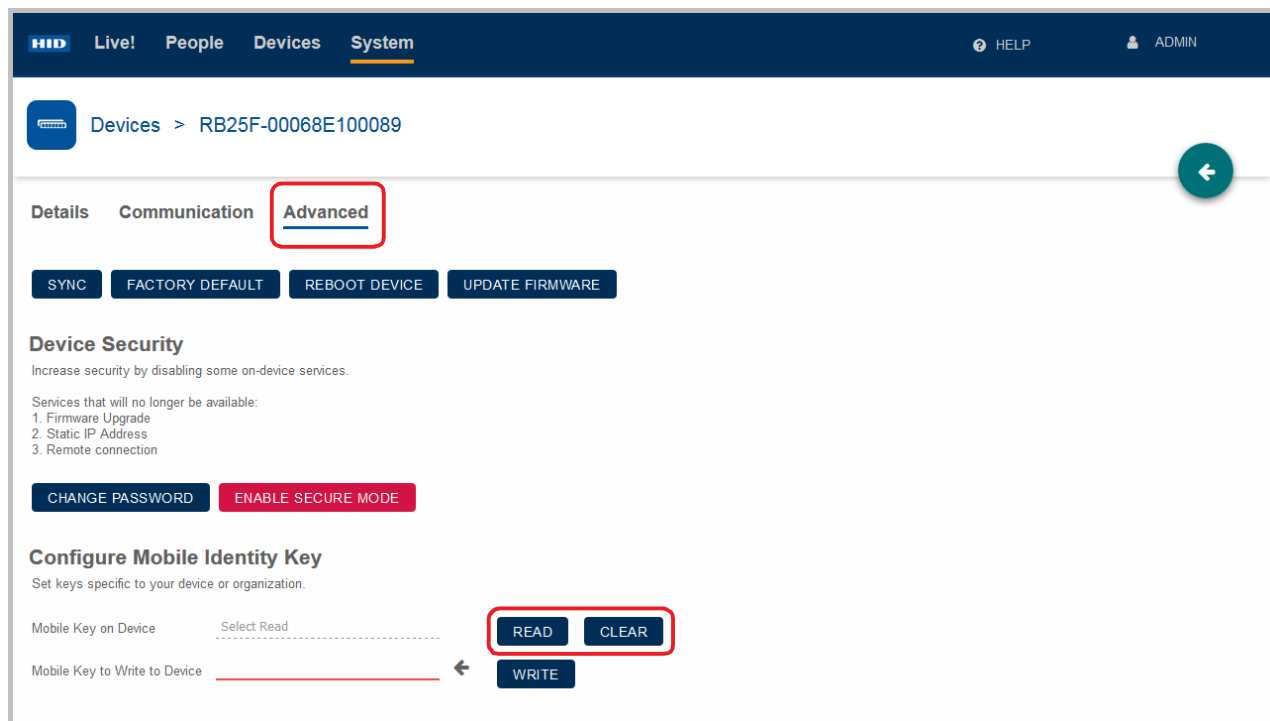
A.3 Load a MOB key onto a device

To load a Mobile Access (MOB) key onto a RB25F device with HID Biometric Manager:

1. In HID Biometric Manager, select the **Devices** option and click on the **Edit** icon [] associated with the device.

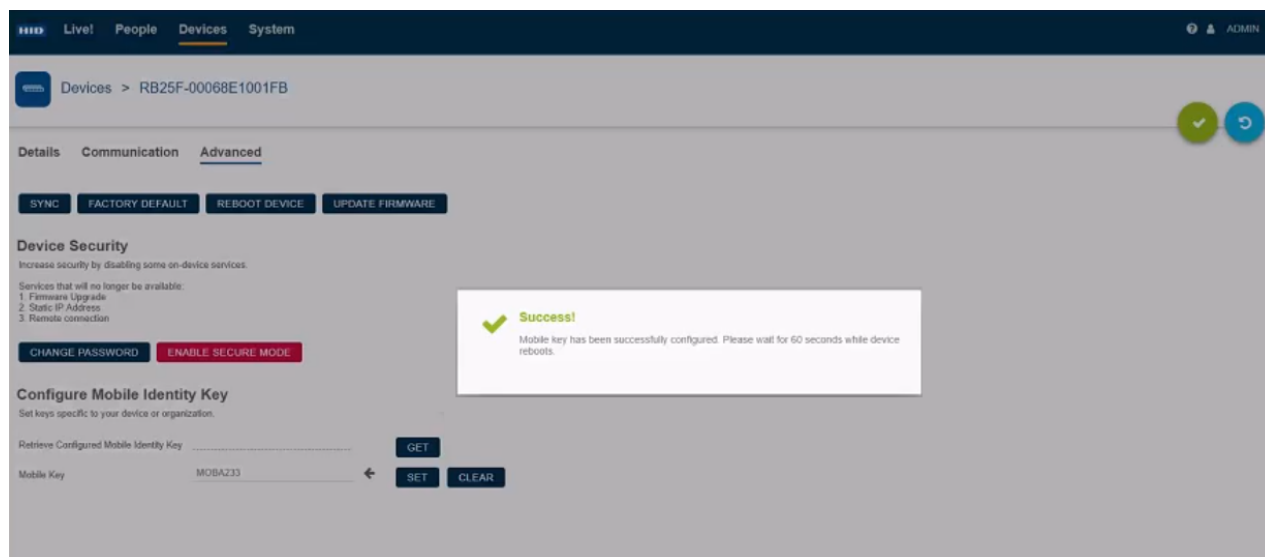
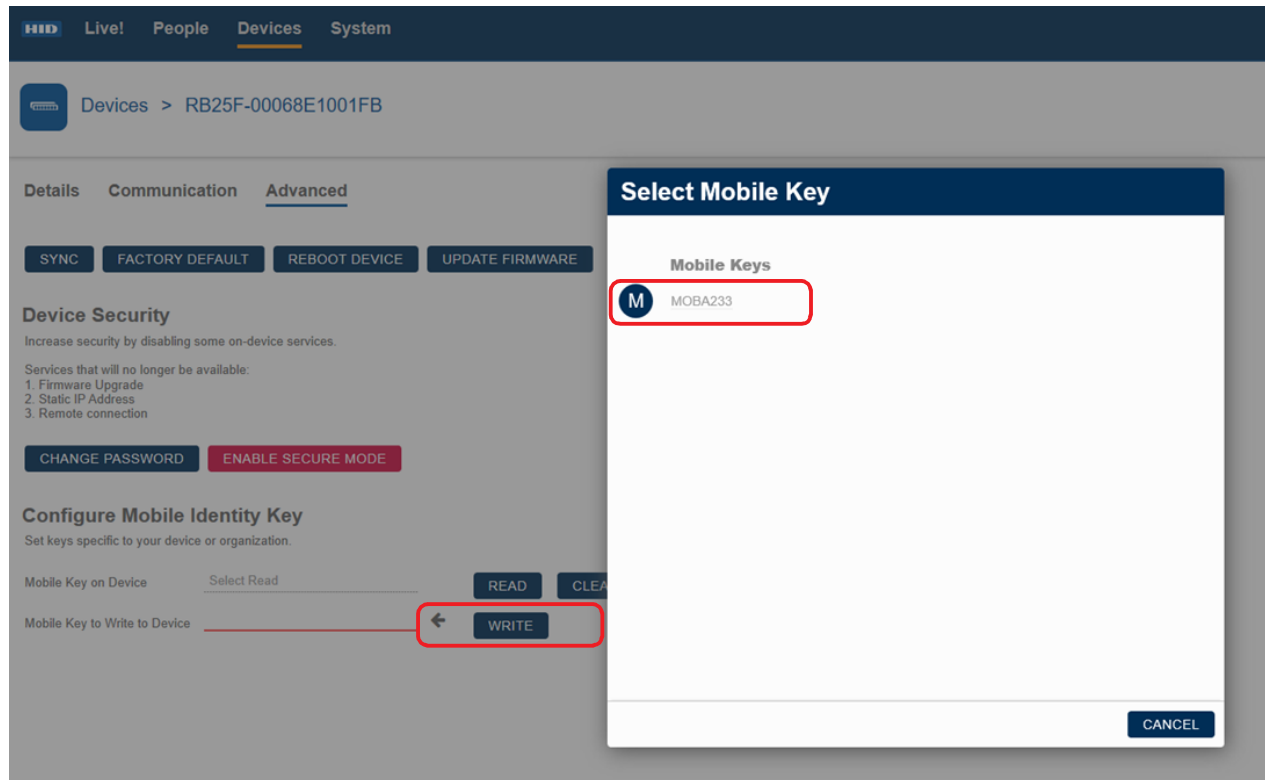


2. On the Devices page, select the **Advanced** option. Click **READ** to check for any previously loaded MOB keys on the device. Click **CLEAR** to remove any displayed MOB keys that have been read from the device.



- Click the arrow icon associated with **Mobile Key to Write to Device** and select a MOB key from the list.
- Click **WRITE** to load the selected MOB key onto the device.

Note: The device can only contain one MOB key at any given time.



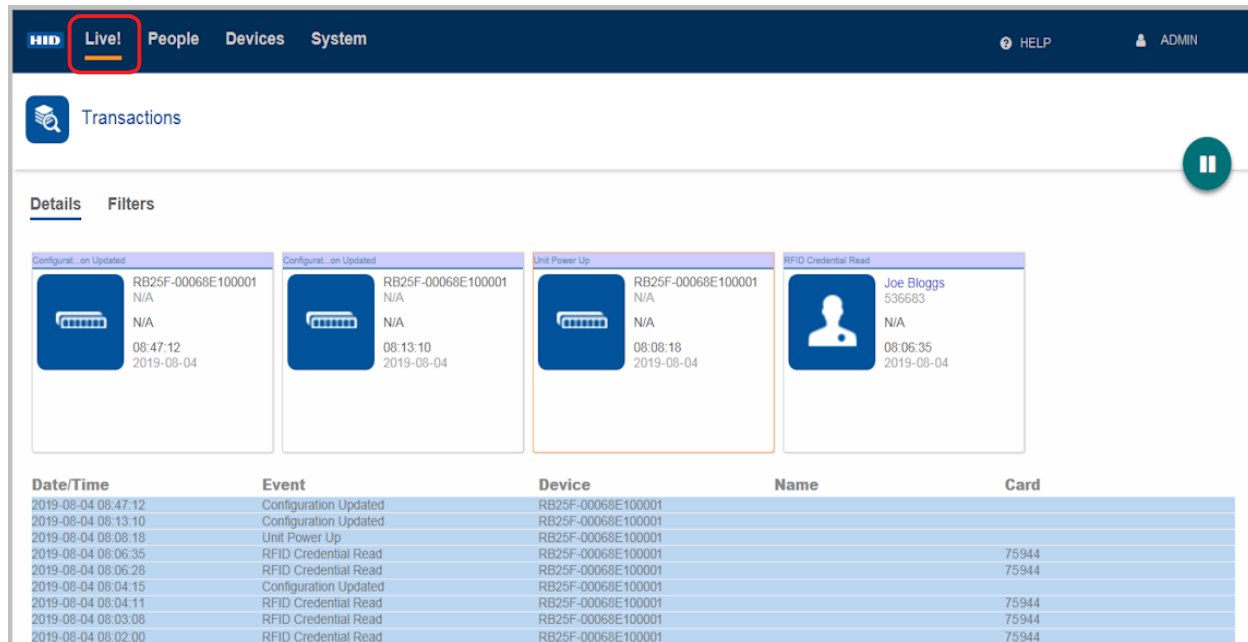
A.4 Test MOB keys are working correctly

As a prerequisite to test that a MOB key working correctly, the Mobile Access Portal administrator must have enrolled mobile users in the system and issued Mobile IDs to the mobile device that has the HID Mobile Access App installed, see *Appendix A - Mobile Access user setup*.



To test a MOB key in Biometric Manager:

1. Log into HID Biometric Manager and click the **Live!** option to view HID Biometric Manager events.



Date/Time	Event	Device	Name	Card
2019-08-04 08:47:12	Configuration Updated	RB25F-00068E100001		
2019-08-04 08:13:10	Configuration Updated	RB25F-00068E100001		
2019-08-04 08:08:18	Unit Power Up	RB25F-00068E100001		
2019-08-04 08:06:35	RFID Credential Read	RB25F-00068E100001	Joe Bloggs	75944
2019-08-04 08:06:28	RFID Credential Read	RB25F-00068E100001	536683	75944
2019-08-04 08:04:15	Configuration Updated	RB25F-00068E100001		
2019-08-04 08:04:11	RFID Credential Read	RB25F-00068E100001		75944
2019-08-04 08:03:08	RFID Credential Read	RB25F-00068E100001		75944
2019-08-04 08:02:00	RFID Credential Read	RB25F-00068E100001		75944

2. Present the mobile device to the RB25F and check the **Live!** screen to see events showing the mobile access read and the associated credential identifier.

Note: Mobile Access read will only work if the RB25F is in one of the authentication modes that support card read, i.e. **Card Only**, **Card or Finger**, or **Card + Finger**. Mobile Access will not work if the RB25F is in finger mode.

Appendix B

B 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.

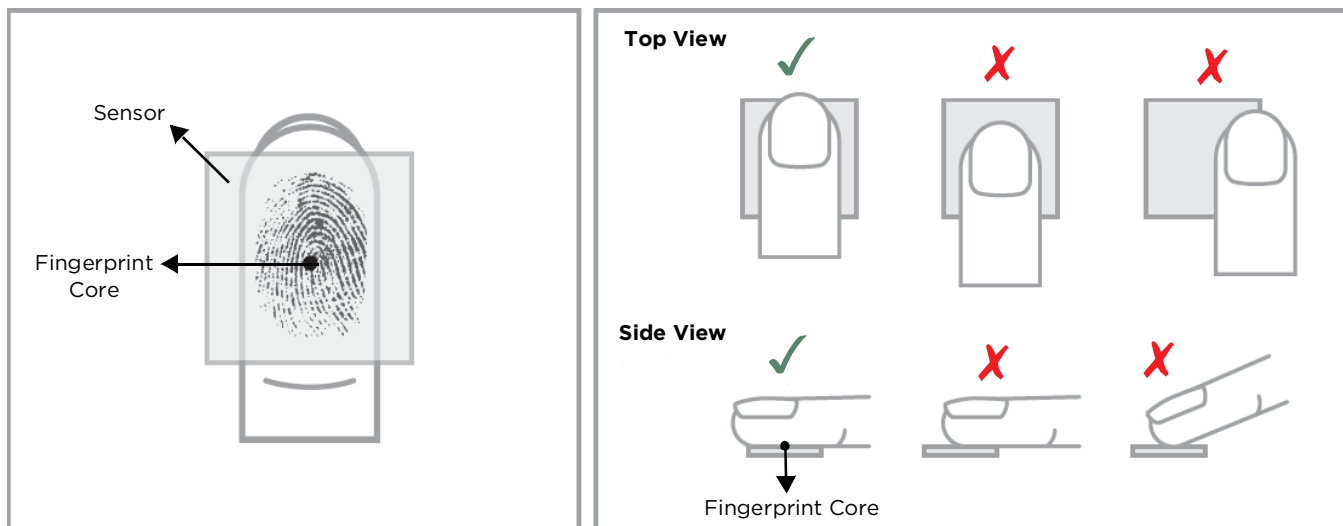
B.1 General guidelines

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

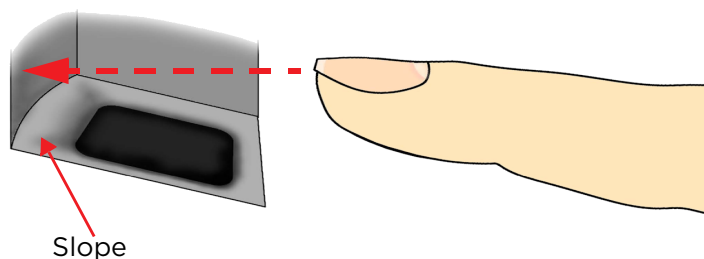
Do not use acidic liquids, alcohol or abrasive materials to clean the sensor.

Common reasons for enrollment failure

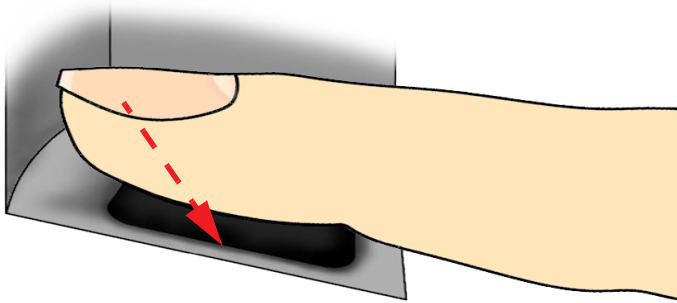
Problem	Solution
Finger is too dry or dirty	Rub the finger in the palm of your hand to moisten/clean it
Finger applied too lightly	Place finger firmly and flat onto the sensor surface
Finger positioned incorrectly	Your finger should cover most of the sensor window
Finger removed or moved during the scan 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

B.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 C

C 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 its local device database. If the presented finger matches the biometric templates retrieved 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> <p>Card or Finger: The RB25F is waiting for either a Credential (Card) to be presented or a finger, stored in its local device database, to be presented. This authentication mode is particularly useful during initial enrollment setup.</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.

Term	Definition
Identification (of Identity)	Typically finding a matching template in a large database of templates. 1:N matching.
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.
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 12 inches (30 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 6 feet (2 meters).
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.

Revision History

Date	Description	Revision
August 2019	Documentation updates relating to Service Pack 1 (RB25F Reader Firmware Version 1.5.0.82 and HID Biometric Manager Software Version 1.0.774.56514): <ul style="list-style-type: none">■ <i>Section 1.3 Related material</i>. New section added.■ <i>Section 1.4 Physical Access Control System overview</i>. Updated system diagram.■ <i>Section 3.2.5 Create Biometric Manager operators</i>. Updated section for new operator role.■ <i>Section 3.4.1 Configure device settings</i>. Updated section for BLE Mobile Access setting and Configure Mobile Identity Key functionality.■ <i>Section 3.4.2 Device firmware update</i>. New section added.■ <i>Section 3.7 System monitoring and Reports</i>. New restructured section to cover event filtering and Transaction reports.■ <i>Appendix A - Biometric Manager Mobile Access setup</i>. New appendix added.	A.2
June 2019	Updates implemented: <ul style="list-style-type: none">■ <i>Section 3.2.1 HID Biometric Manager software install</i>. Updated procedure.	A.1
February 2019	Initial release.	A.0

