HID® Biometric Manager™

Administration Guide

Software Version 1.0.1103.59811, Service Pack 2.2

PLT-04029, A.4
June 2020

Powering
Trusted Identities

Copyright

© 2019-2020 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, iCLASS SE, Seos, HID Mobile Access, HID Reader Manager, HID Elite, HID Origo and HID Biometric Manager 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.

Contacts

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

Americas and Corporate	**Asia Pacific**
611 Center Ridge Drive Austin, TX 78753 USA Phone: +1 866 607 7339	19/F 625 King's Road North Point, Island East Hong Kong Phone: +852 3160 9833
Europe, Middle East and Africa (EMEA)	**Brazil**
3 Cae Gwyrdd Green Meadow Springs Cardiff CF15 7AB United Kingdom Phone: +44 (0) 2920 528 500	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**.

What's new

Date	Description	Revision
June 2020	Updates to support HID Biometric Manager Service Pack 2.2 (RB25F Reader Firmware Version 1.5.1.22 and HID Biometric Manager Software Version 1.0.1103.59811)	A.4

A complete list of revisions is available in **Revision history**

Introduction ... 5

1.1 Document purpose ... 6

1.2 Intended audience ... 6

1.3 Related material ... 6

1.4 Physical Access Control System overview ... 7

1.5 HID Biometric Manager ... 8

1.5.1 Credential Database ... 8

1.5.2 Data Import ... 8

1.5.3 Reader Service ... 8

1.6 Browser compatible device ... 8

1.7 RB25F ... 8

1.8 Panels and Door Controllers ... 9

1.9 Network setups examples ... 10

HID Biometric Manager overview ... 11

2.1 System requirements ... 12

2.2 TCP Port usage ... 12

2.3 HID Biometric Manager initial setup ... 13

2.3.1 HID Biometric Manager software install ... 13

2.3.2 HID Biometric Manager initial login ... 15

2.4 Resetting administration password ... 18

2.4.1 Configure time zone setting ... 19

2.5 Device installation and configuration ... 21

2.5.1 Configure device settings ... 23

2.5.2 Device firmware update ... 26

2.5.3 Reset a device ... 29

2.5.4 Uninstall a device ... 30

2.6 Enrollment ... 31

2.6.1 Enroll people ... 31

2.6.2 Enroll Cards ... 33

2.6.3 Enroll Biometrics ... 36

2.7 Load HID Elite keys ... 39

2.7.1 Create Biometric Manager operators ... 41

2.7.2 Configure software/firmware update settings ... 43

2.7.3 Setting static IP for HBM network ... 45

2.7.4 Setting static IP for a specific device ... 46

2.8 Enforce Seos read ... 47

2.9 Device profiles ... 48

2.9.1 Create a device profile ... 48

2.9.2 Edit a device profile 50
2.9.3 Delete a device profile 54
2.10 Device health indication 55
2.11 Device debug page 56
2.12 Tamper settings 58
2.13 Write fingerprint templates to a card 59
2.14 Backup and recovery 61
2.14.1 Generate recovery key 61
2.14.2 Backup procedure 62
2.14.3 Restore procedure 63
2.15 System monitoring and Reports 65
2.15.1 View Biometric Manager events 65
2.15.2 Transaction Reports 67
Biometric Manager Mobile Access setup 69
A.1 Setup prerequisites 70
A.1.1 HID Mobile Identities setup 70
A.1.2 HID Reader Manager setup 70
A.1.3 Mobile Access user setup 70
A.2 Validate a Reader Manager account in HID Biometric Manager 71
A.3 Test MOB keys are working correctly 73
Fingerprint template encryption 74
Acronyms and terminology 76

Section **01**

Introduction

Powering
Trusted Identities

1.1 Document purpose

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

For more information on the RB25F device, refer to *HID iCLASS SE® RB25F User Guide* (PLT-04900).

1.2 Intended audience

This document is intended for personnel performing the following roles:

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

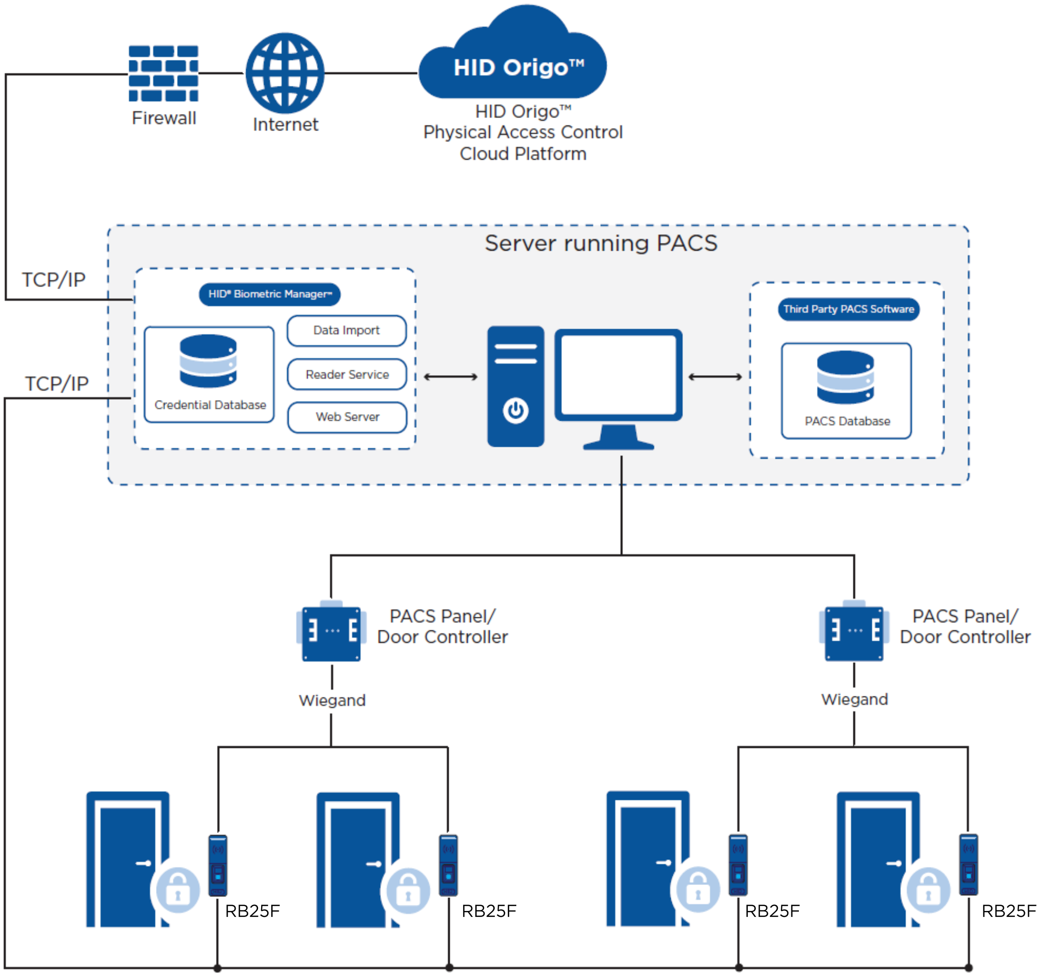
1.4 Physical Access Control System overview

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 they claim 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 you to configure RB25F device settings via a web browser, 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 **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.

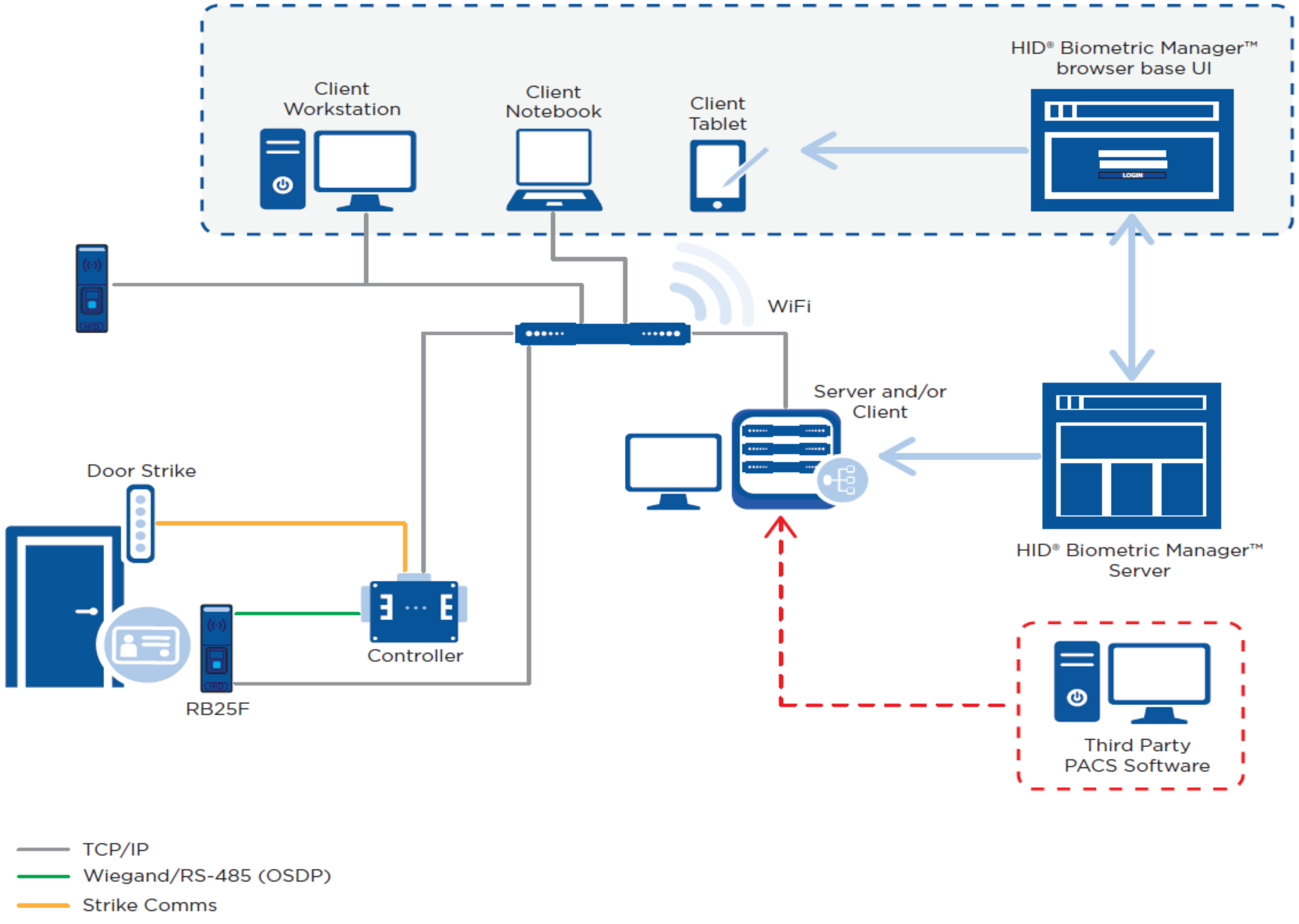
1.8 Panels and Door Controllers

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 setups 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 DCHP 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 DCHP 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.

Section **02**

HID Biometric Manager overview

Powering
Trusted Identities

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 **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 **Device installation and configuration** and enroll people in the system, add credentials, collect and store associated biometric data see **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 **Enrollment**.

2.1 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)

2.2 TCP Port usage

HID Biometric Manager TCP port usage:

- 883 Communication (MQTT Broker)
- 8883 Communication (MQTT Broker)
- 80 REST (Initial MQTT Configuration)
- 10500 Device discovery
- 22 (SSH) Firmware upgrade

2.3 HID Biometric Manager initial setup

2.3.1 HID Biometric Manager software install

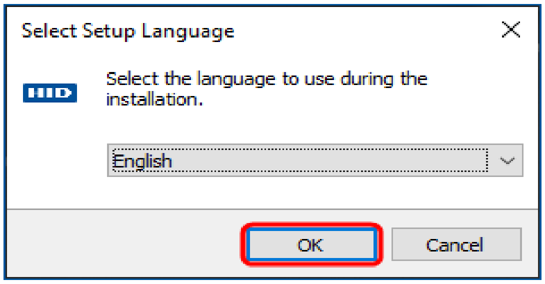
It is recommended that HID Biometric Manager is installed on a DHCP network server that automatically provides and assigns IP addresses, default gateways and other network parameters to client devices.

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

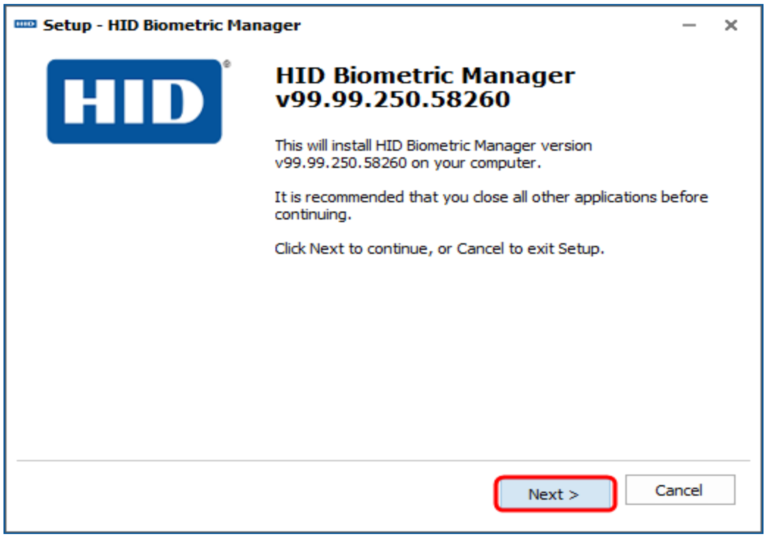
3. Select the HID Biometric language and click **OK**.


Select Setup Language

Select the language to use during the installation.

English

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


Setup - HID Biometric Manager

HID Biometric Manager
v99.99.250.58260

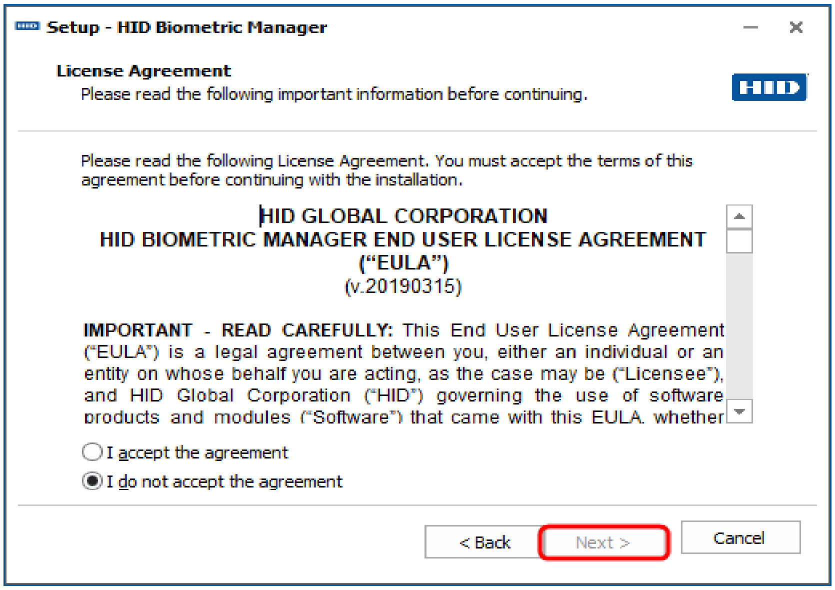
This will install HID Biometric Manager version v99.99.250.58260 on your computer.

It is recommended that you close all other applications before continuing.

Click Next to continue, or Cancel to exit Setup.

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.



License Agreement

Please read the following important information before continuing.

Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.

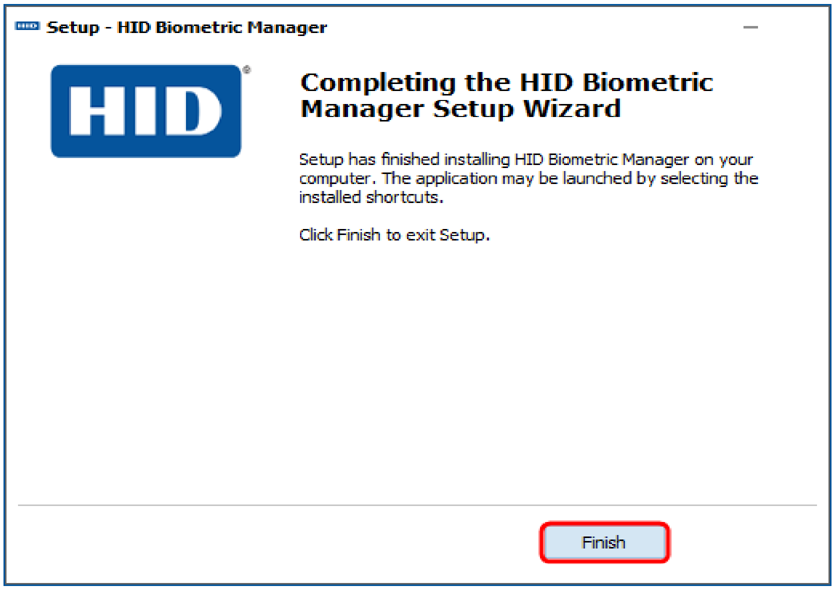
HID GLOBAL CORPORATION
HID BIOMETRIC MANAGER END USER LICENSE AGREEMENT
("EULA")
(v.20190315)

IMPORTANT - READ CAREFULLY: This End User License Agreement ("EULA") is a legal agreement between you, either an individual or an entity on whose behalf you are acting, as the case may be ("Licensee"), and HID Global Corporation ("HID") governing the use of software products and modules ("Software") that came with this EULA, whether

○ I accept the agreement

● I do not accept the agreement

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



Completing the HID Biometric Manager Setup Wizard

Setup has finished installing HID Biometric Manager on your computer. The application may be launched by selecting the installed shortcuts.

Click Finish to exit Setup.

2.3.2 HID Biometric Manager initial login

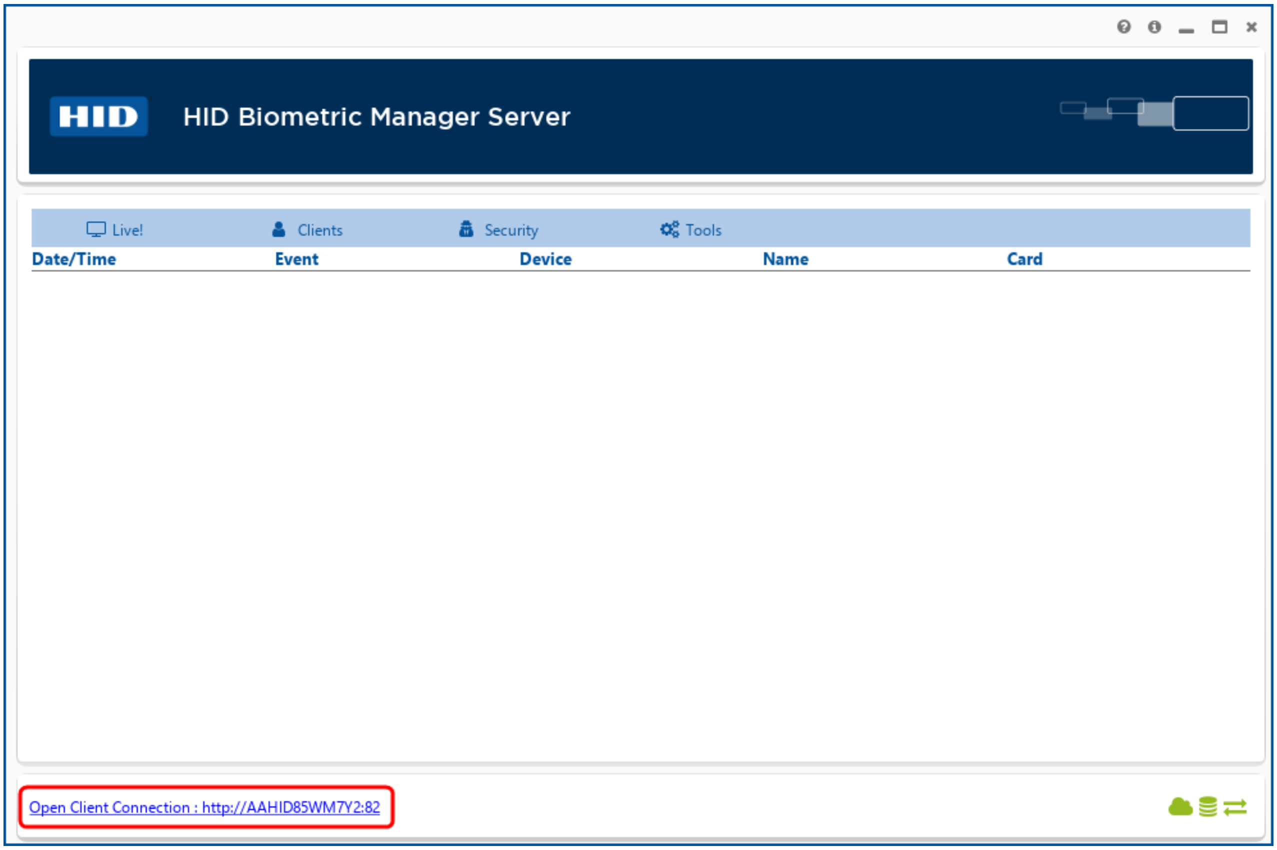
On the server where HID Biometric Manager has been installed:

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.

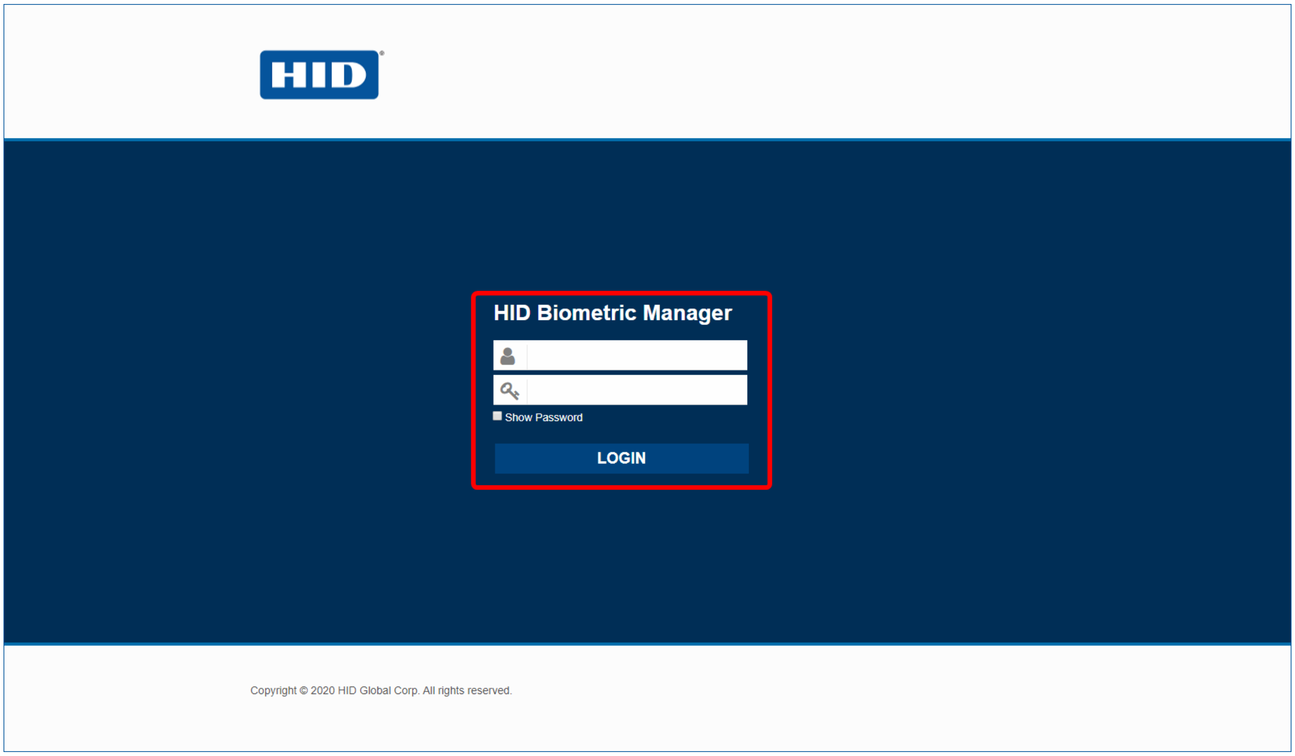
Note: The size of the database may impact how long it takes the Biometric Manager application to launch. Start up feedback is indicated with an on screen progress bar.

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.

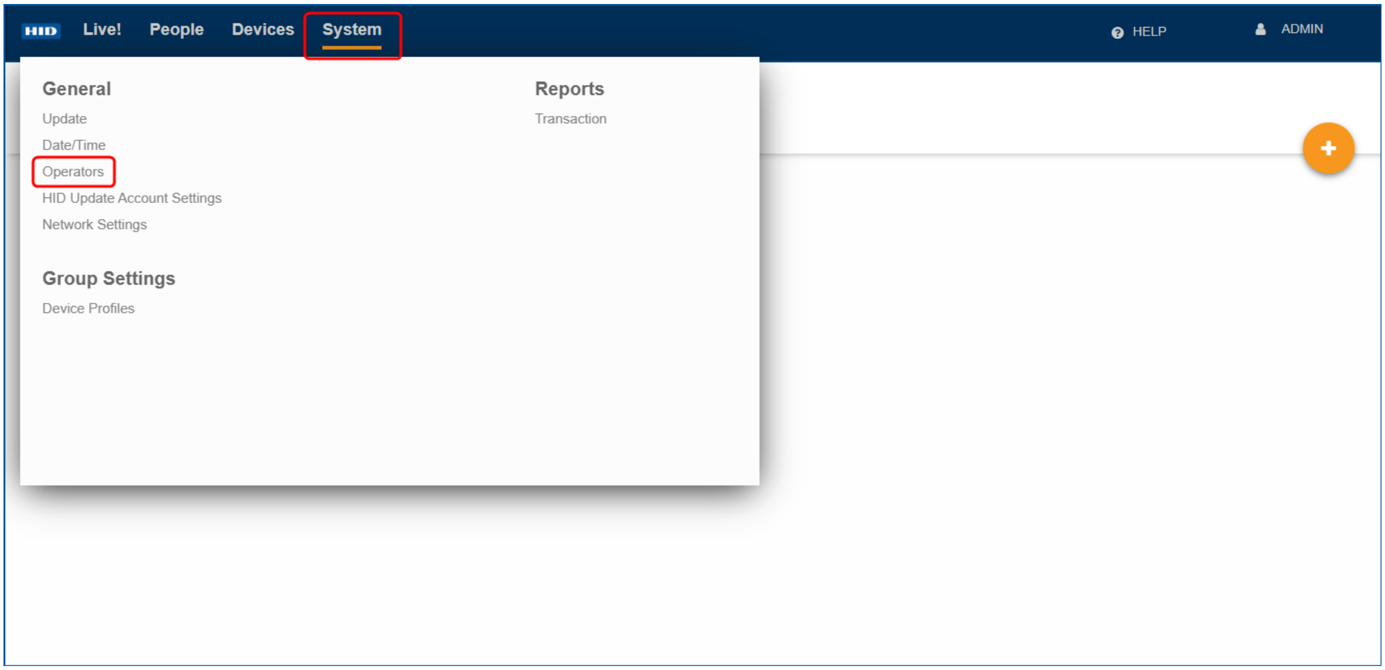
Note: If the **Open Client Connection** link url fails to connect to HID Biometric Manager due to a port issue, change the default port number (443) in the link url to: **http://hostname:82/HIDBiometric/HIDBiometricManager.html**


HID
HID Biometric Manager Server
Live!
Clients
Security
Tools
Date/Time
Event
Device
Name
Card
Open Client Connection : http://AAHID85WM7Y2:82

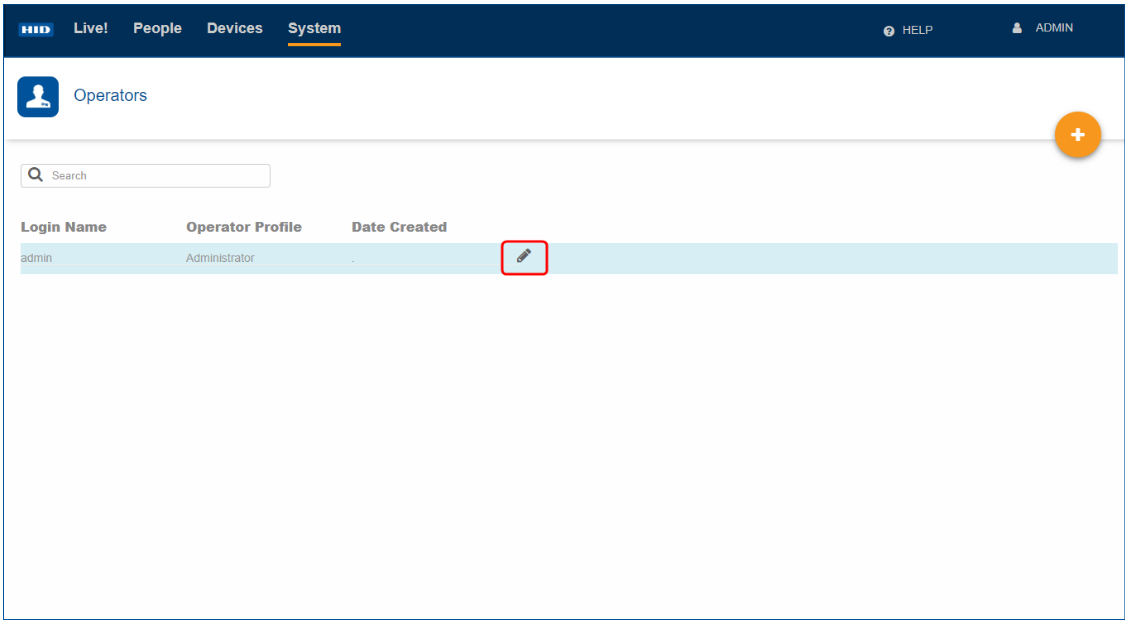
3. Enter the initial default admin User Name (**admin**) and Password (**password**) and click **LOGIN**.



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.

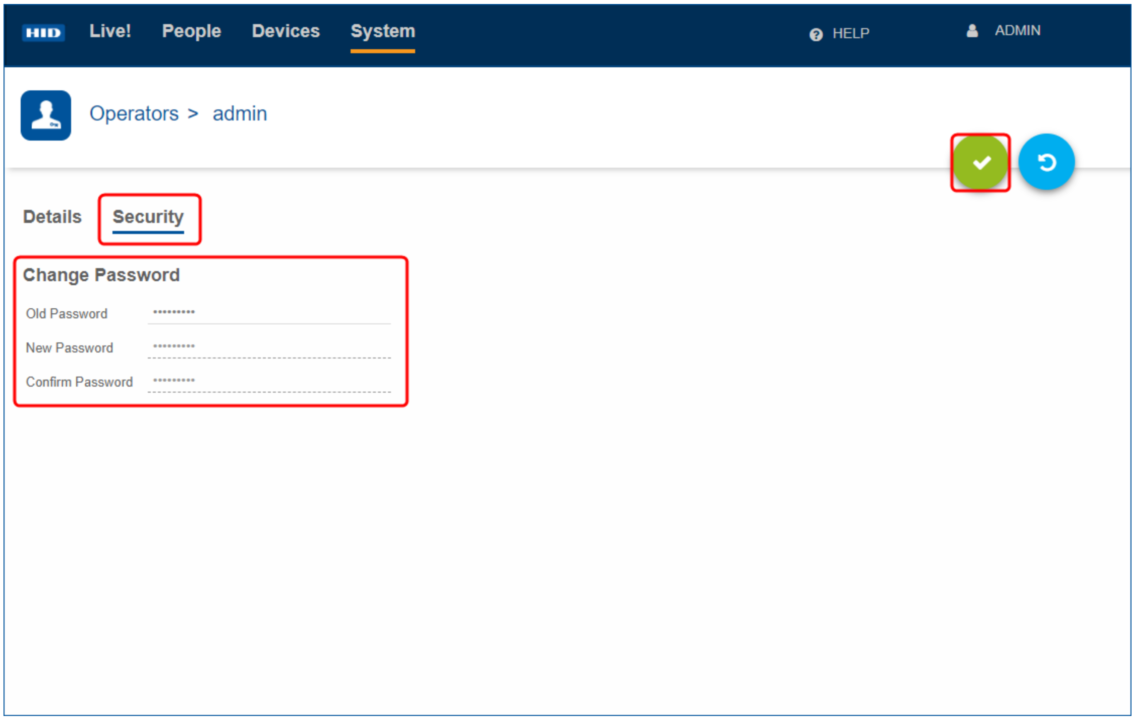


Login Name	Operator Profile	Date Created
admin	Administrator	-

6. Select the **Security** option 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.



Change Password

Old Password ••••••••••

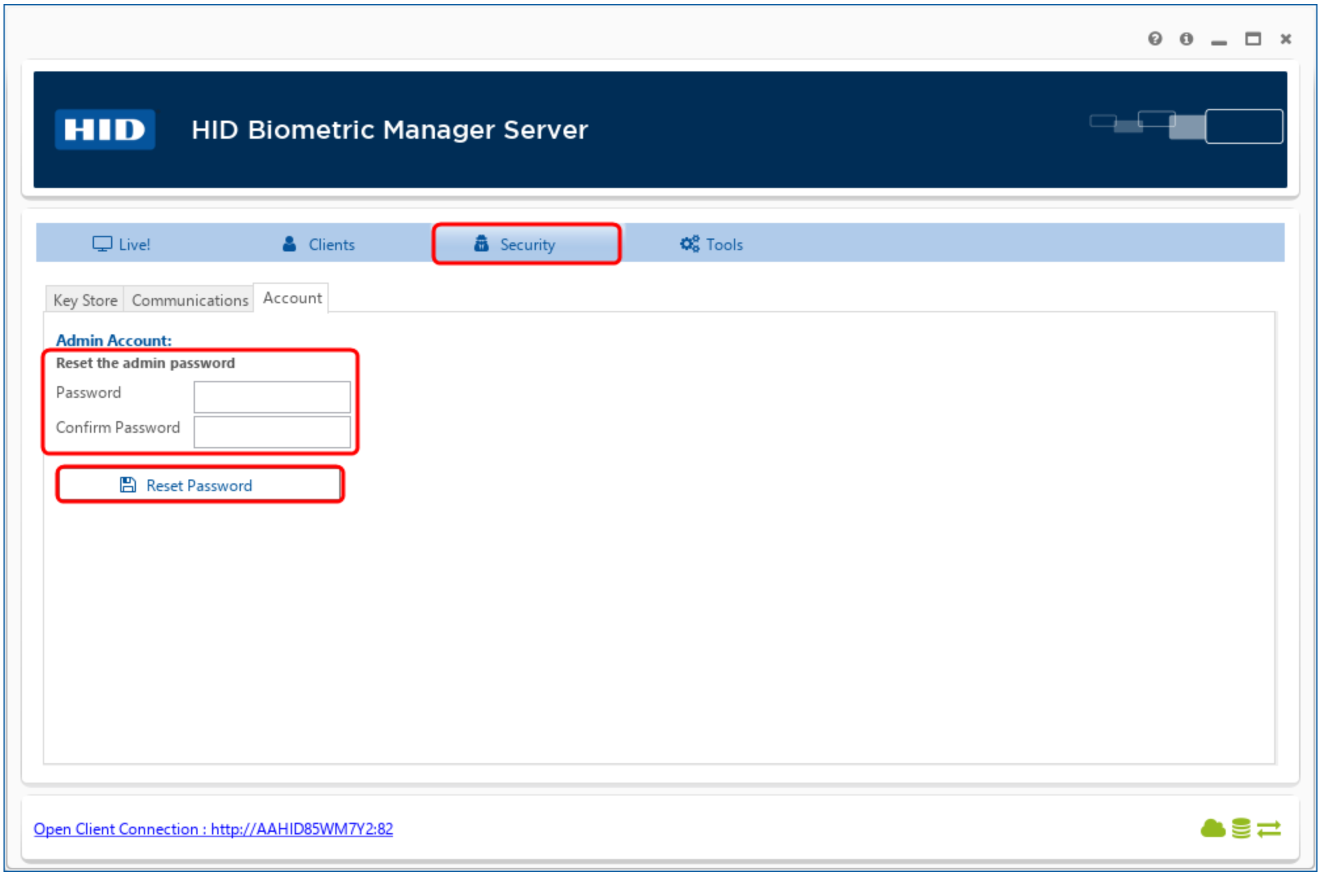
New Password ••••••••••

Confirm Password ••••••••••

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

2.4 Resetting administration password

Resetting the administrator password can be achieved in the **HID Biometric Manager Server** under **Security**>**Account** before log in.

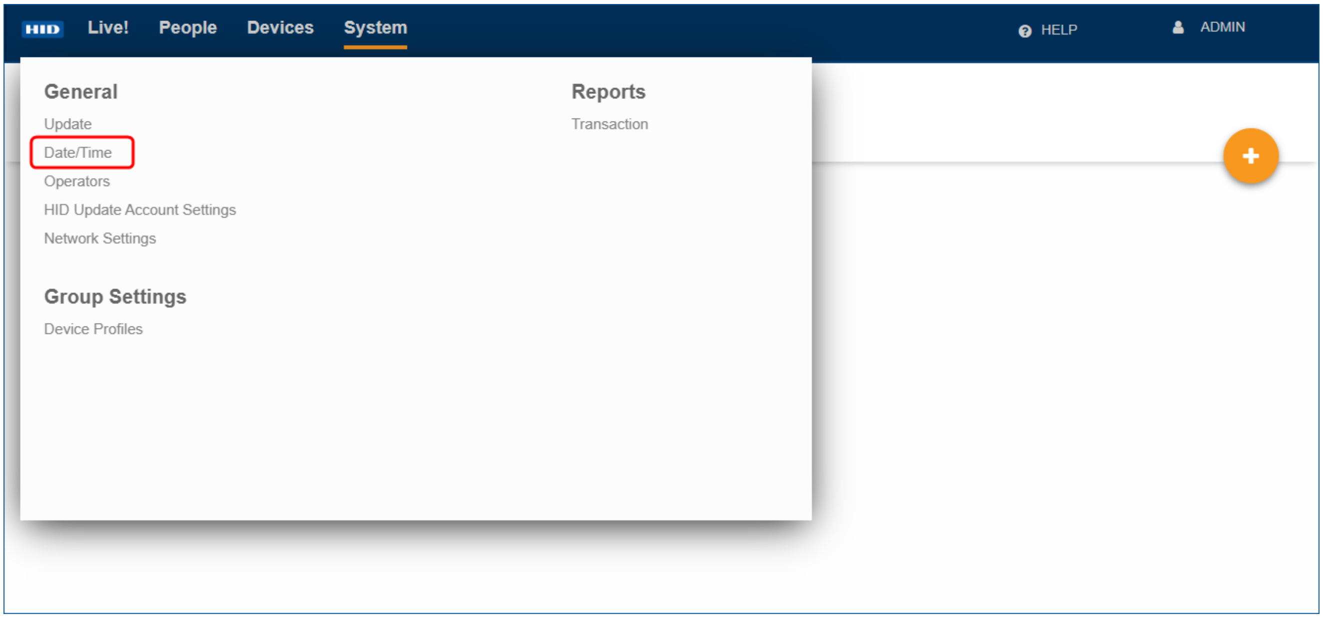


This method is used when the user cannot log in to change the administrator password as shown in **HID Biometric Manager initial login**

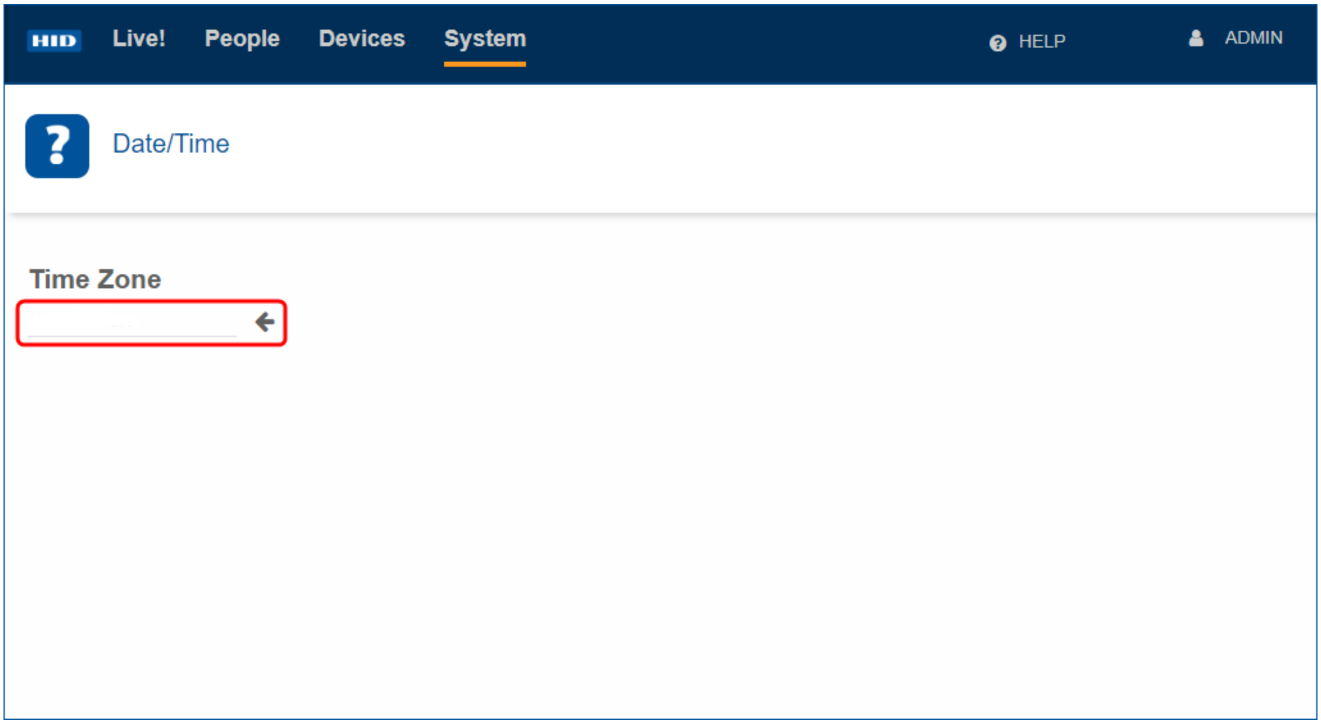
2.4.1 Configure time zone setting

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.

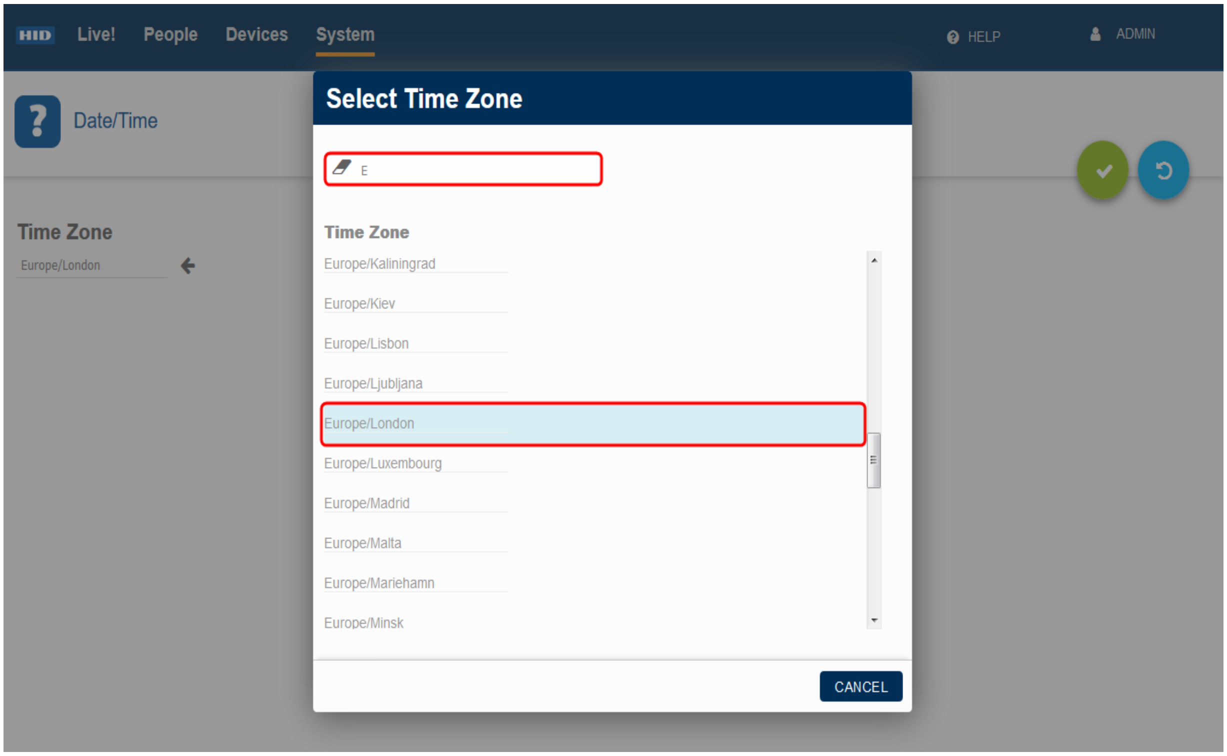


3. Select the **Time Zone** arrow icon to access a list of selectable time zones.



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.



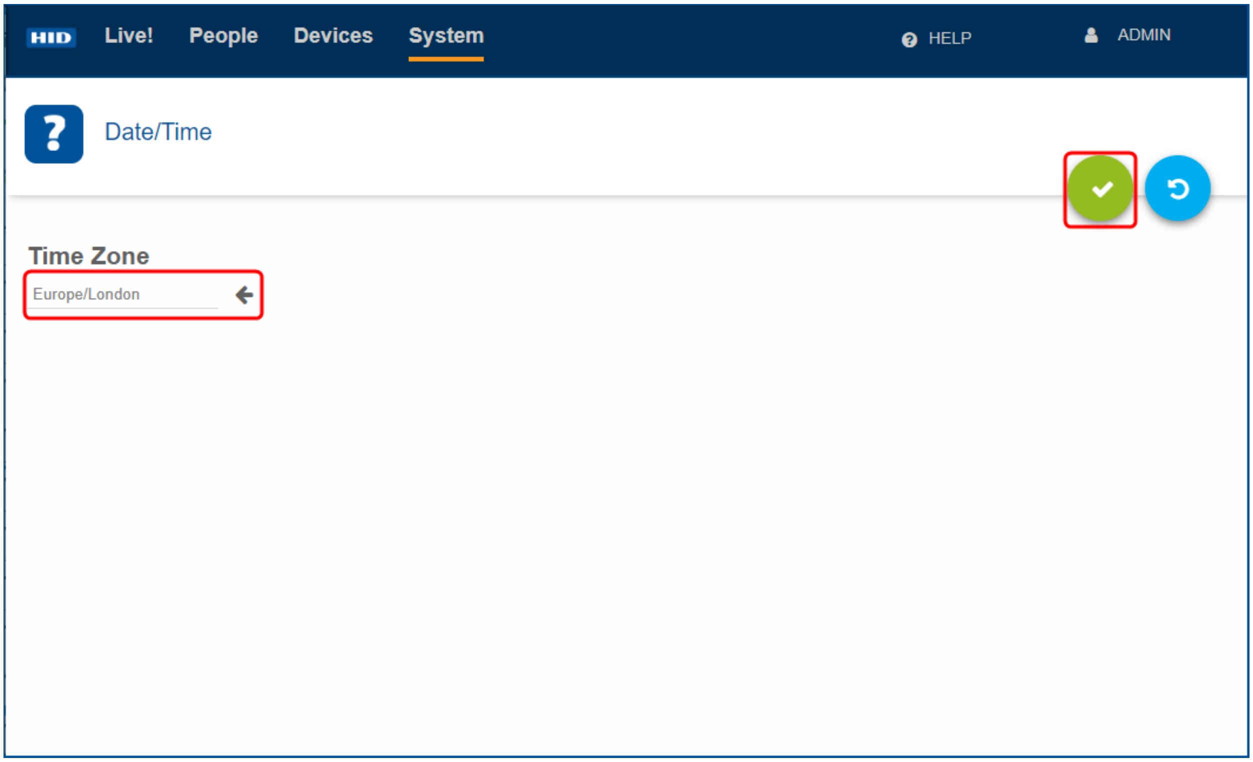
Time Zone
Europe/London

Select Time Zone

E

Time Zone
Europe/Kaliningrad
Europe/Kiev
Europe/Lisbon
Europe/Ljubljana
Europe/London
Europe/Luxembourg
Europe/Madrid
Europe/Malta
Europe/Mariehamn
Europe/Minsk

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



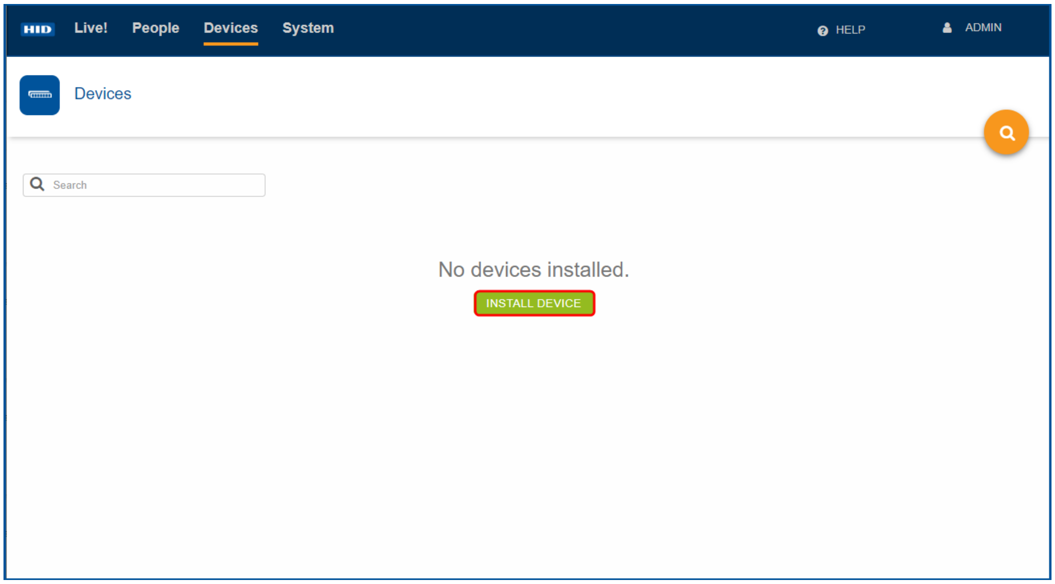
Time Zone
Europe/London

2.5 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 **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**.

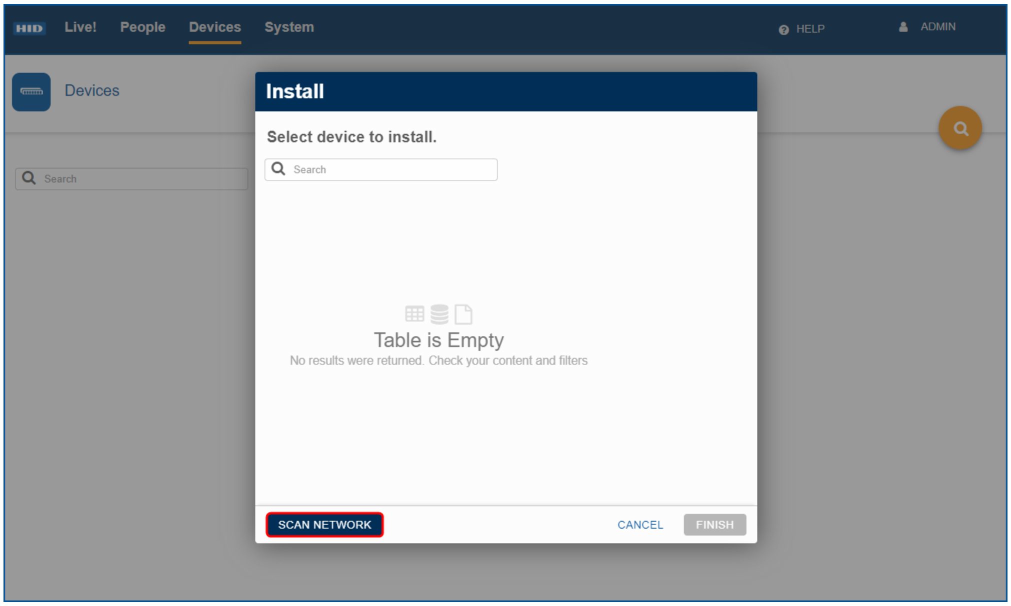
Note: If devices are already installed, to add additional devices click the Install icon [🔍].



No devices installed.

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 **TCP Port usage** are open. The **Search** function can be used to search the list of displayed devices.

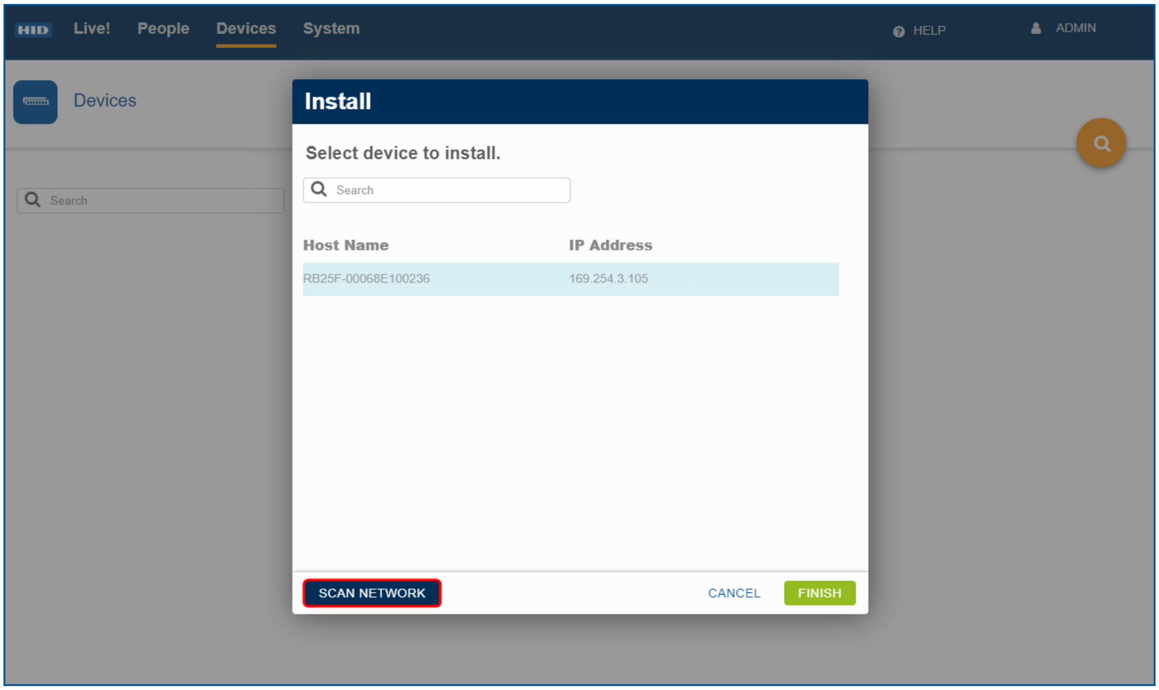


Select device to install.

Table is Empty

No results were returned. Check your content and filters

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



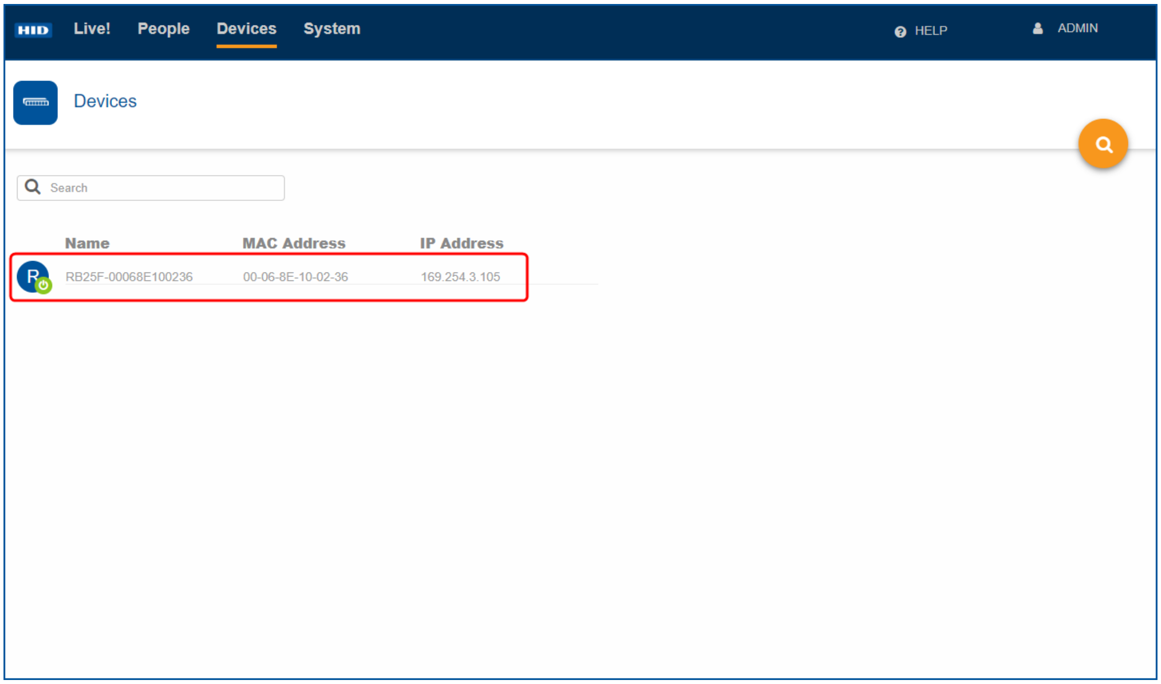
Install

Select device to install.

Host Name	IP Address
RB25F-00068E100236	169.254.3.105

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

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



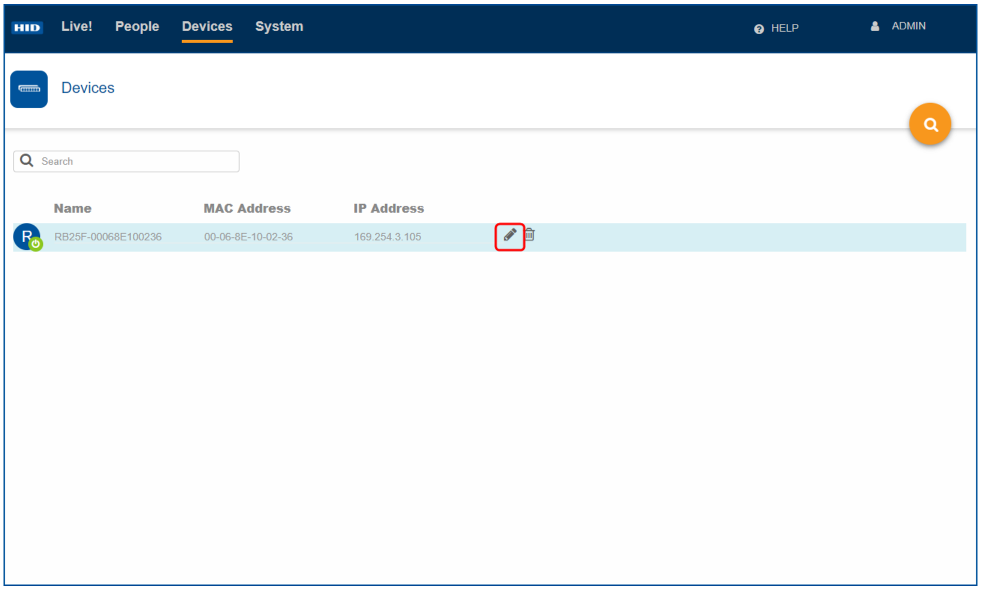
Name	MAC Address	IP Address
RB25F-00068E100236	00-06-8E-10-02-36	169.254.3.105

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

2.5.1 Configure device settings

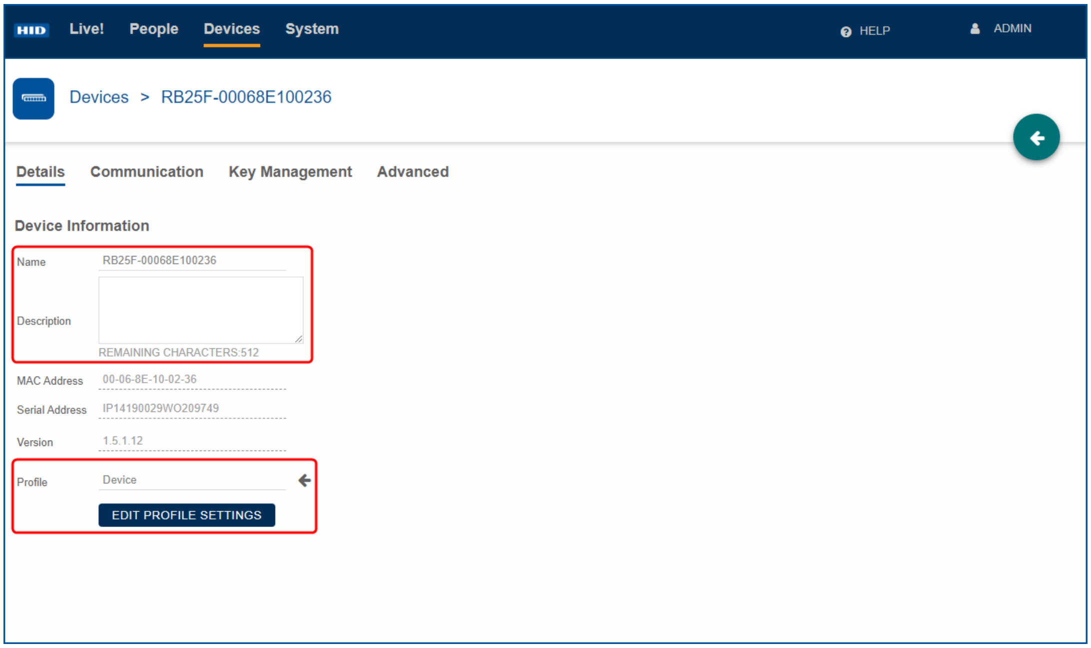
To access and configure settings associated with an installed device:

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.



Name	MAC Address	IP Address
RB25F-00068E100236	00-06-8E-10-02-36	169.254.3.105

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 **Edit a device profile**.



Device Information

Name: RB25F-00068E100236

Description:

REMAINING CHARACTERS:512

MAC Address: 00-06-8E-10-02-36

Serial Address: IP14190029WO209749

Version: 1.5.1.12

Profile: Device

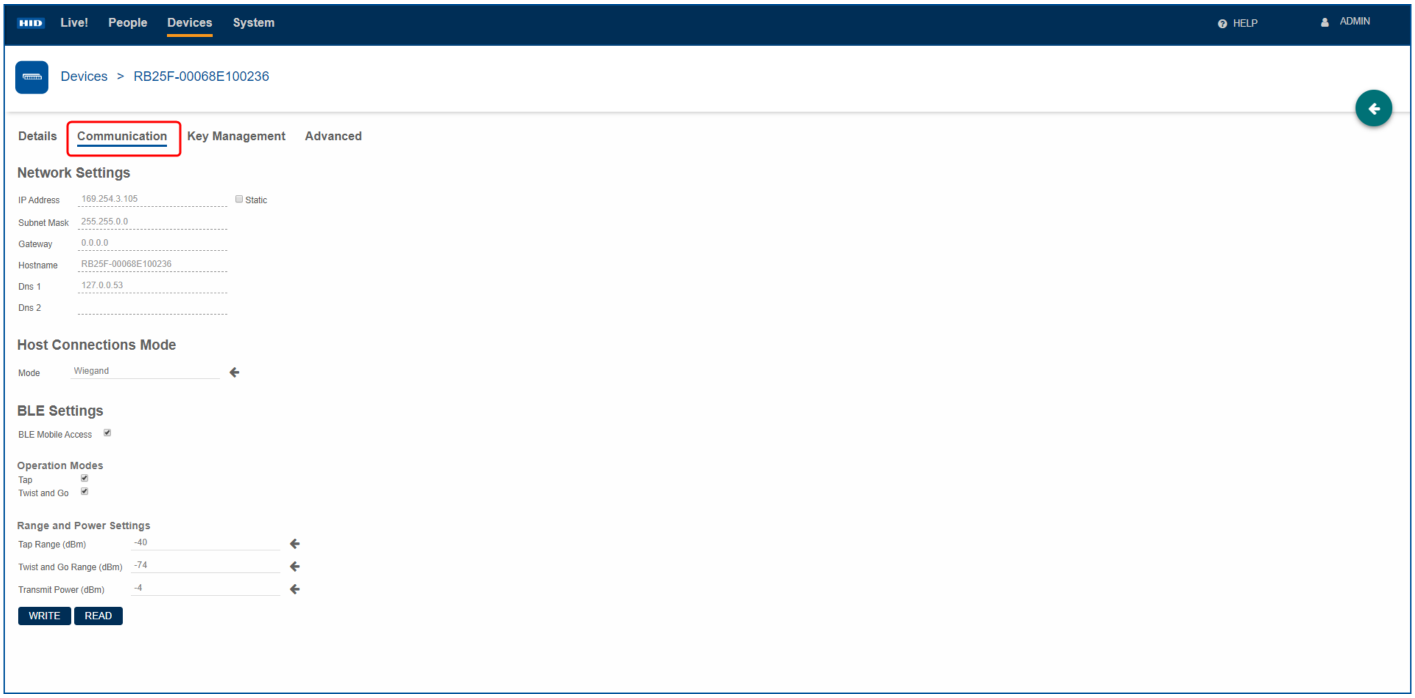
5. On the **Devices** screen, select **Communication**.
6. On the **Communication** screen you can configure:
   - **Network Settings:** To use a static IP address select the **Static** option. Enter a static IP address (IPv4) and also the Subnet Mask and Gateway.
   - **Host Connections Mode:** Set 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 [✓].



Devices > RB25F-00068E100236

Network Settings

IP Address 169.254.3.105 □ Static
Subnet Mask 255.255.0.0
Gateway 0.0.0.0
Hostname RB25F-00068E100236
Dns 1 127.0.0.53
Dns 2

Host Connections Mode

Mode Wiegand

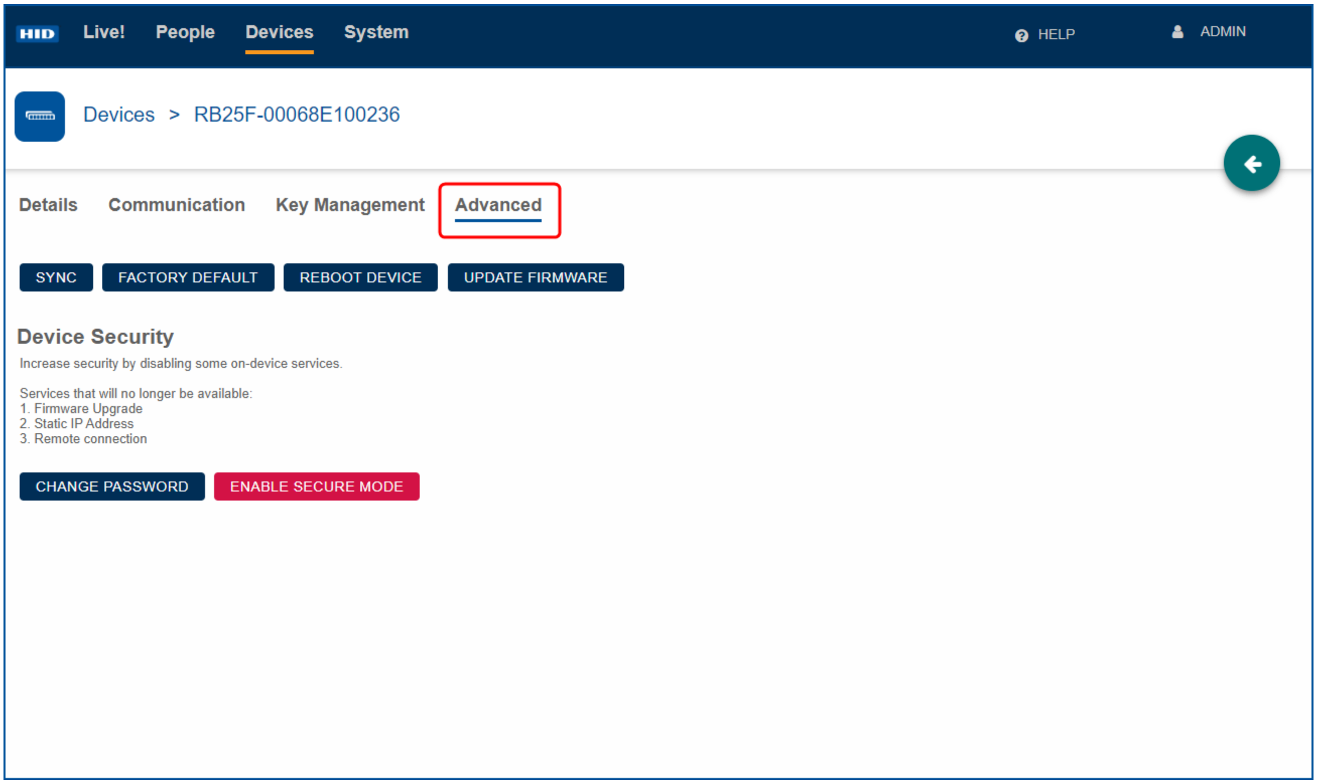
BLE Settings

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

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 **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:** This turns on encryption in the communication channel.
    - **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 written to the device, keys have to loaded onto HID Biometric Manager, see **Biometric Manager Mobile Access setup**.
9. Click **SYNC** option. For the selected device all settings are copied from HID Biometric Manager to the RB25F.



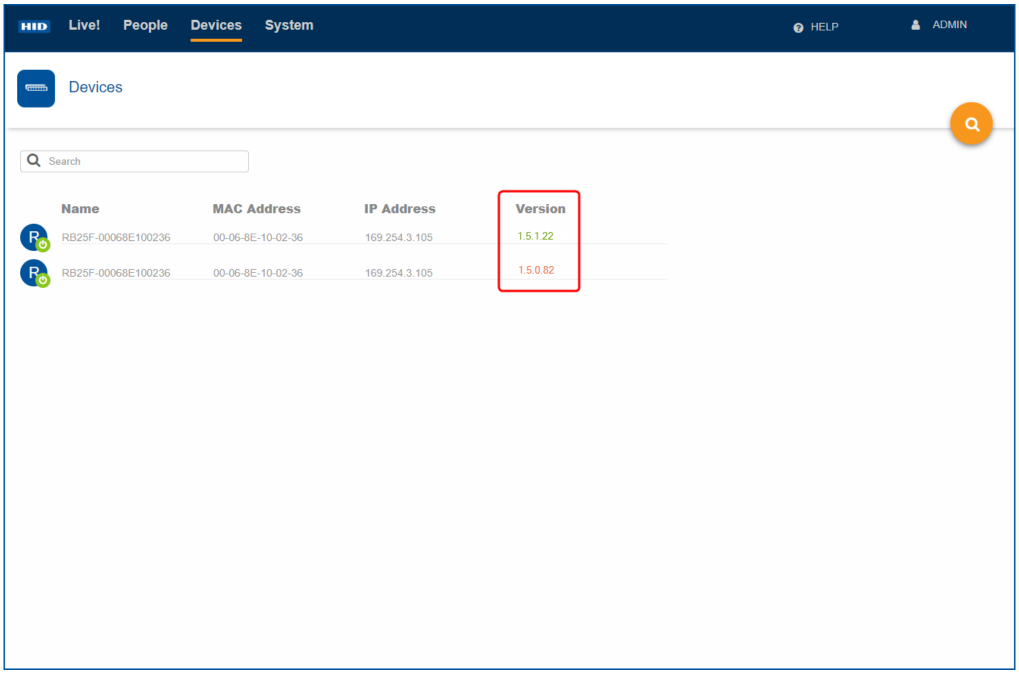
Device Security

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

2.5.2 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.



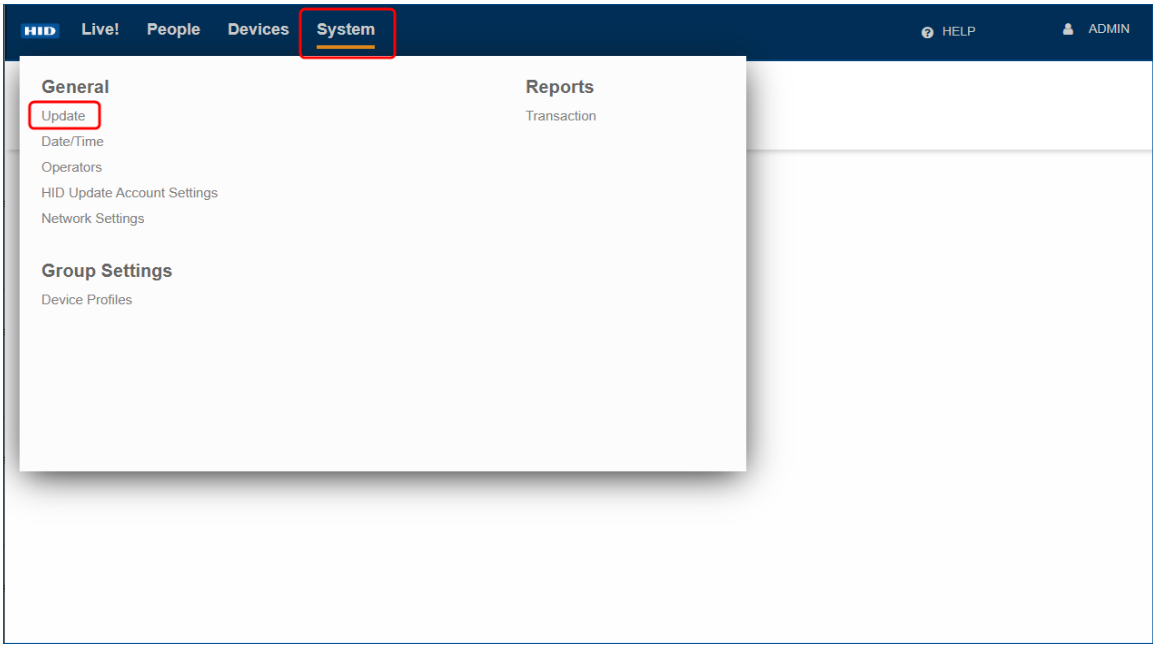
Name	MAC Address	IP Address	Version
RB25F-00068E100236	00-06-8E-10-02-36	169.254.3.105	1.5.1.22
RB25F-00068E100236	00-06-8E-10-02-36	169.254.3.105	1.5.0.82

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.

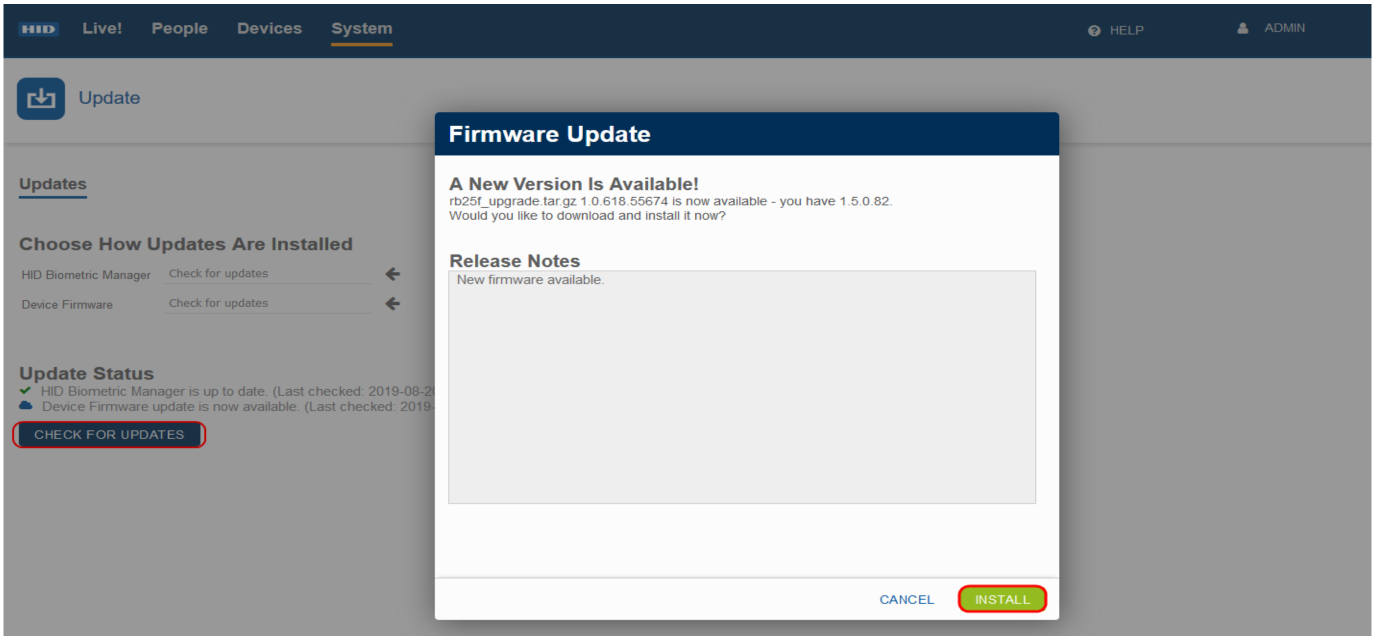
Important: It is recommended that device firmware updates should be carefully scheduled as all devices are updated and will be unavailable for use during the firmware update period.

To update device firmware:

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



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



HID Biometric Manager is up to date. (Last checked: 2019-08-2

Device Firmware update is now available. (Last checked: 2019-

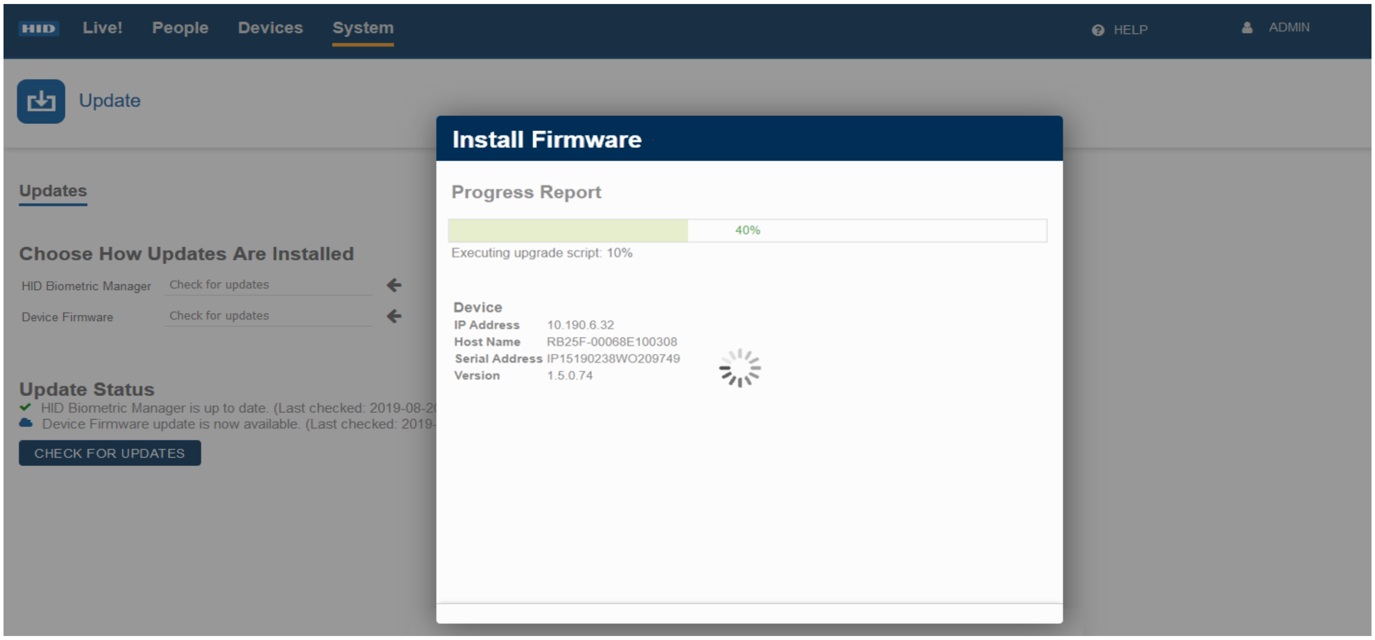
A New Version Is Available!

rb25f_upgrade.tar.gz 1.0.618.55674 is now available - you have 1.5.0.82.
Would you like to download and install it now?

New firmware available.

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.



HID Biometric Manager is up to date. (Last checked: 2019-08-2

Device Firmware update is now available. (Last checked: 2019-

Executing upgrade script: 10%

Device

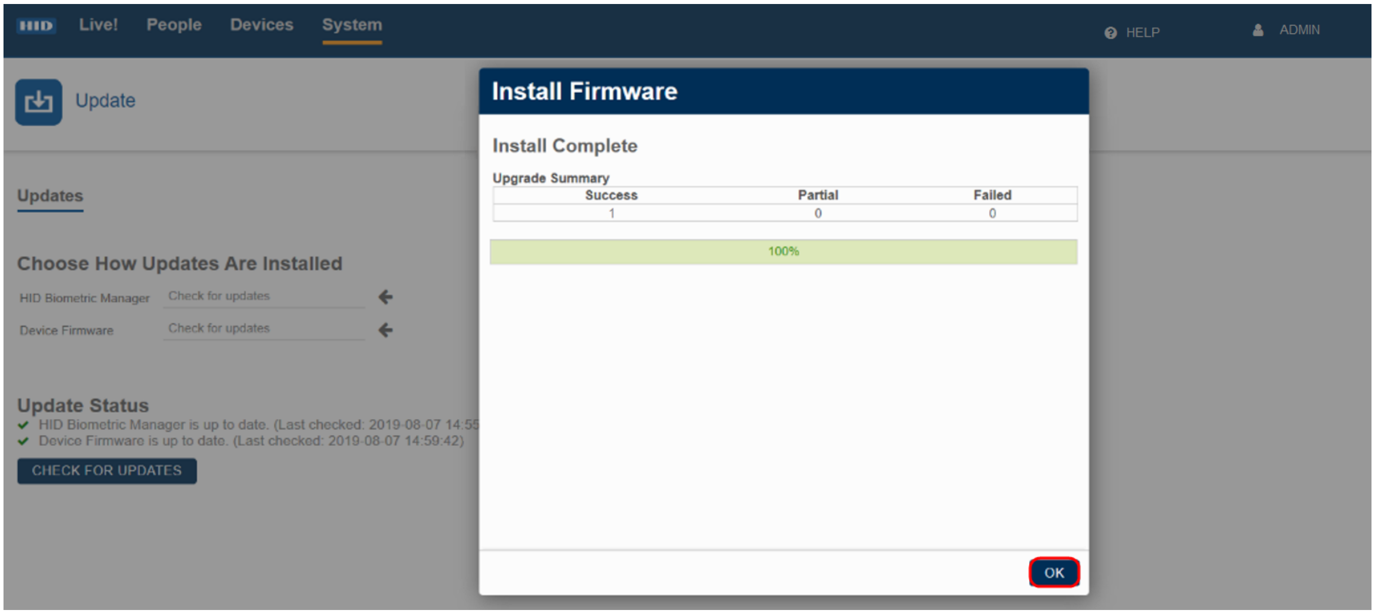
IP Address	10.190.6.32
Host Name	RB25F-00068E100308
Serial Address	IP15190238WO209749
Version	1.5.0.74

3. 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 **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.



Choose How Updates Are Installed

HID Biometric Manager	Check for updates
Device Firmware	Check for updates

Update Status

✓ HID Biometric Manager is up to date. (Last checked: 2019-08-07 14:55

✓ Device Firmware is up to date. (Last checked: 2019-08-07 14:59:42)

CHECK FOR UPDATES

Install Firmware

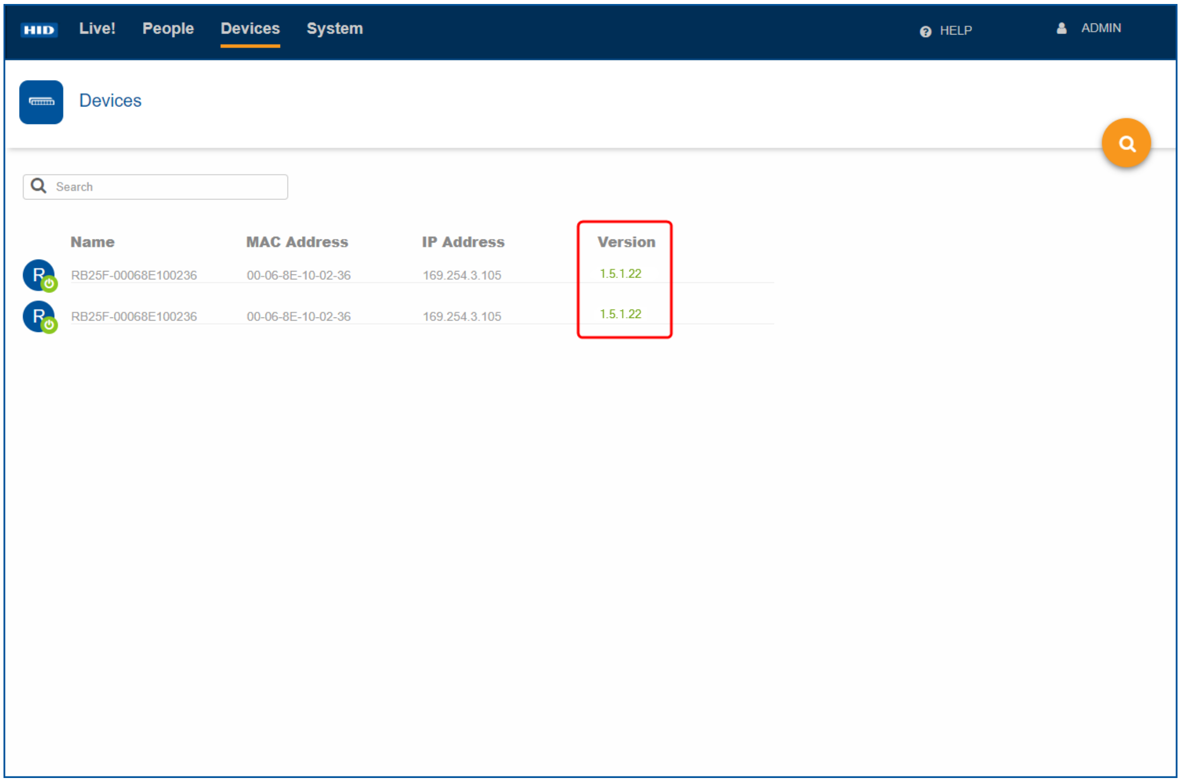
Install Complete

Upgrade Summary

Success	Partial	Failed
1	0	0

100%

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

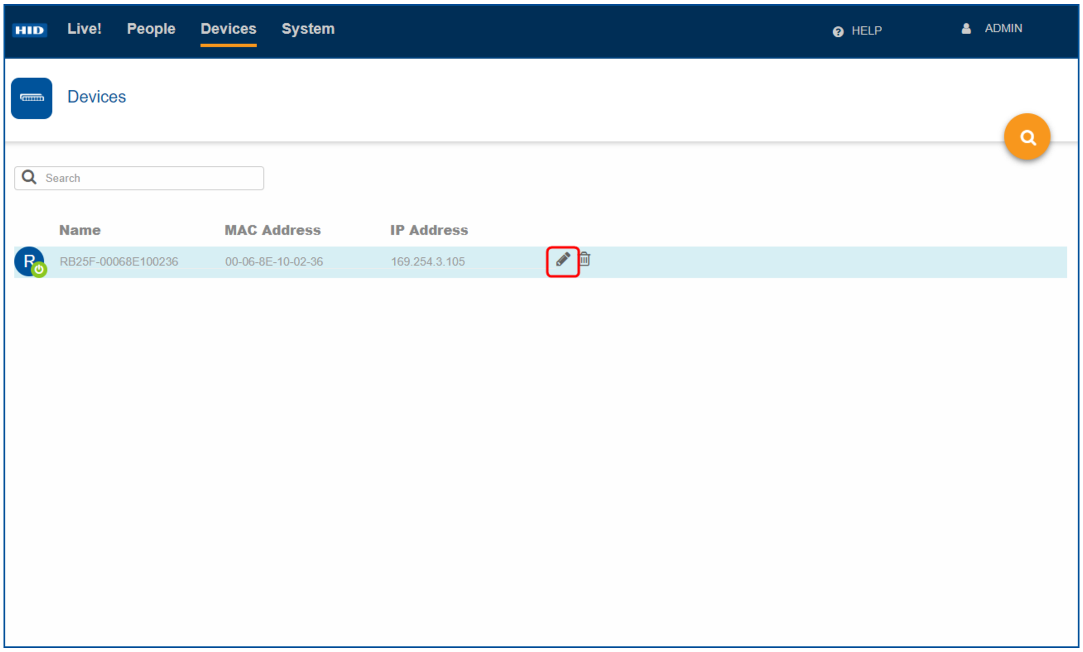


Name	MAC Address	IP Address	Version
RB25F-00068E100236	00-06-8E-10-02-36	169.254.3.105	1.5.1.22
RB25F-00068E100236	00-06-8E-10-02-36	169.254.3.105	1.5.1.22

2.5.3 Reset a device

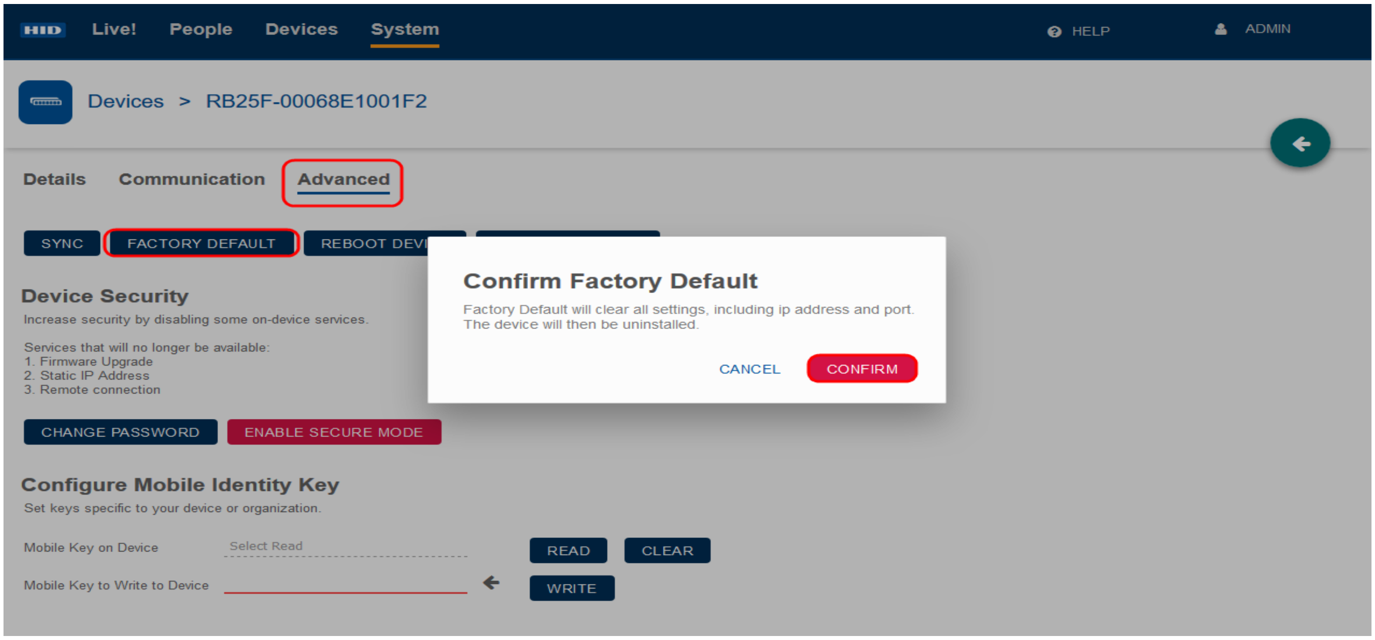
To clear all device settings, including IP address and port:

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.



Name	MAC Address	IP Address
RB25F-00068E100236	00-06-8E-10-02-36	169.254.3.105

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



Device Security

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

Configure Mobile Identity Key

Set keys specific to your device or organization.

Mobile Key on Device: Select Read

Mobile Key to Write to Device:

Confirm Factory Default

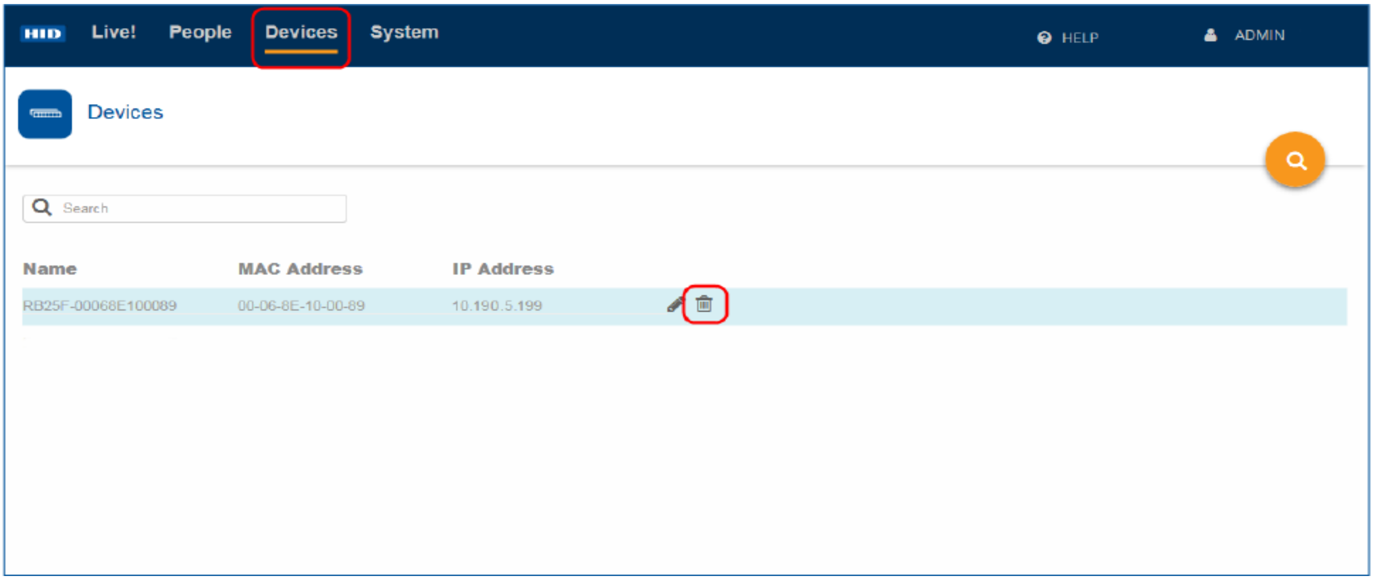
Factory Default will clear all settings, including ip address and port. The device will then be uninstalled.

Note: Where communication between HID Biometric Manager and the RB25F is not possible, factory default reset can be carried out at the reader, see *HID iCLASS SE RB25F User Guide* (PLT-04900).

2.5.4 Uninstall a device

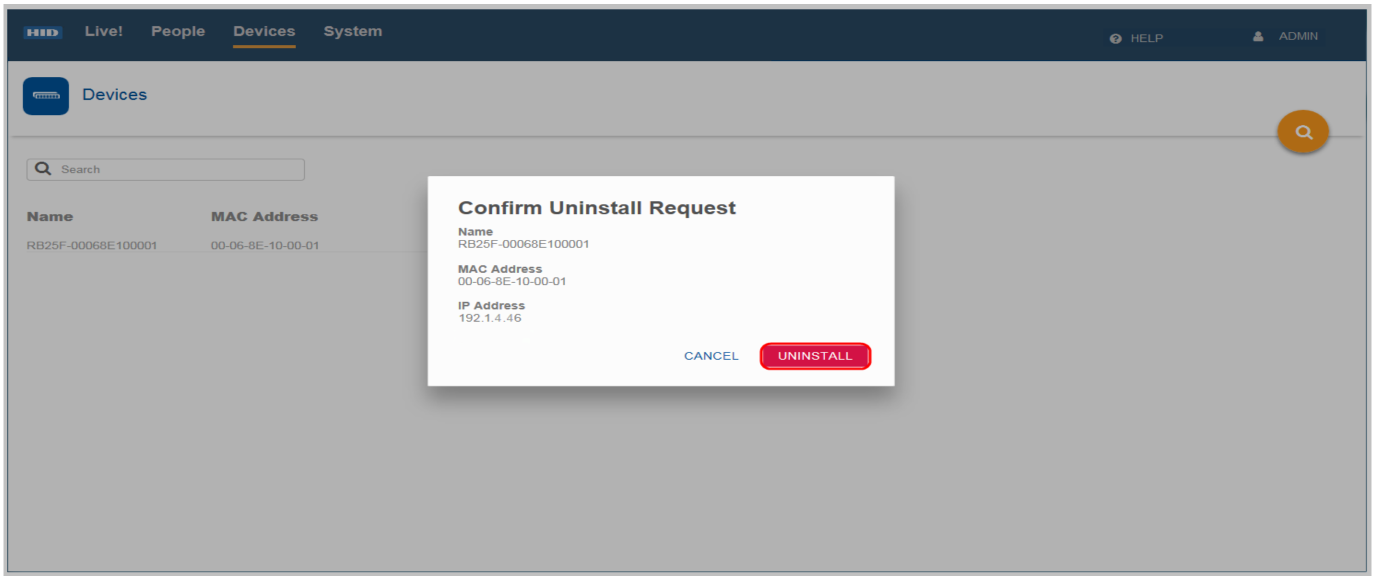
To uninstall a device (possibly as a means to resolving issues by removing the device from the database, power cycling, then re-installing the device):

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.



Name	MAC Address	IP Address
RB25F-00068E100089	00-06-8E-10-00-89	10.190.5.199

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



Name	MAC Address
RB25F-00068E100001	00-06-8E-10-00-01

Confirm Uninstall Request

Name
RB25F-00068E100001

MAC Address
00-06-8E-10-00-01

IP Address
192.1.4.46

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 **Device installation and configuration**.

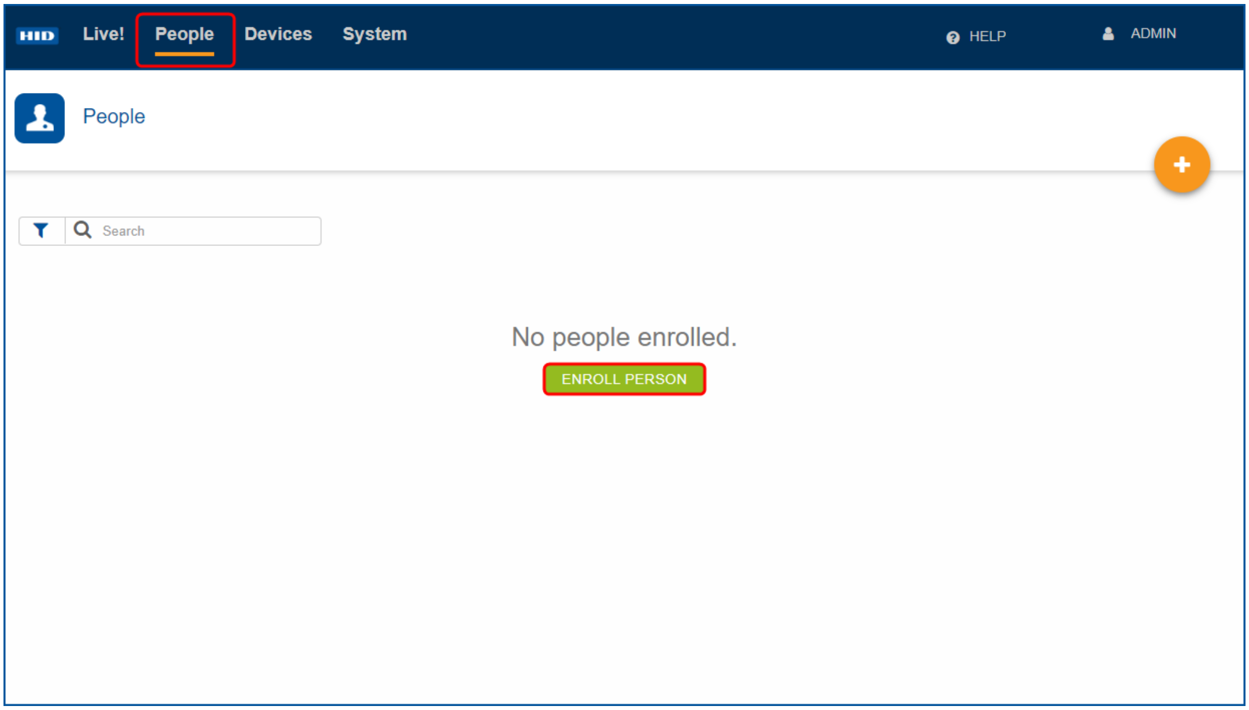
2.6 Enrollment

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

2.6.1 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, click the **Add** icon [+] to enroll additional people.

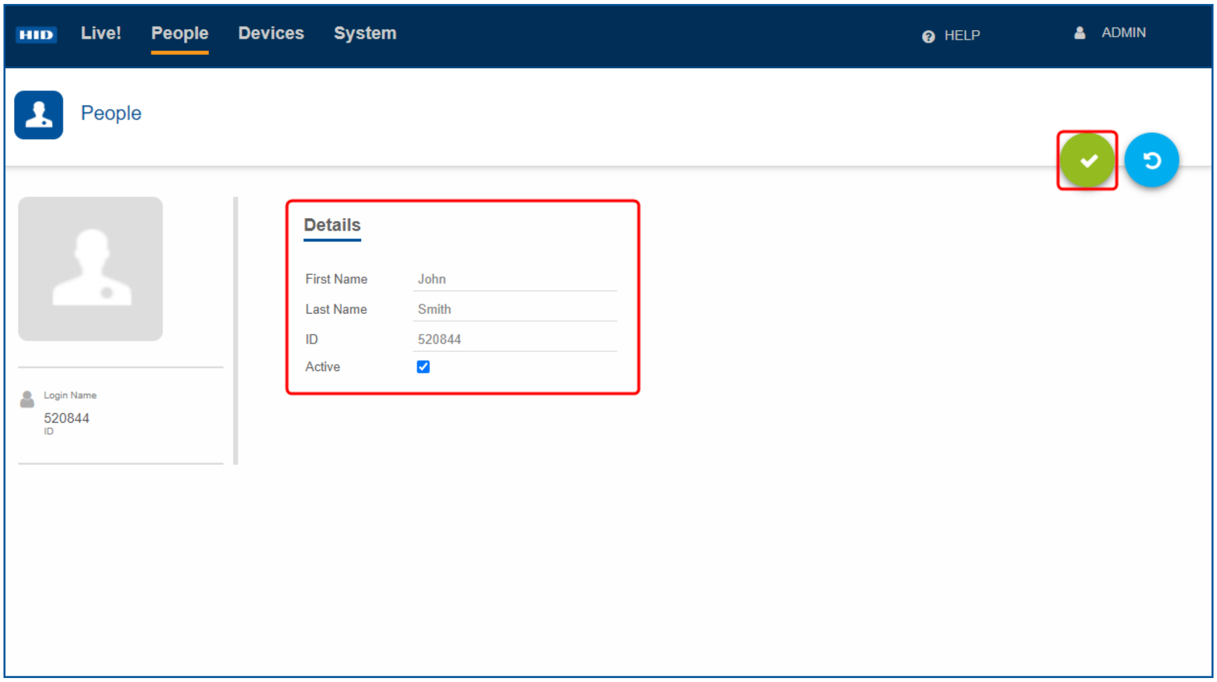


No people enrolled.

3. Enter the persons details (**First Name/Last Name**) and an **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's record is not displayed on the **People** screen.

5. Click the **Save** icon [✓].



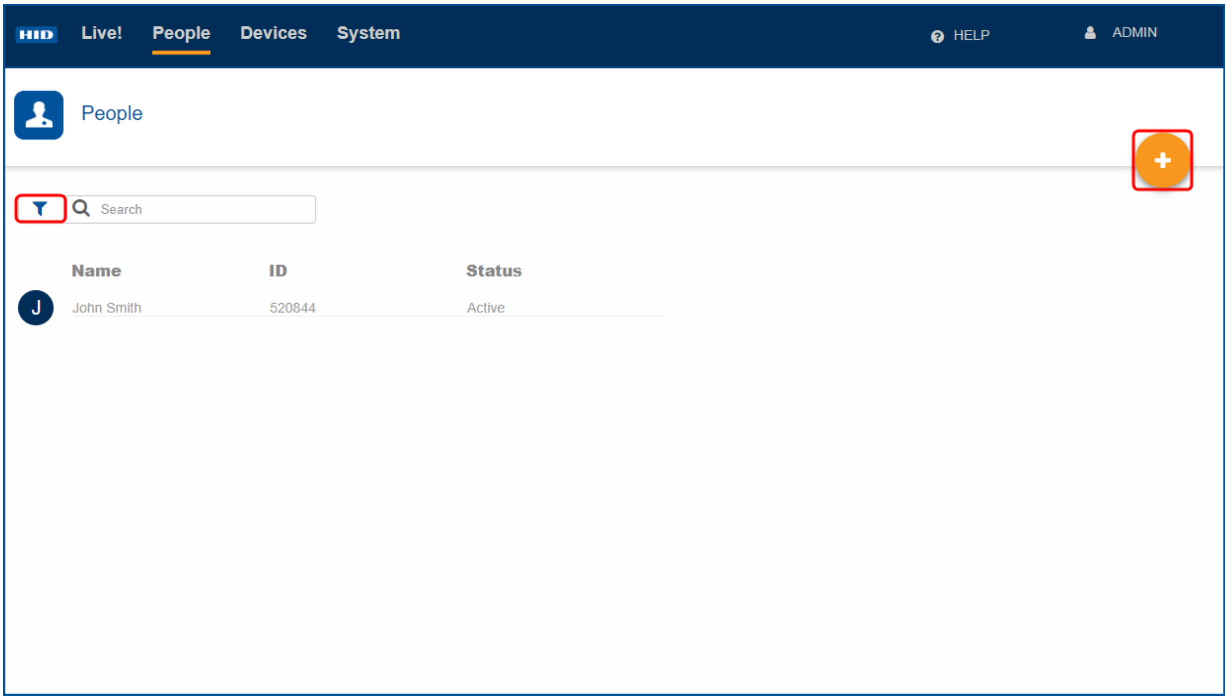
Details

First Name John
Last Name Smith
ID 520844
Active ☑

Login Name
520844
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.



	Name	ID	Status
J	John Smith	520844	Active

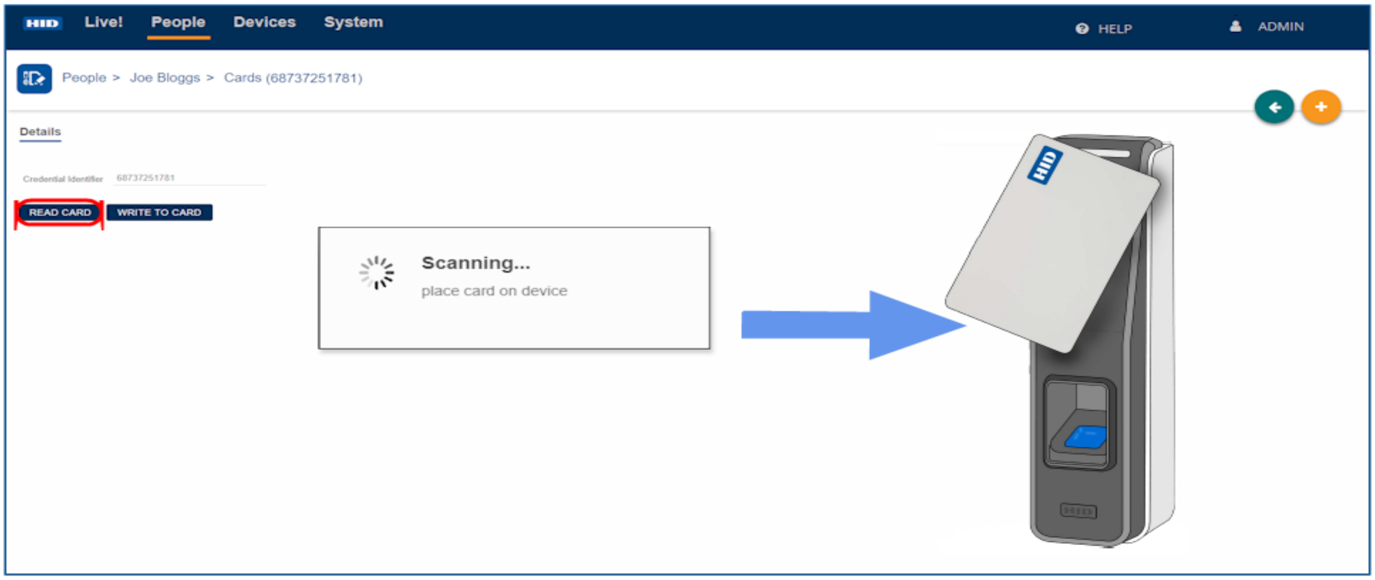
2.6.2 Enroll Cards

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

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 **Edit a device profile**.



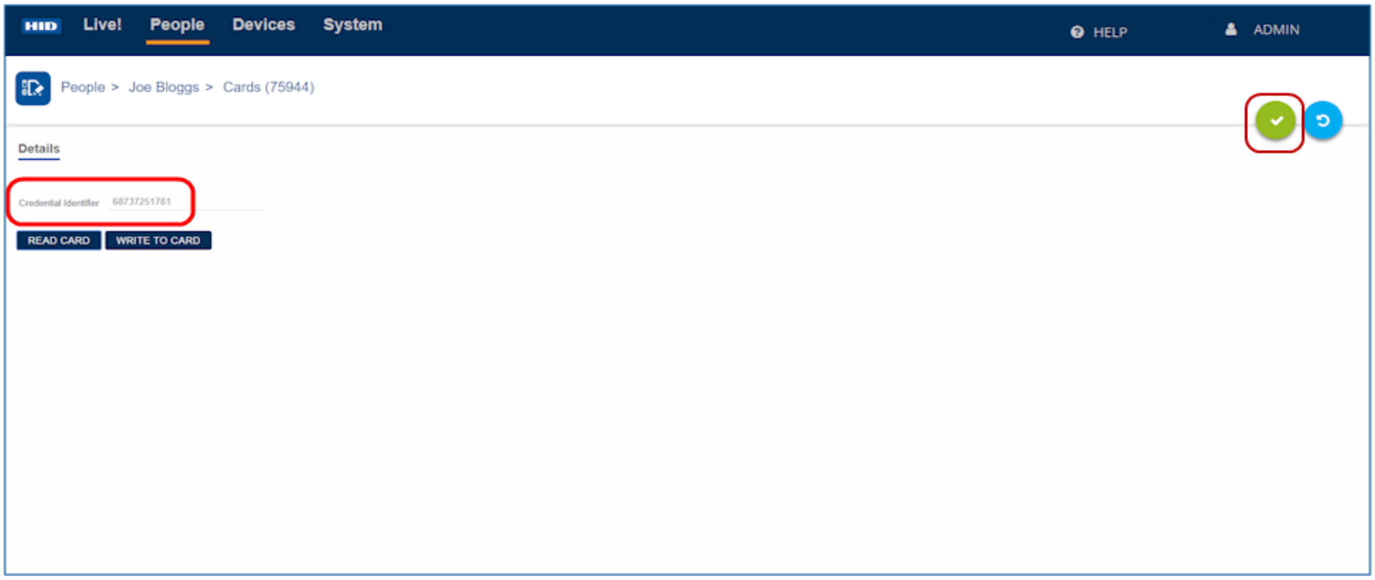
People > Joe Bloggs > Cards (68737251781)

Credential Identifier 68737251781

Scanning...
place card on device

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.



People > Joe Bloggs > Cards (75944)

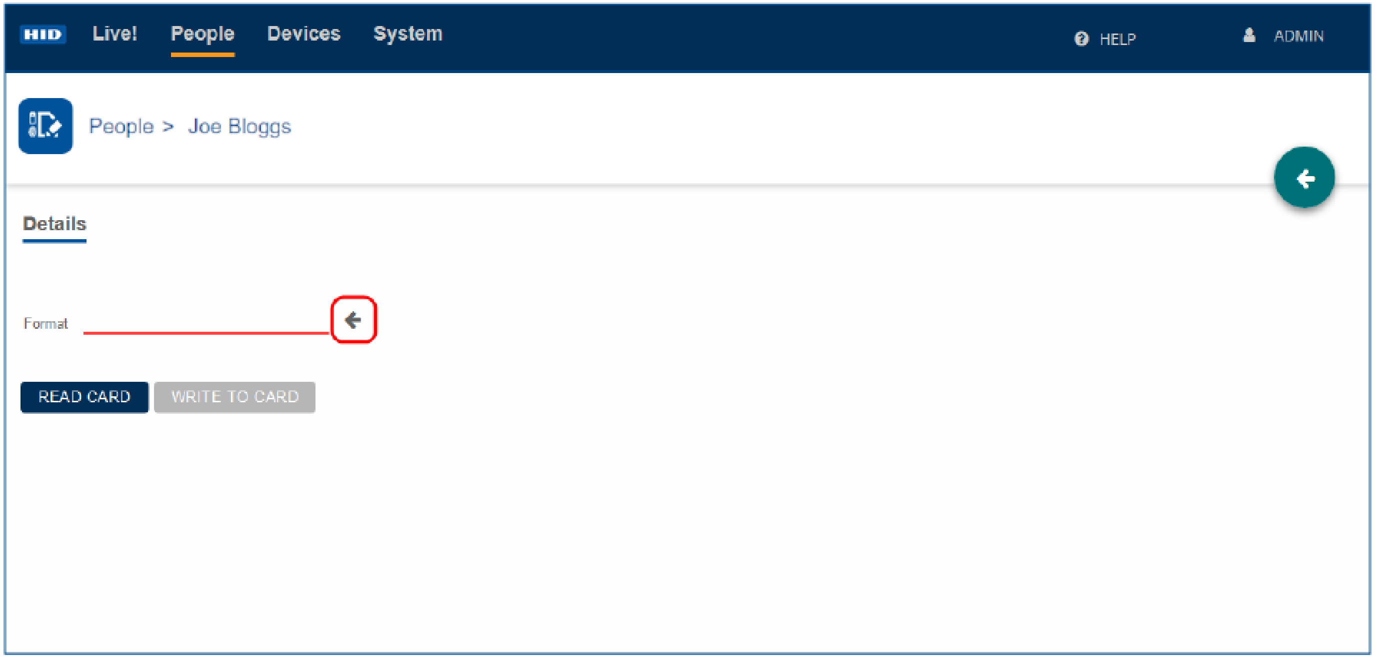
Credential Identifier 68737251781

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

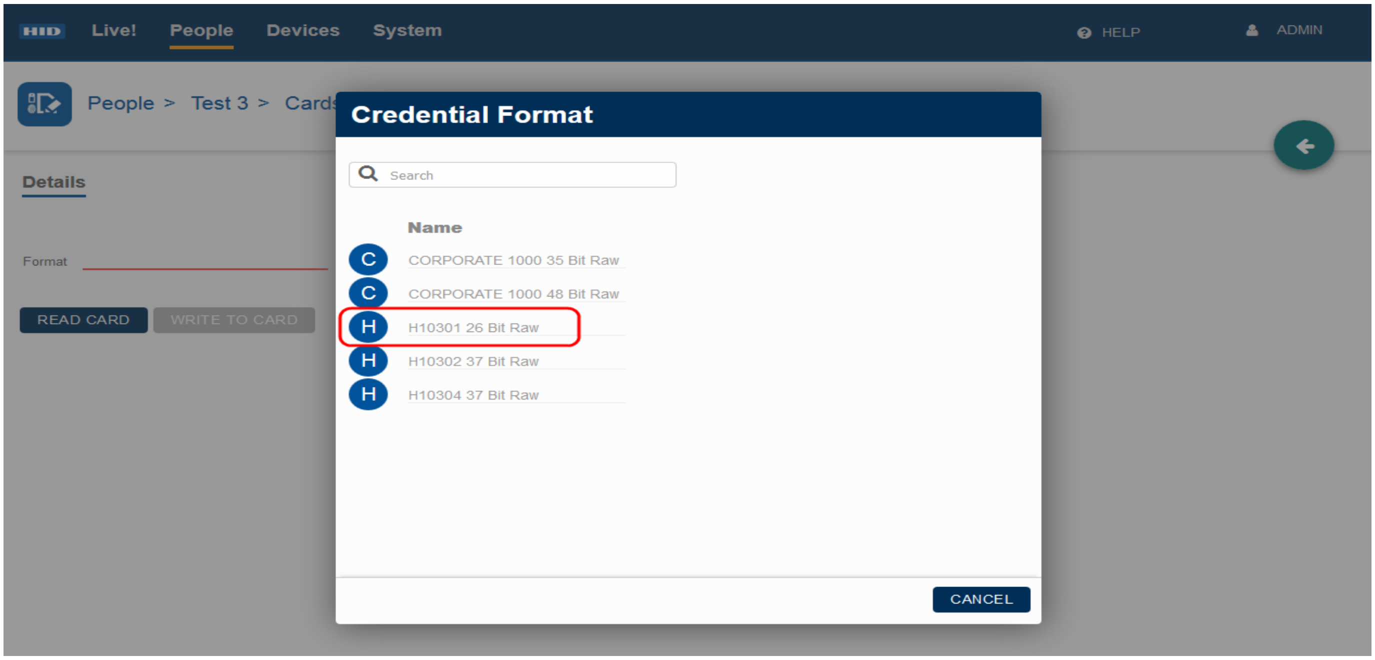
Manually enter card details

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.

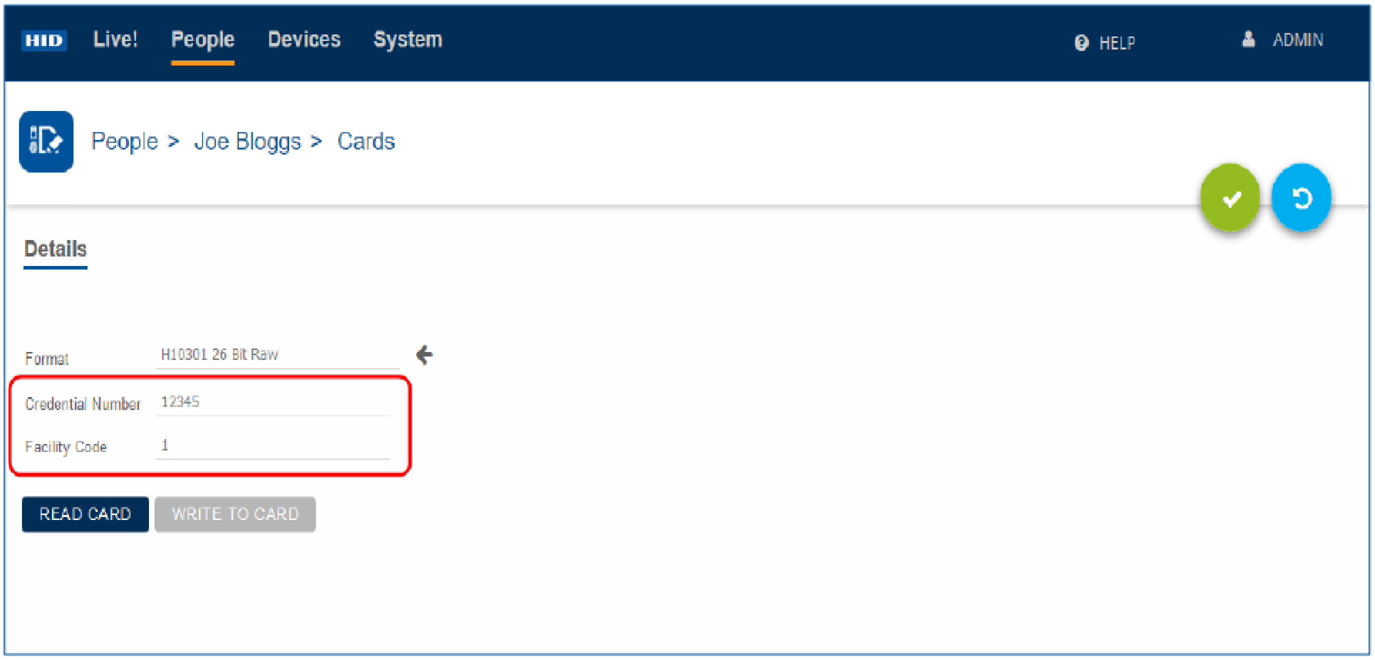


2. Select the **Credential Format** appropriate for the card in use.



	Name
C	CORPORATE 1000 35 Bit Raw
C	CORPORATE 1000 48 Bit Raw
H	H10301 26 Bit Raw
H	H10302 37 Bit Raw
H	H10304 37 Bit Raw

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



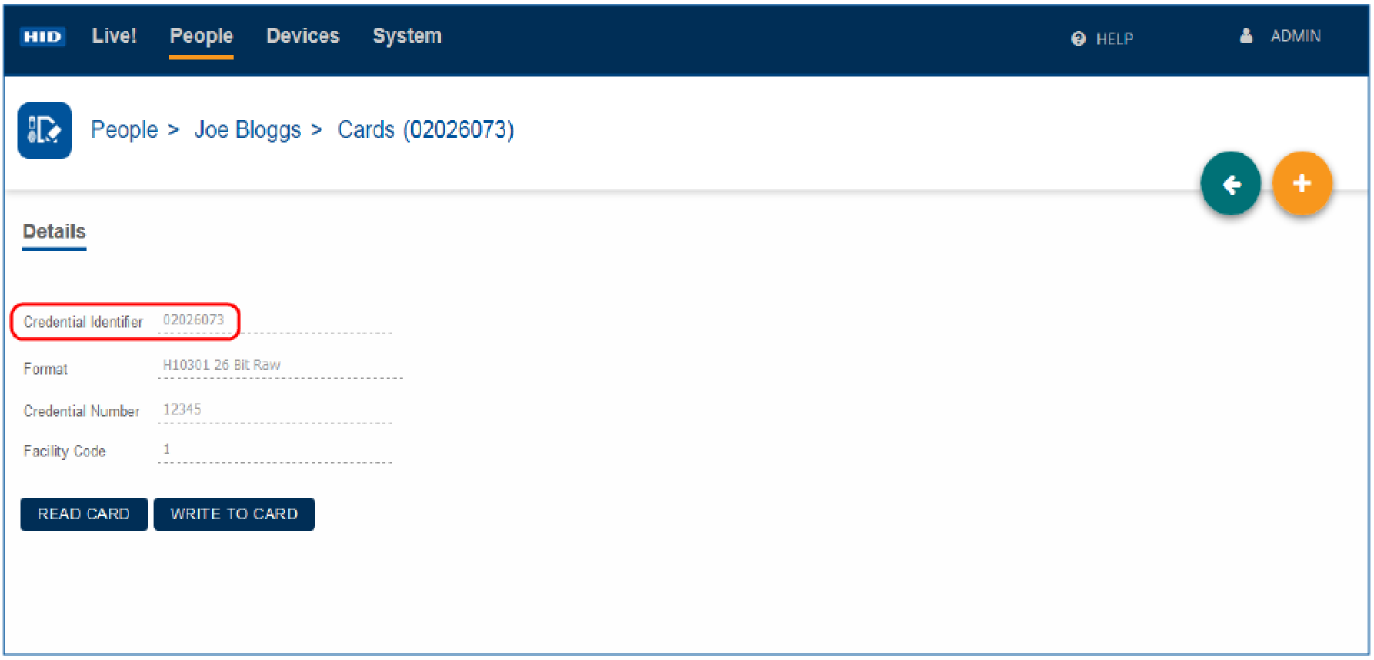
Format H10301 26 Bit Raw

Credential Number 12345

Facility Code 1

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.



Credential Identifier 02026073

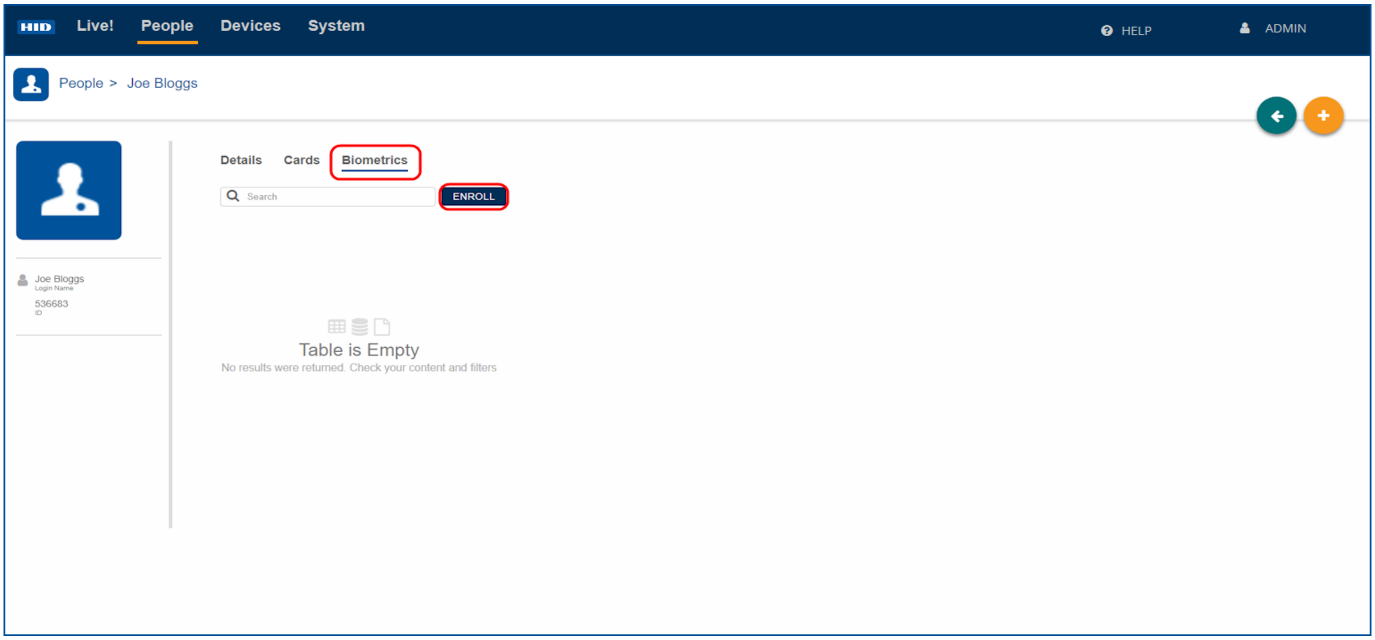
Format H10301 26 Bit Raw

Credential Number 12345

Facility Code 1

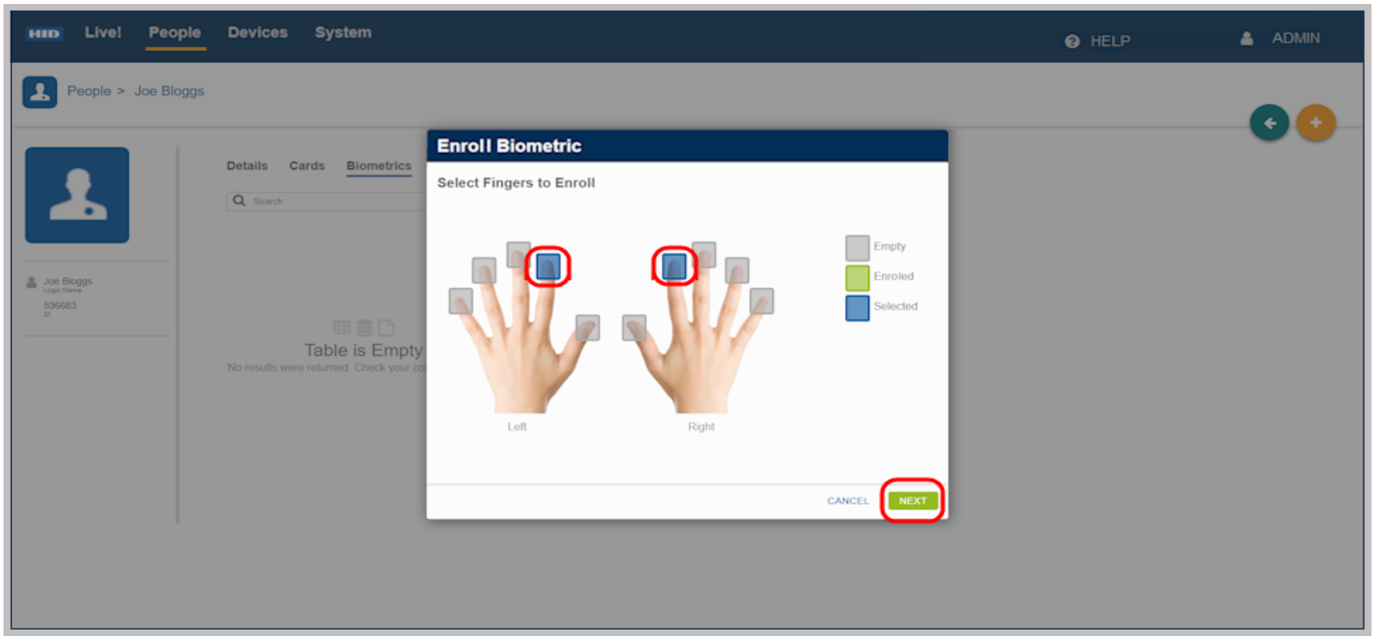
2.6.3 Enroll Biometrics

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



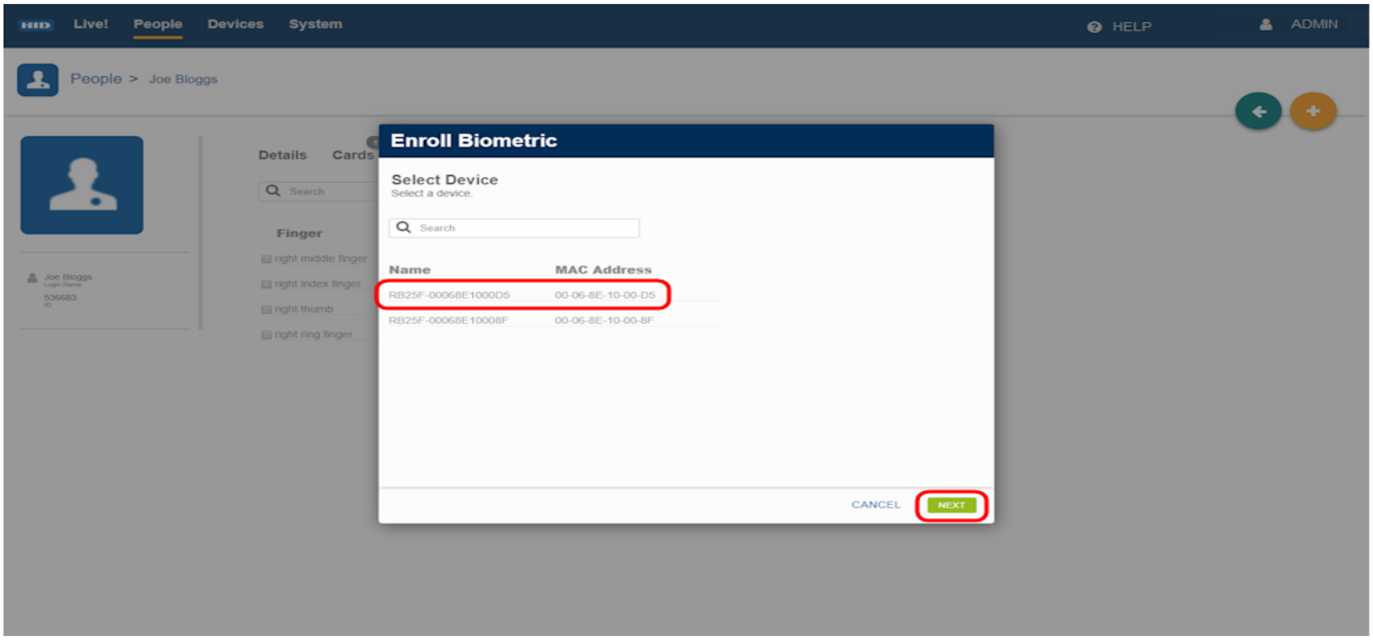
4. In the **Enroll Biometric** dialog select the fingers you wish to enroll and click **Next**.

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.



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 **Configure device settings**.



Enroll Biometric

Select Device
Select a device.

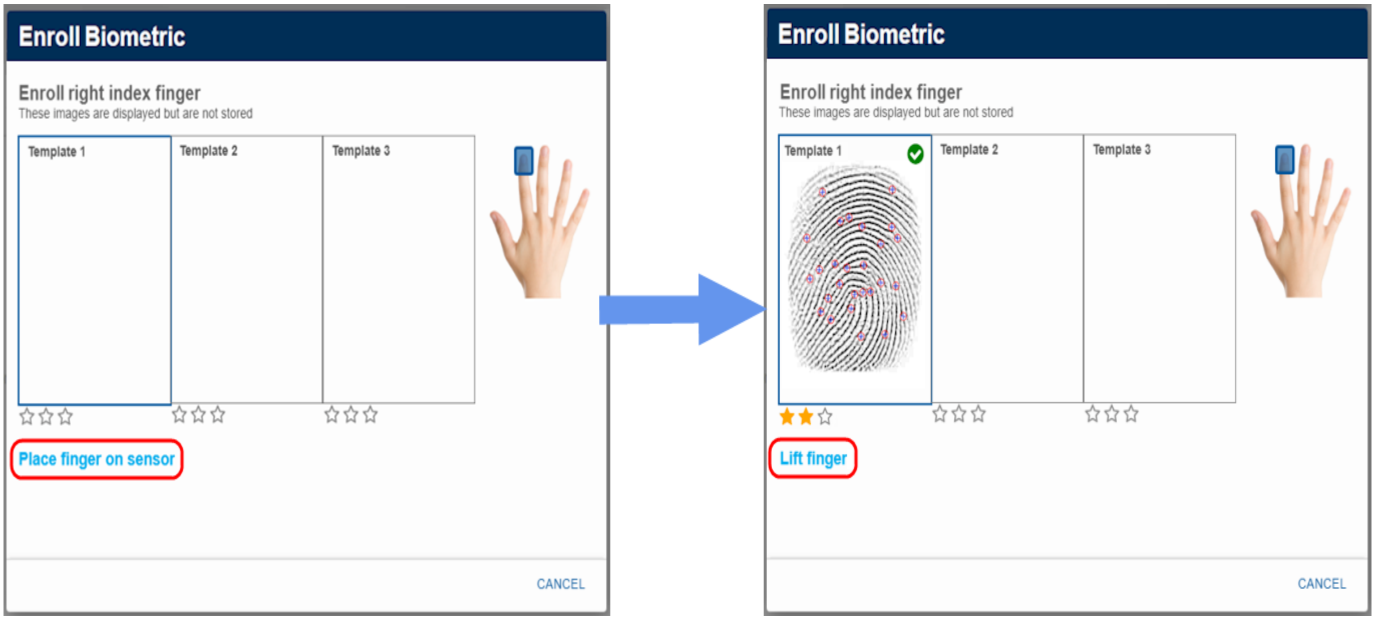
Search

Name	MAC Address
RB25F-00068E1000D5	00-06-8E-10-00-D5
RB25F-00068E10008F	00-06-8E-10-00-8F

CANCEL NEXT

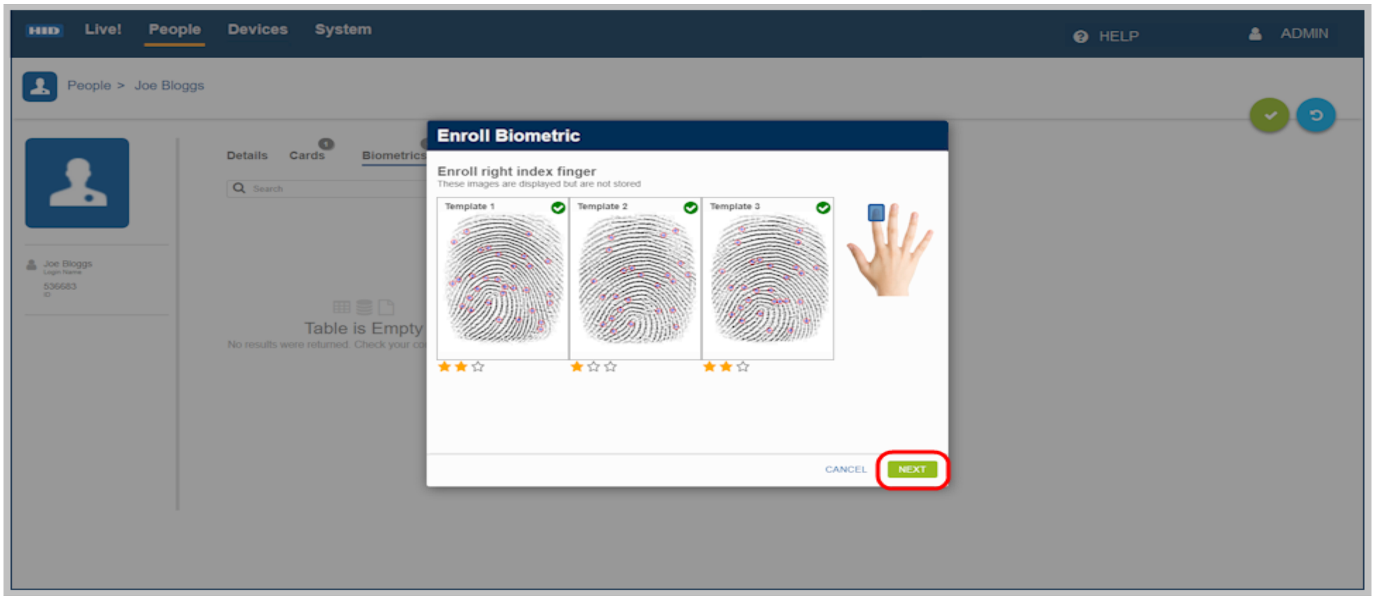
6. For the highlighted finger you will be prompted to **<Place finger on sensor>** followed by **<Lift finger>**. It is recommended that you follow the on-screen prompts, in the correct sequence, to ensure a successful finger scan.

Note: For information regarding the correct method of presenting fingers to the scanner during the biometric enrollment process, see *HID iCLASS SE® RB25F User Guide* (PLT-04900).



7. 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.

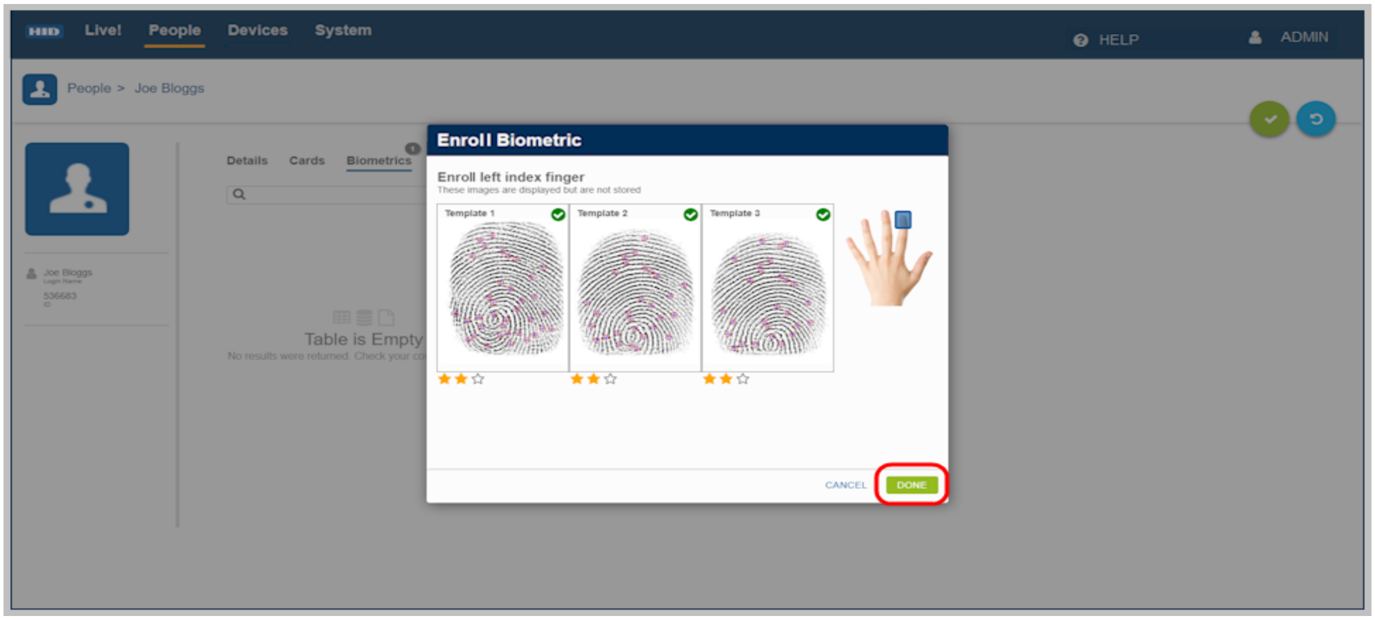


Enroll right index finger

These images are displayed but are not stored

8. 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.
9. 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.



Enroll left index finger

These images are displayed but are not stored

2.7 Load HID Elite keys

This feature allows HID to push HID Elite™ keys to the customer via the web. Currently, only Seos® cards are supported by the HID Elite keys.

Note: Standard keys will not work on the RB25F once Elite keys have been loaded to the device.

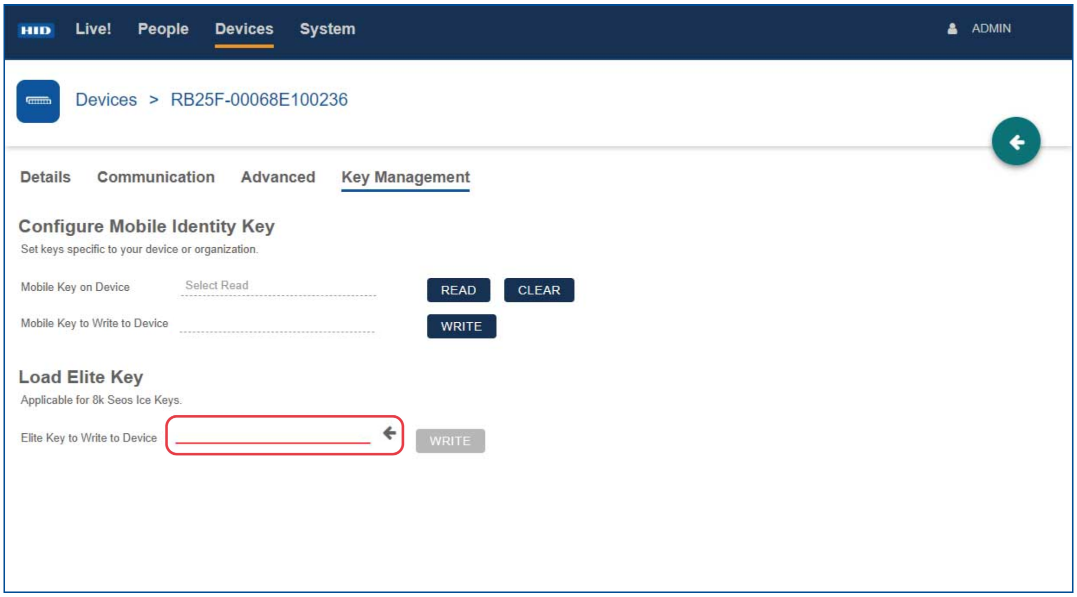
Note: After a factory reset, the device cannot be checked for standard or Elite key configurations.

The reader technician account needs to be setup in order to perform this operation. See **Validate a Reader Manager account in HID Biometric Manager**

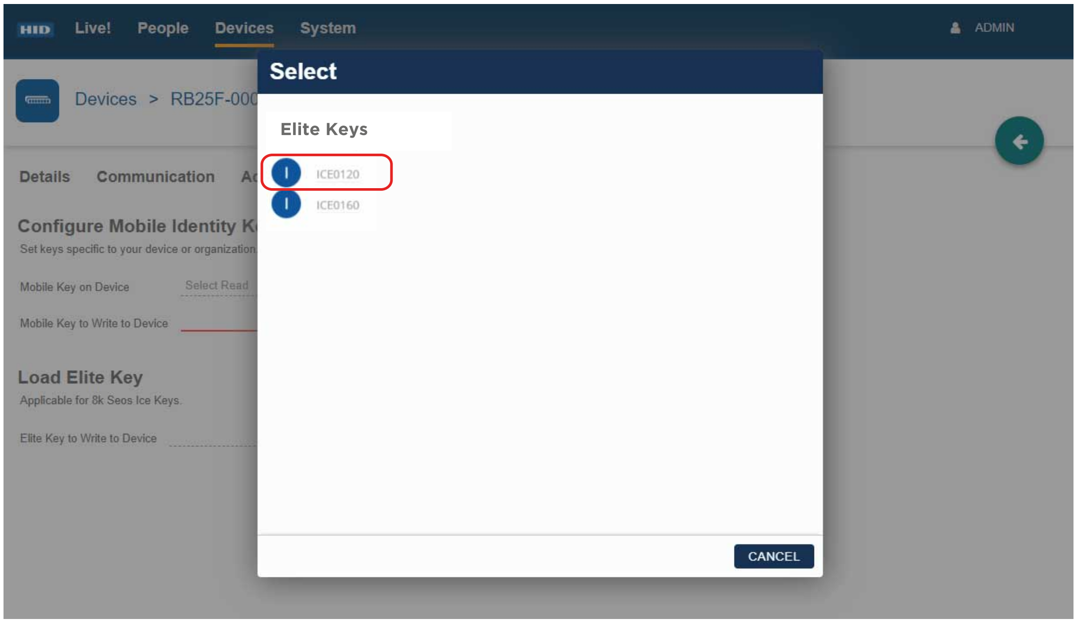
Note: You need to be fully enrolled in HID Elite with an ICE Key reference for RB25F to load your ICE Key in the field. This may require contacting HID Credential Programs for confirmation of enrolment.

To load Elite keys:

1. Select a device.
2. Open the **Key Management** tab.
3. Click the arrow to select Elite keys.


HID
Live!
People
Devices
System
ADMIN
Devices > RB25F-00068E100236
Details
Communication
Advanced
Key Management
Configure Mobile Identity Key
Set keys specific to your device or organization.
Mobile Key on Device
Select Read
READ
CLEAR
Mobile Key to Write to Device
WRITE
Load Elite Key
Applicable for 8k Seos Ice Keys.
Elite Key to Write to Device
WRITE

4. Select a key set to load.


HID
Live!
People
Devices
System
ADMIN
Devices > RB25F-000
Details
Communication
Configure Mobile Identity K
Set keys specific to your device or organization
Mobile Key on Device
Select Read
Mobile Key to Write to Device
Load Elite Key
Applicable for 8k Seos Ice Keys.
Elite Key to Write to Device
Select
Elite Keys
ICE0120
ICE0160
CANCEL

5. With the key set selected, click **Write**.

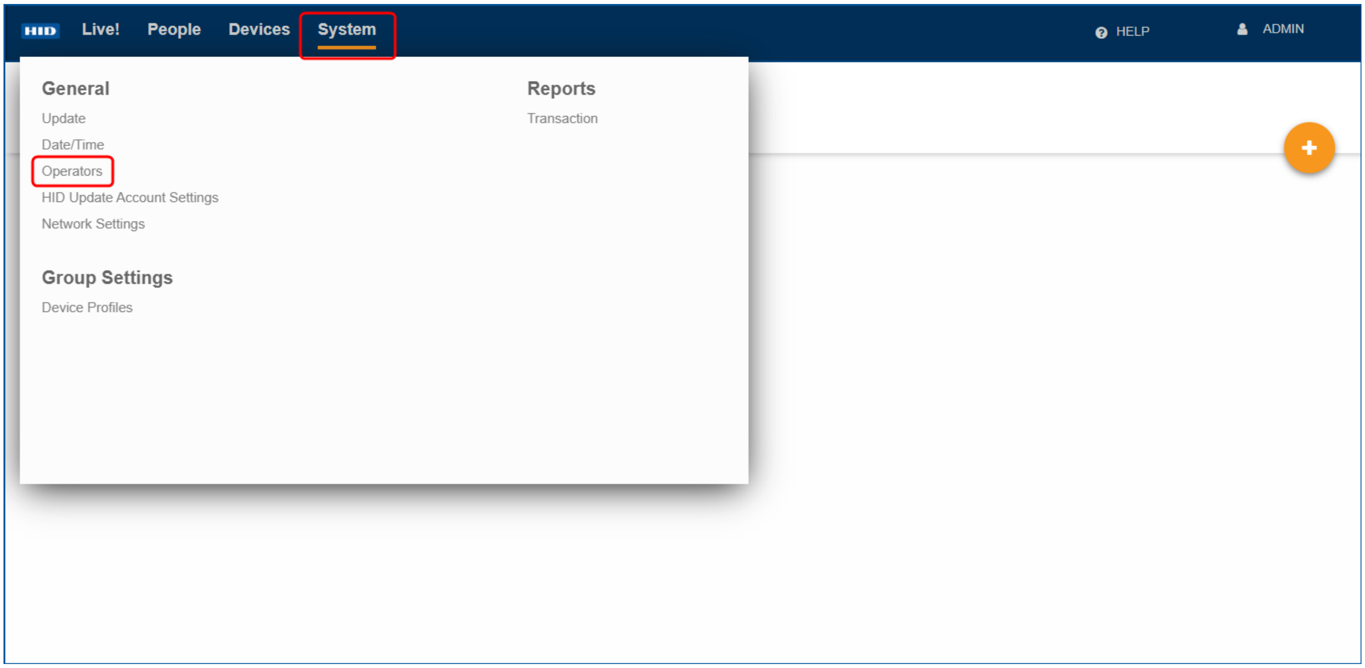
2.7.1 Create Biometric Manager operators

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

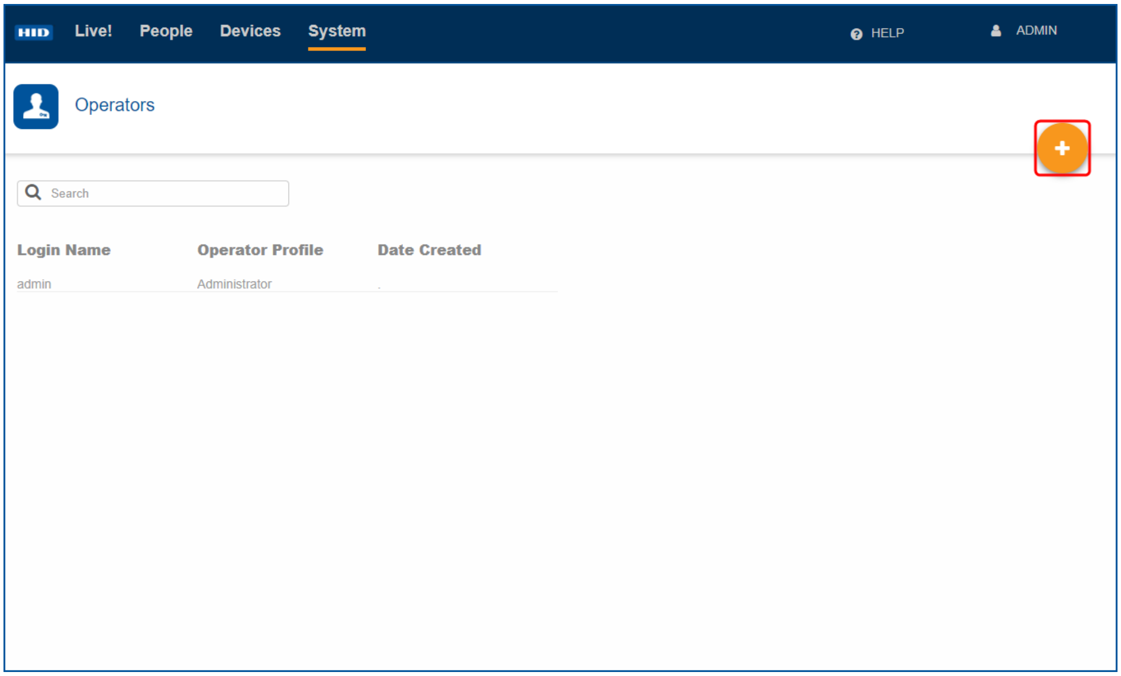
- **Administrator:** This operator role has full access to Biometric Manager web application with functions to install and manage RB25F devices, enroll people in the system, add credentials, and collect and store associated biometric data.
- **Device Administrator:** This operator role is intended for 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.

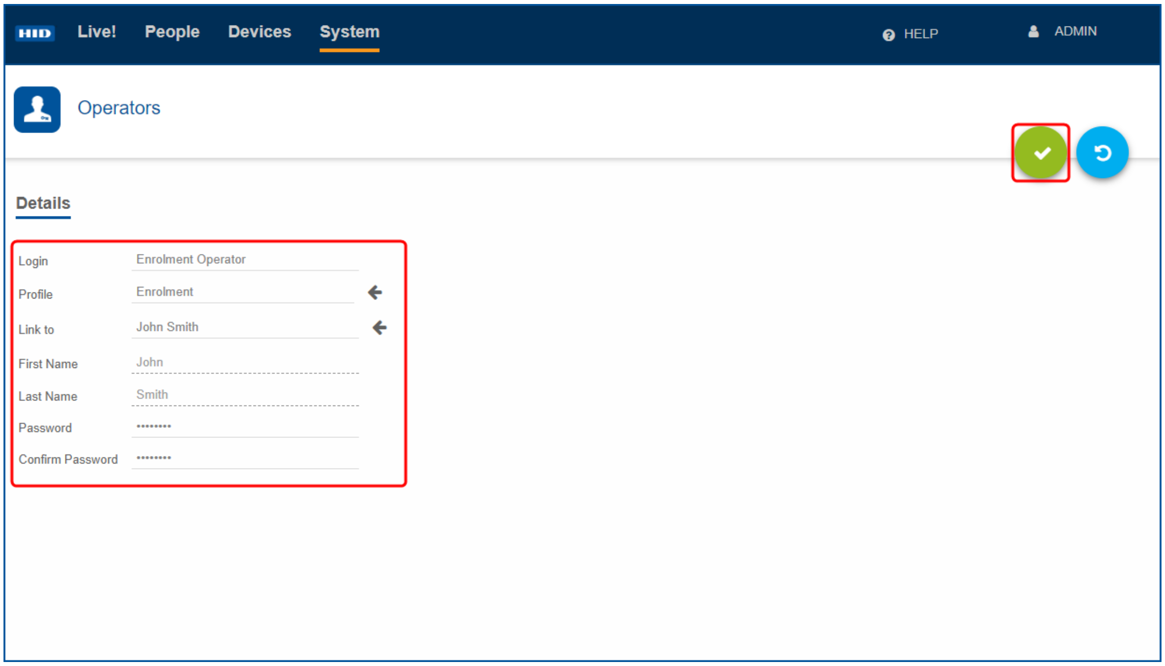


3. To add and operator, click the New icon [+].



Login Name	Operator Profile	Date Created
admin	Administrator	.

4. 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.
5. Click the **Save** icon [✓] to save the operator profile.

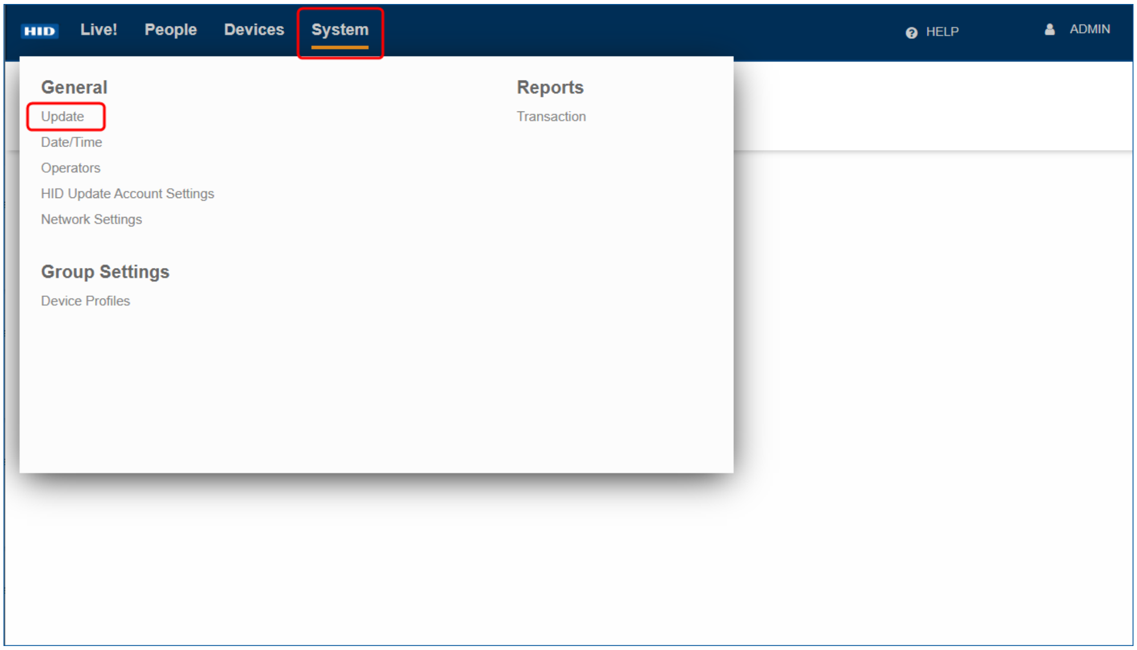


Login	Enrolment Operator
Profile	Enrolment
Link to	John Smith
First Name	John
Last Name	Smith
Password	••••••••
Confirm Password	••••••••

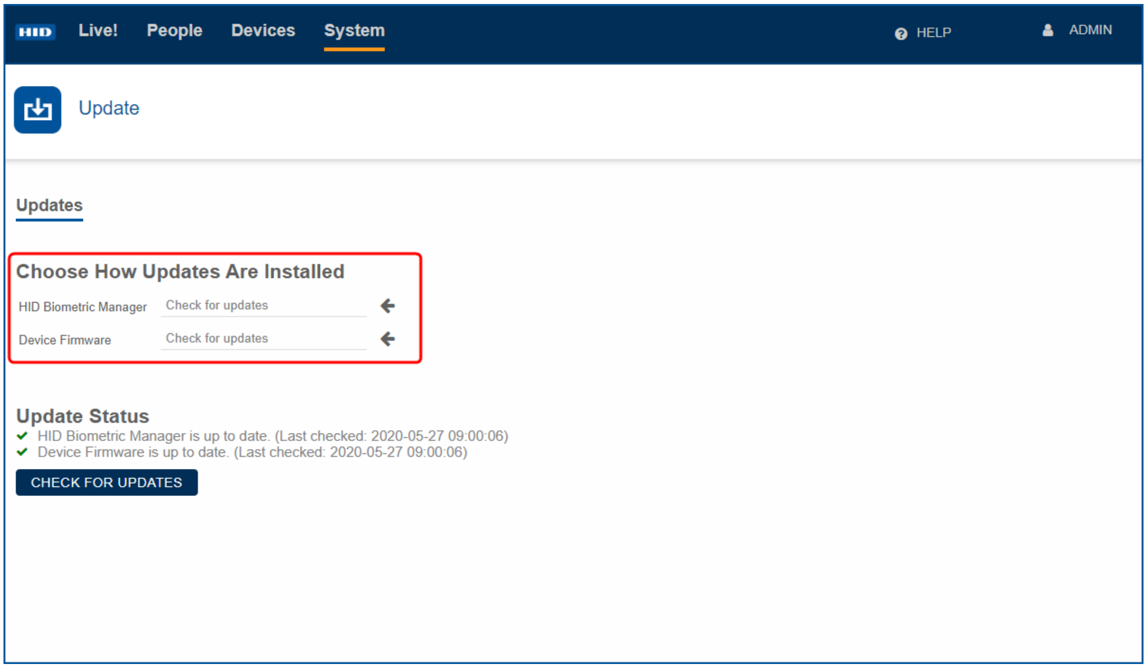
2.7.2 Configure software/firmware update settings

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 setings.



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.



Choose How Updates Are Installed

HID Biometric Manager: Check for updates

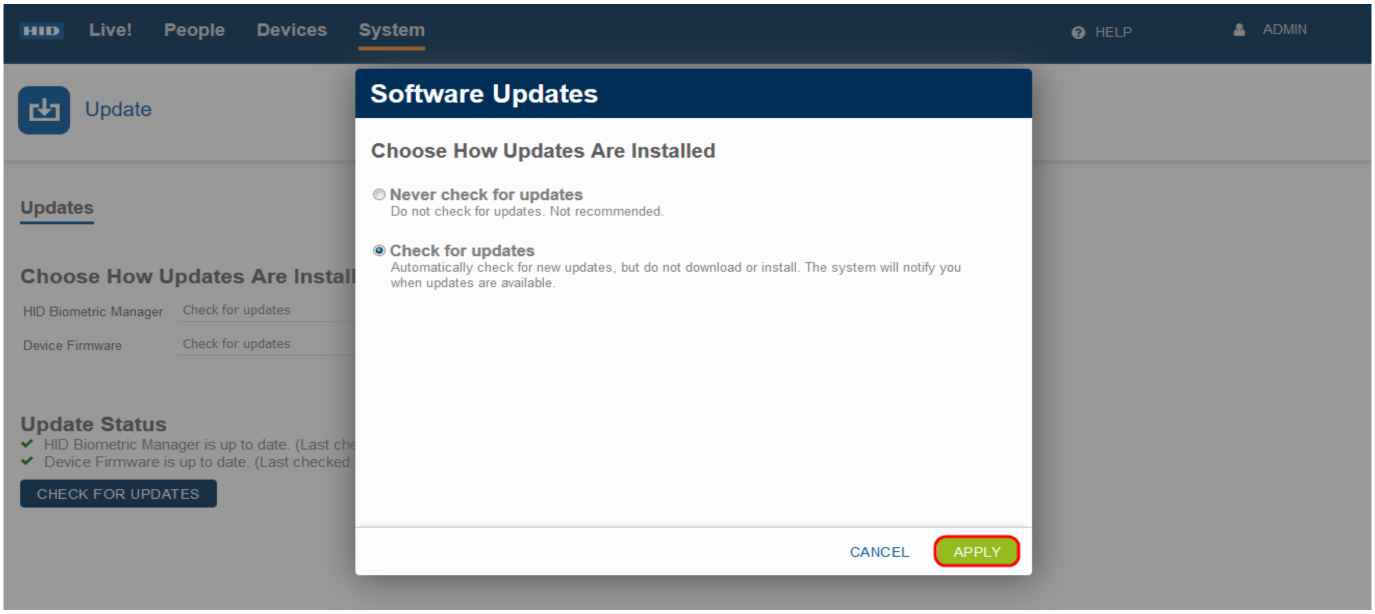
Device Firmware: Check for updates

Update Status

✓ HID Biometric Manager is up to date. (Last checked: 2020-05-27 09:00:06)

✓ Device Firmware is up to date. (Last checked: 2020-05-27 09:00:06)

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



Choose How Updates Are Installed

HID Biometric Manager: Check for updates

Device Firmware: Check for updates

Update Status

✓ HID Biometric Manager is up to date. (Last che

✓ Device Firmware is up to date. (Last checked:

CHECK FOR UPDATES

Software Updates

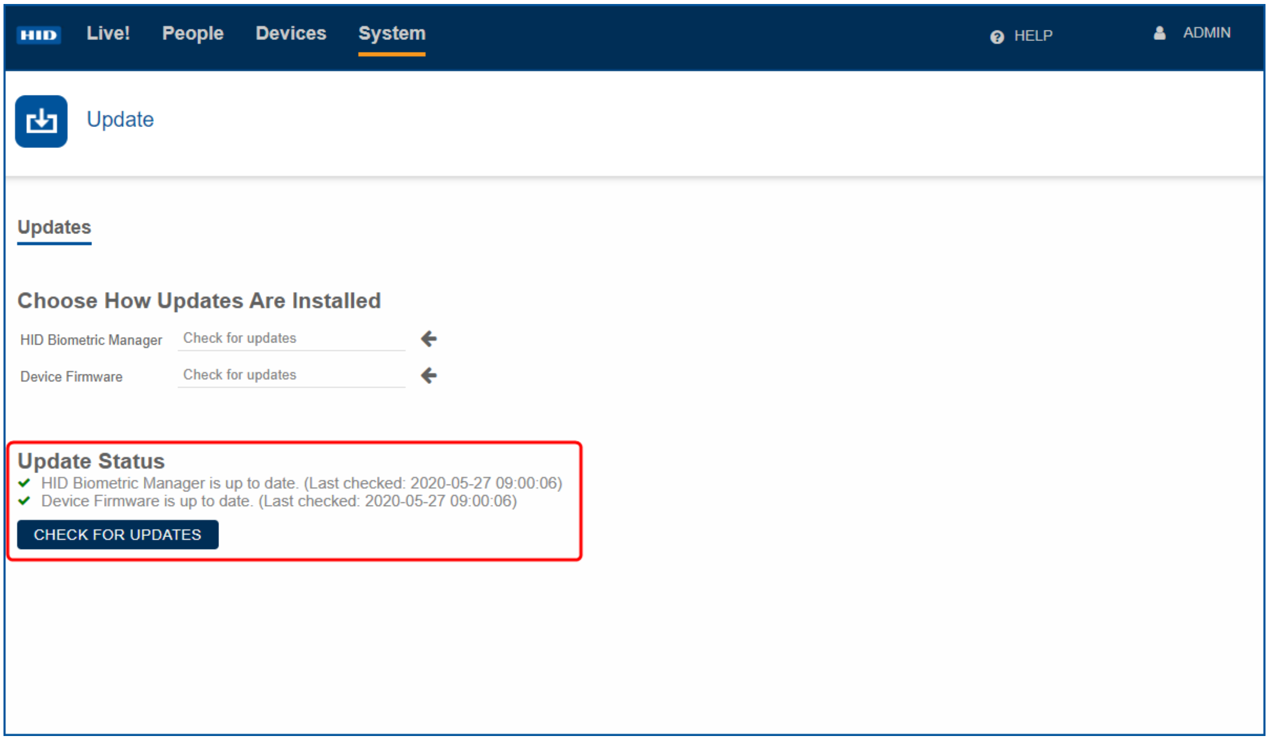
Choose How Updates Are Installed

○ **Never check for updates**
Do not check for updates. Not recommended.

● **Check for updates**
Automatically check for new updates, but do not download or install. The system will notify you when updates are available.

CANCEL 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 **Device firmware update**.



Choose How Updates Are Installed

HID Biometric Manager: Check for updates

Device Firmware: Check for updates

Update Status

✓ HID Biometric Manager is up to date. (Last checked: 2020-05-27 09:00:06)

✓ Device Firmware is up to date. (Last checked: 2020-05-27 09:00:06)

CHECK FOR UPDATES

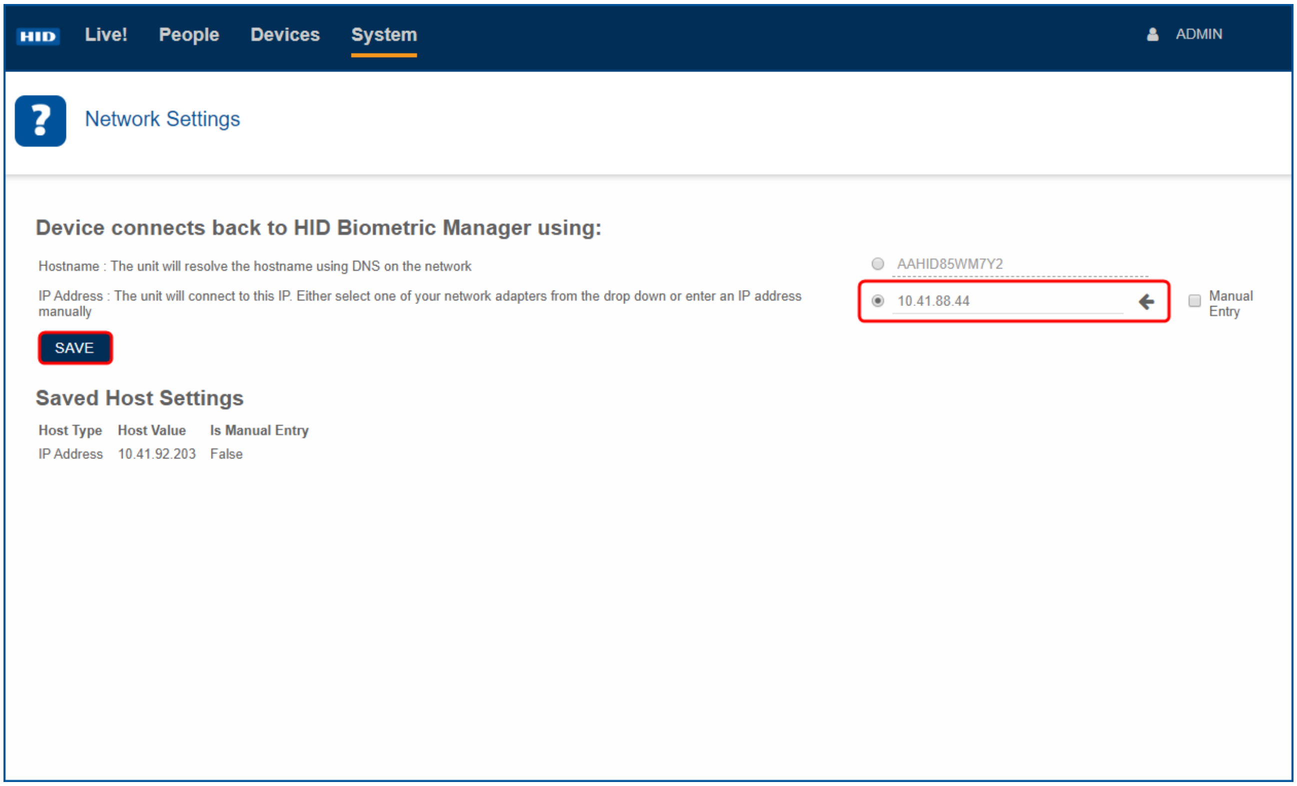
2.7.3 Setting static IP for HBM network

HID Biometric Manager has a feature that allows each device and the HBM network to have a static IP address. When all connected devices and the HBM network are configured with the correct static IP settings, the system continues to operate if the DHCP server is turned off.

To set the static IP for the HBM network:

1. Select **Network Settings** from the **System** menu.
2. Select **IP Address**and click the arrow to select a **Host IP** from the list.

   Note: Tick the Manual Entry box to manually enter the IP Address.



Device connects back to HID Biometric Manager using:

Hostname : The unit will resolve the hostname using DNS on the network ○ AAHID85WM7Y2

IP Address : The unit will connect to this IP. Either select one of your network adapters from the drop down or enter an IP address manually ● 10.41.88.44 □ Manual Entry

SAVE

Saved Host Settings

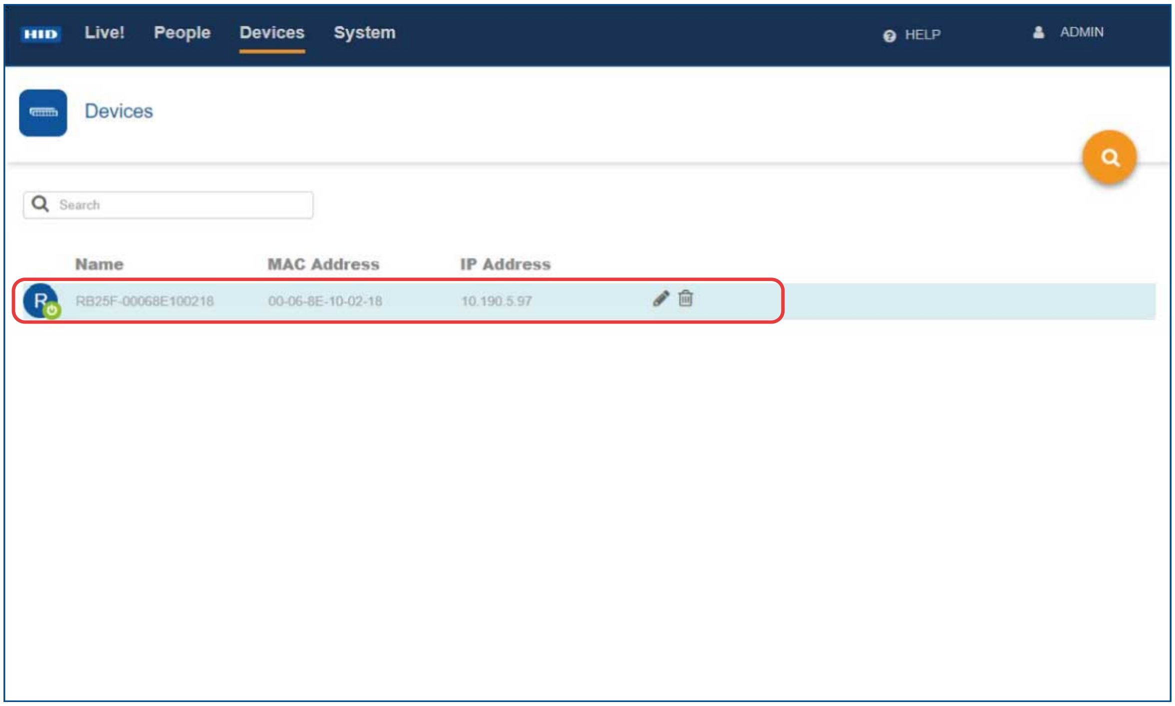
Host Type	Host Value	Is Manual Entry
IP Address	10.41.92.203	False

3. Click **Save** to finish.

2.7.4 Setting static IP for a specific device

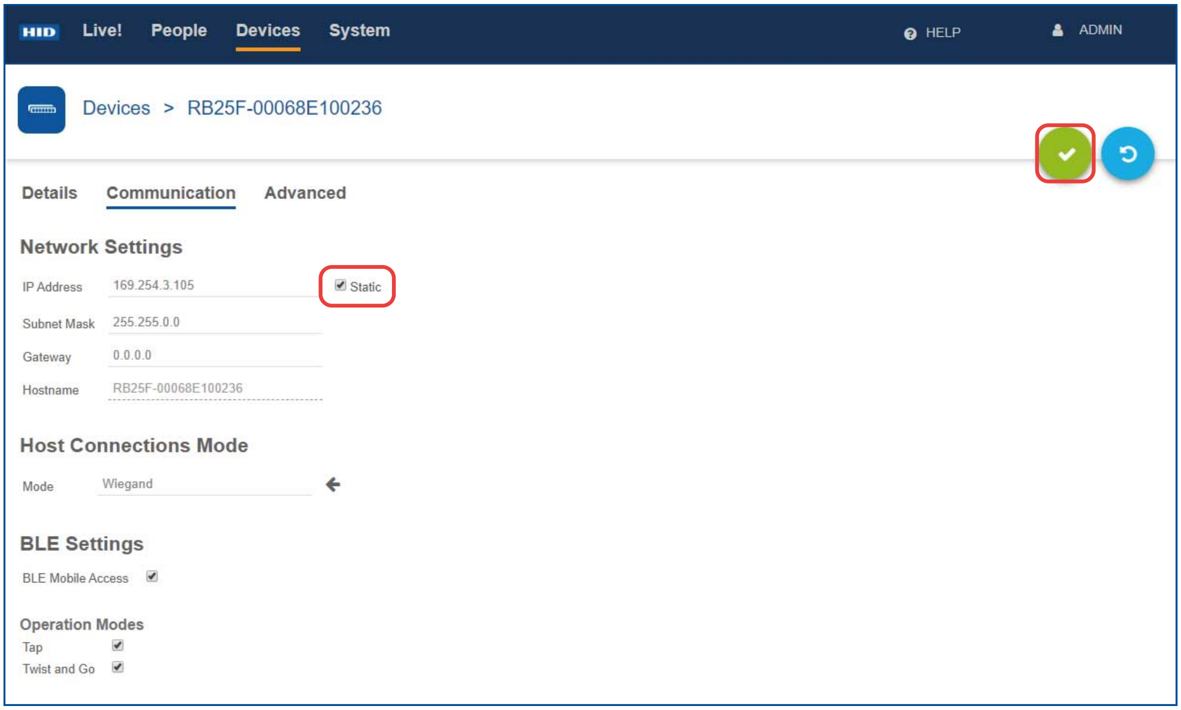
To set the static IP for an individual device:

1. Open the **Devices** page.
2. Select a device to configure.



Name	MAC Address	IP Address
RB25F-00068E100218	00-06-8E-10-02-18	10.190.5.97

3. On the **Devices** page, select the **Communications** tab.
4. Tick the **Static** box to set the static IP address.



Network Settings

IP Address 169.254.3.105 ☑ Static

Subnet Mask 255.255.0.0

Gateway 0.0.0.0

Hostname RB25F-00068E100236

Host Connections Mode

Mode Wiegand

BLE Settings

BLE Mobile Access ☑

Operation Modes

Tap ☑

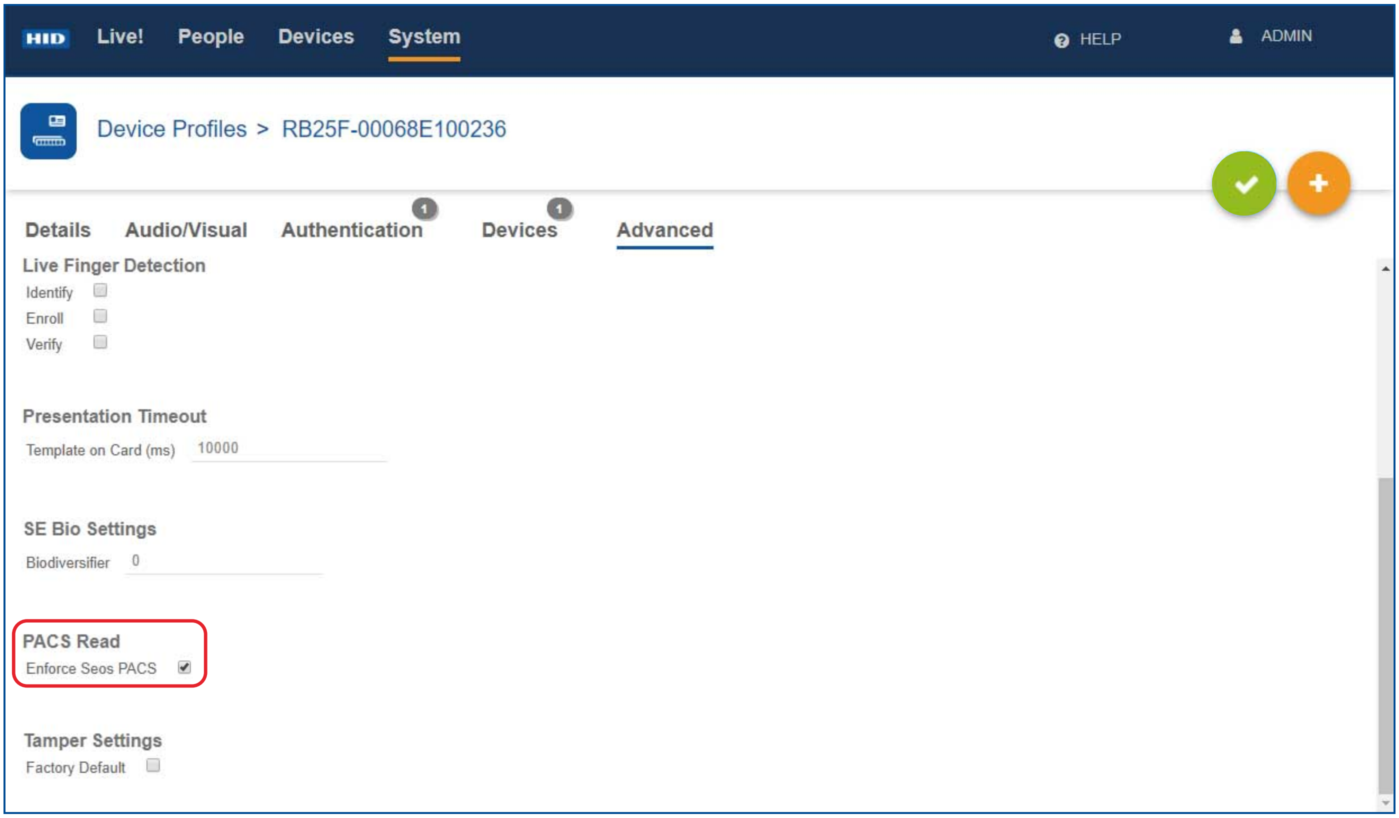
Twist and Go ☑

5. Click **Save** ✓ to finish.

2.8 Enforce Seos read

The reader will only read PACS data of a Seos card with this feature enabled. If only using credentials that are multi technology HID cards with Seos or Seos cards with static UID, this feature is recommended.

The **Enforce Seos PACS** option can be toggled on or off in **Device Profiles** under the **Advanced** tab.



Device Profiles > RB25F-00068E100236

Live Finger Detection
Identify □
Enroll □
Verify □

Presentation Timeout
Template on Card (ms) 10000

SE Bio Settings
Biodiversifier 0

PACS Read
Enforce Seos PACS ☑

Tamper Settings
Factory Default □

Click the **Save** ✓ icon to finish.

Note: If using Seos credentials without this option enabled, the PACS data read will not be consistent.

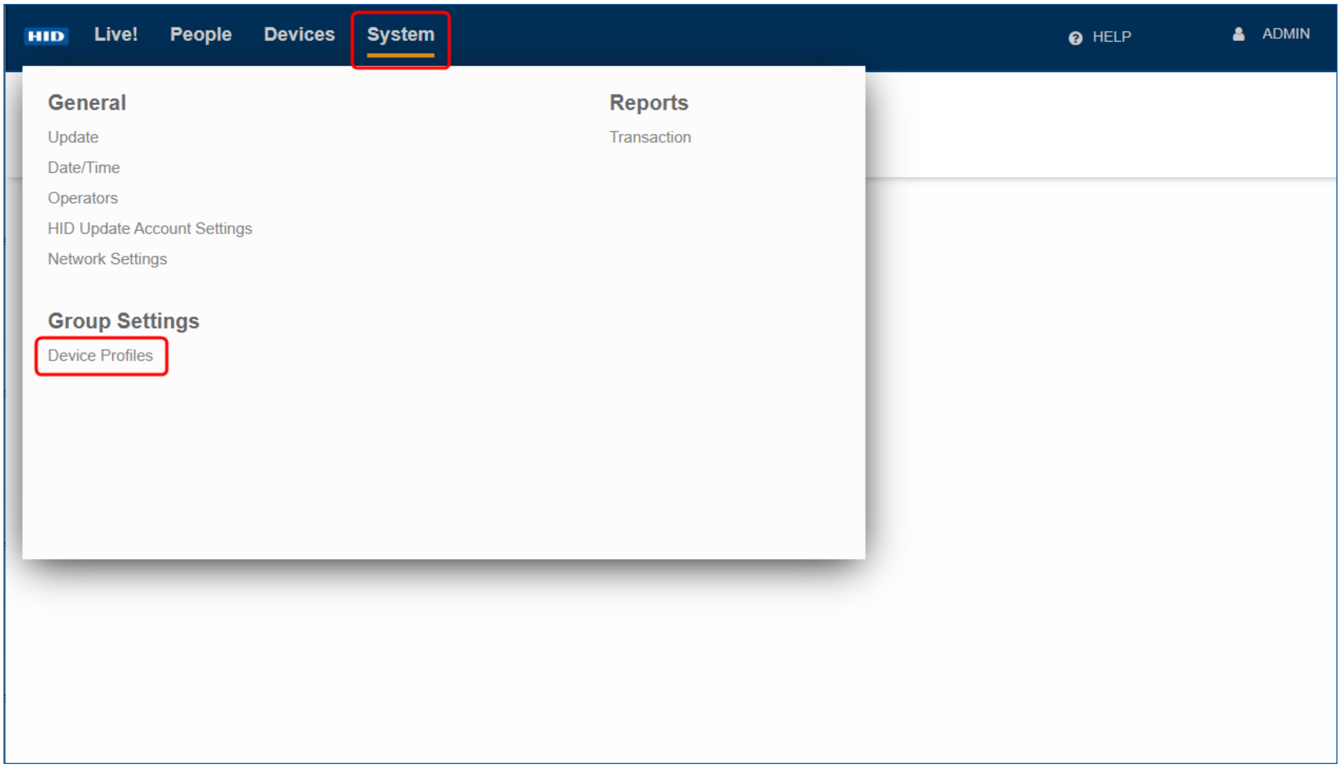
2.9 Device profiles

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.

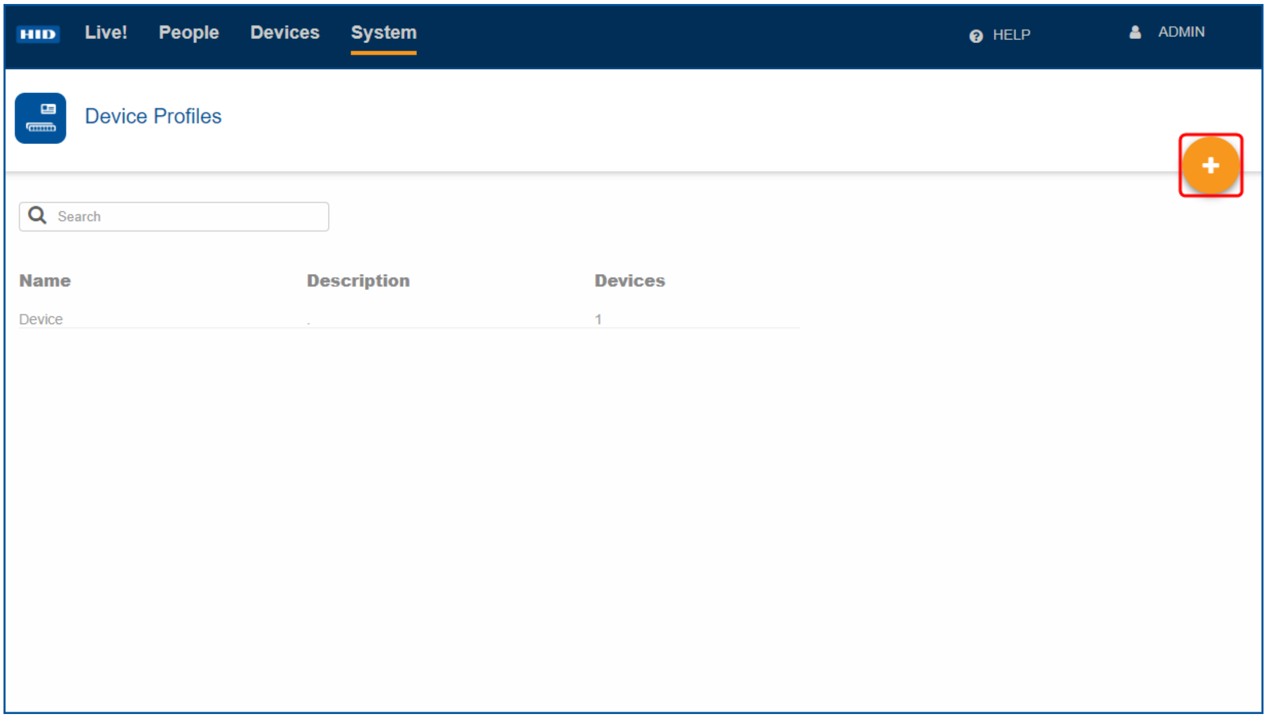
2.9.1 Create a device profile

To create a new device profile:

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

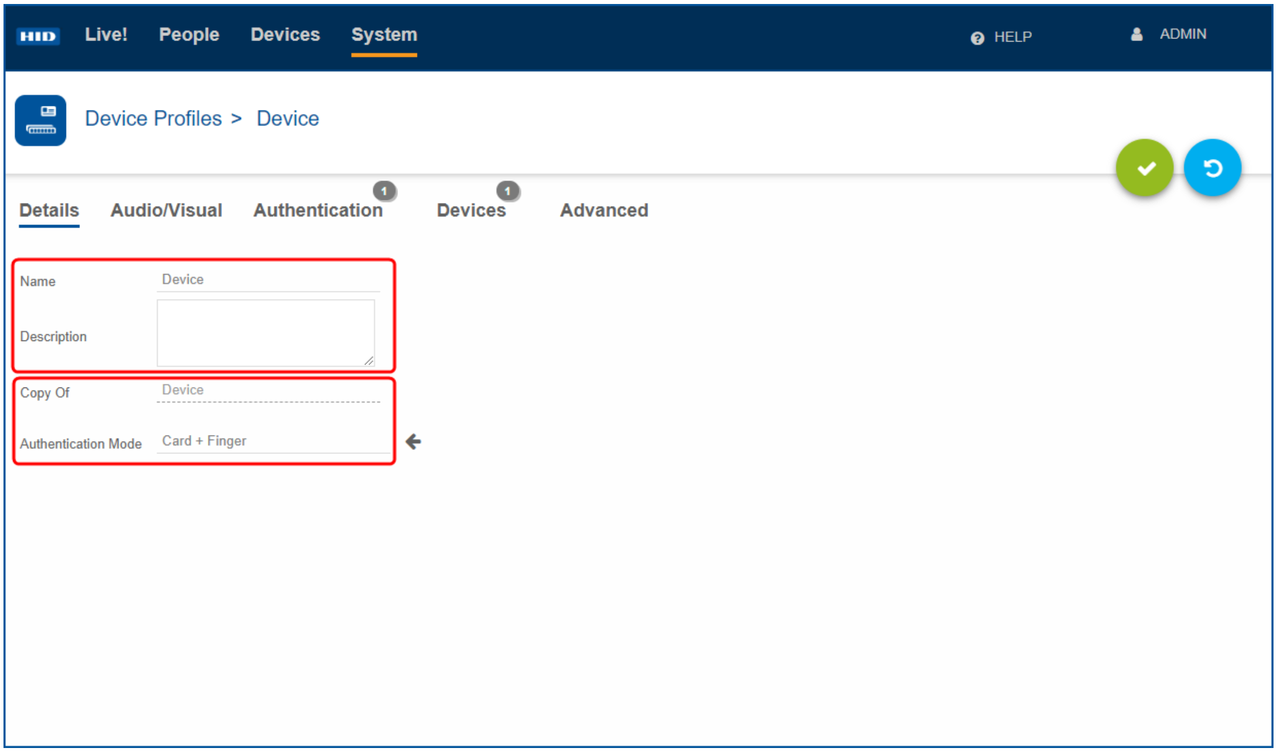


2. Click the **Add** icon [+].



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

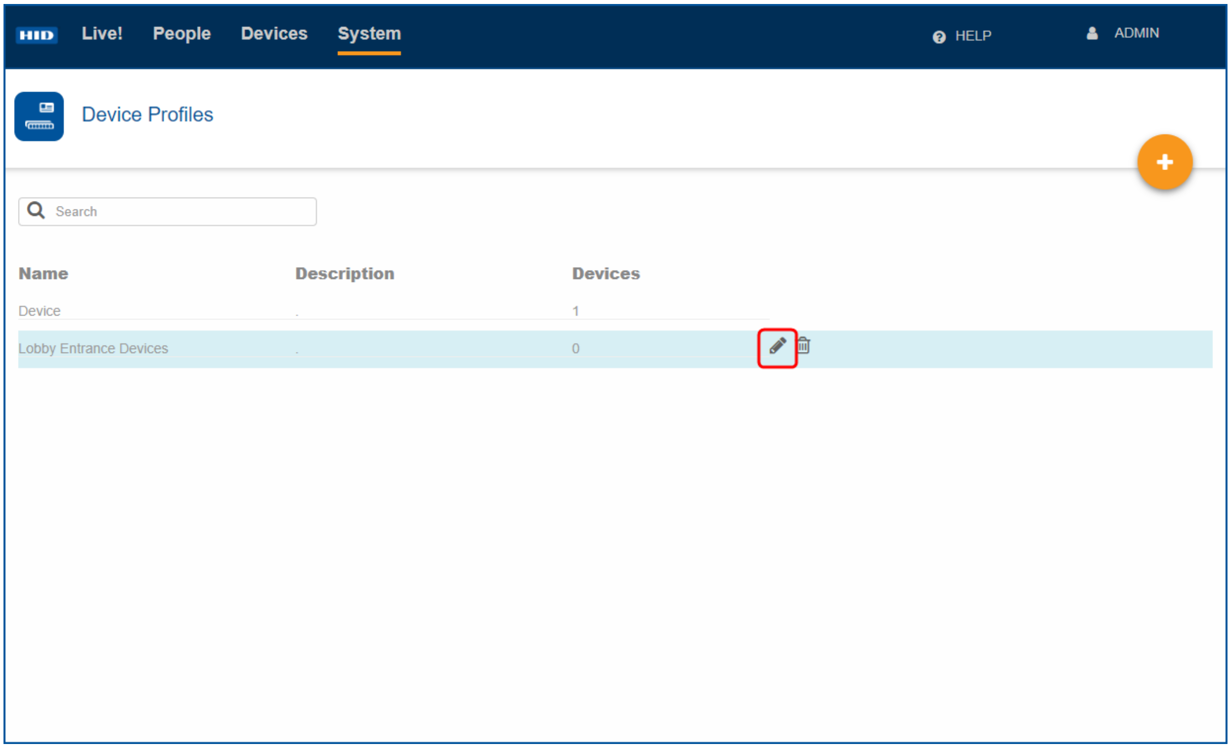
Note: Select the arrow icon associated with **Authentication Mode** to select an Authentication Mode. Device Profile attributes can now be edited. See [Edit a device profile](#).



Name: Device
Description:
Copy Of: Device
Authentication Mode: Card + Finger

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 **Edit a device profile**.



Device Profiles

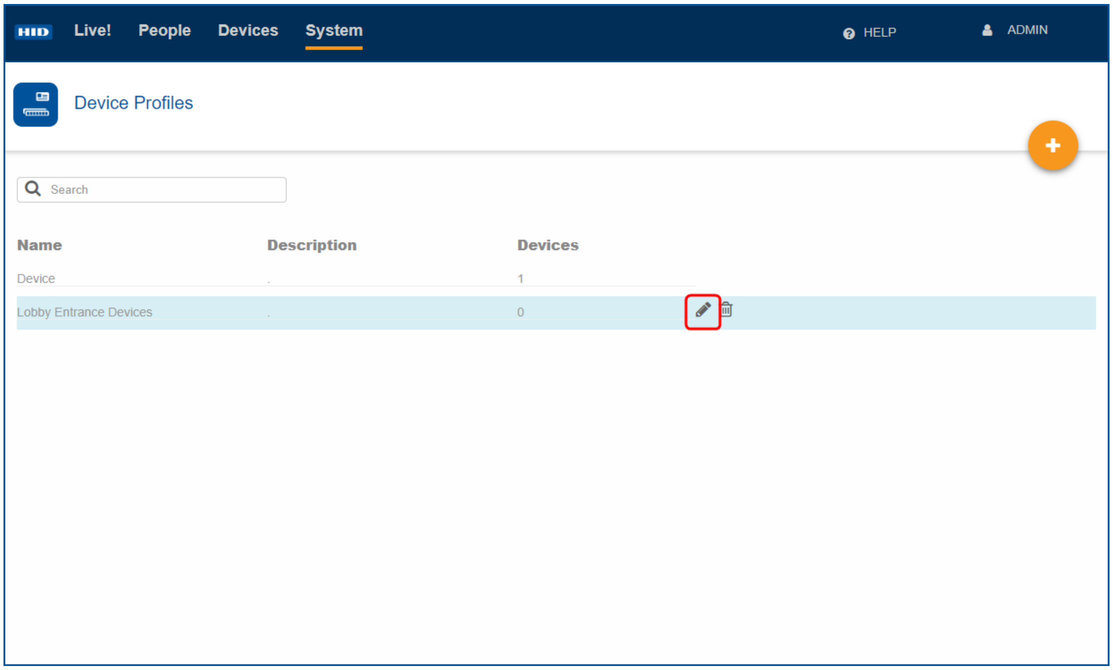
Search

Name	Description	Devices
Device	.	1
Lobby Entrance Devices	.	0

2.9.2 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.



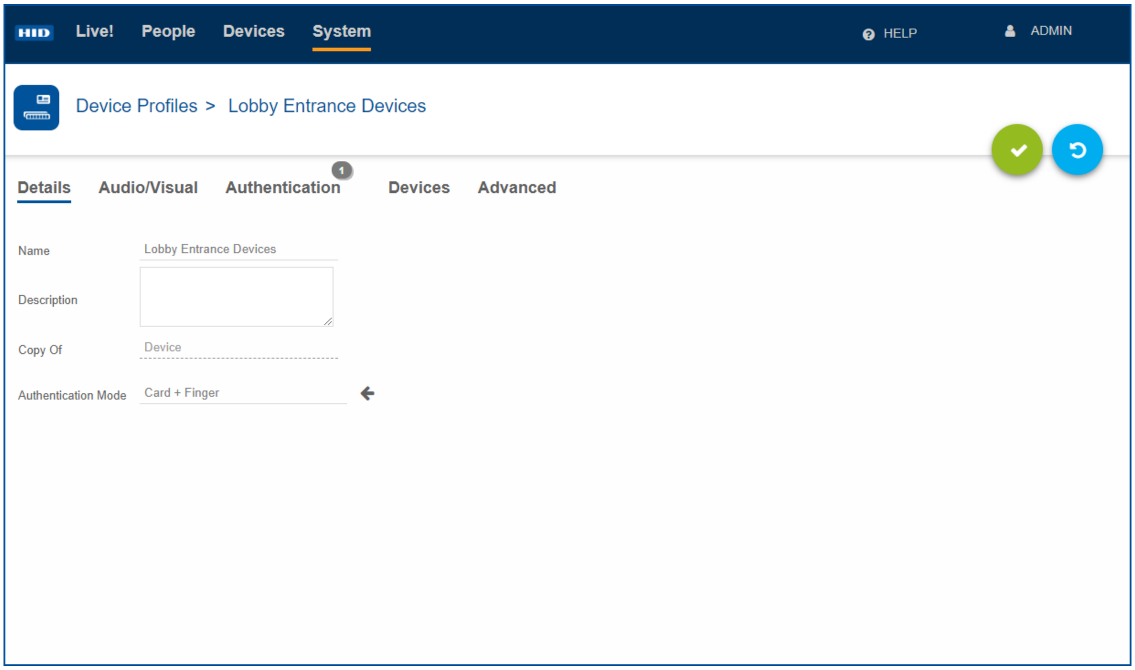
Device Profiles

Search

Name	Description	Devices
Device	.	1
Lobby Entrance Devices	.	0

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 [Acronyms and terminology](#).

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



Name: Lobby Entrance Devices

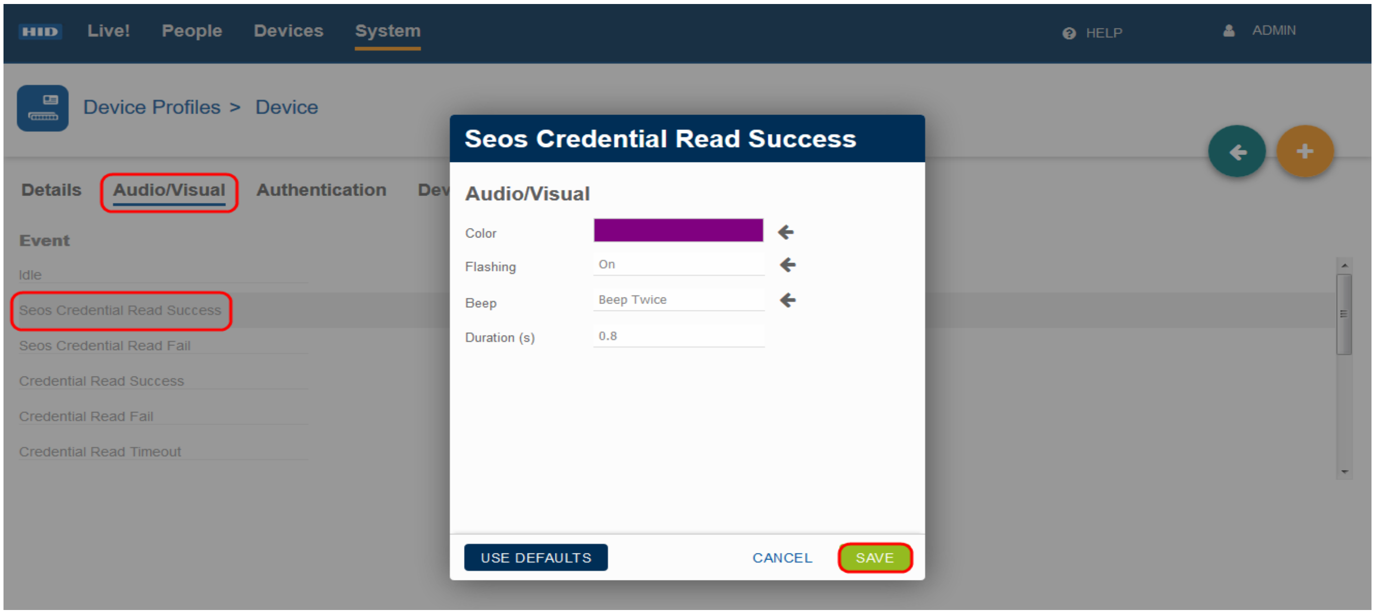
Description:

Copy Of: Device

Authentication Mode: Card + Finger

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 setings.

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



Event
- Idle
- Seos Credential Read Success
- Seos Credential Read Fail
- Credential Read Success
- Credential Read Fail
- Credential Read Timeout

Seos Credential Read Success

Audio/Visual

Color: 🟪

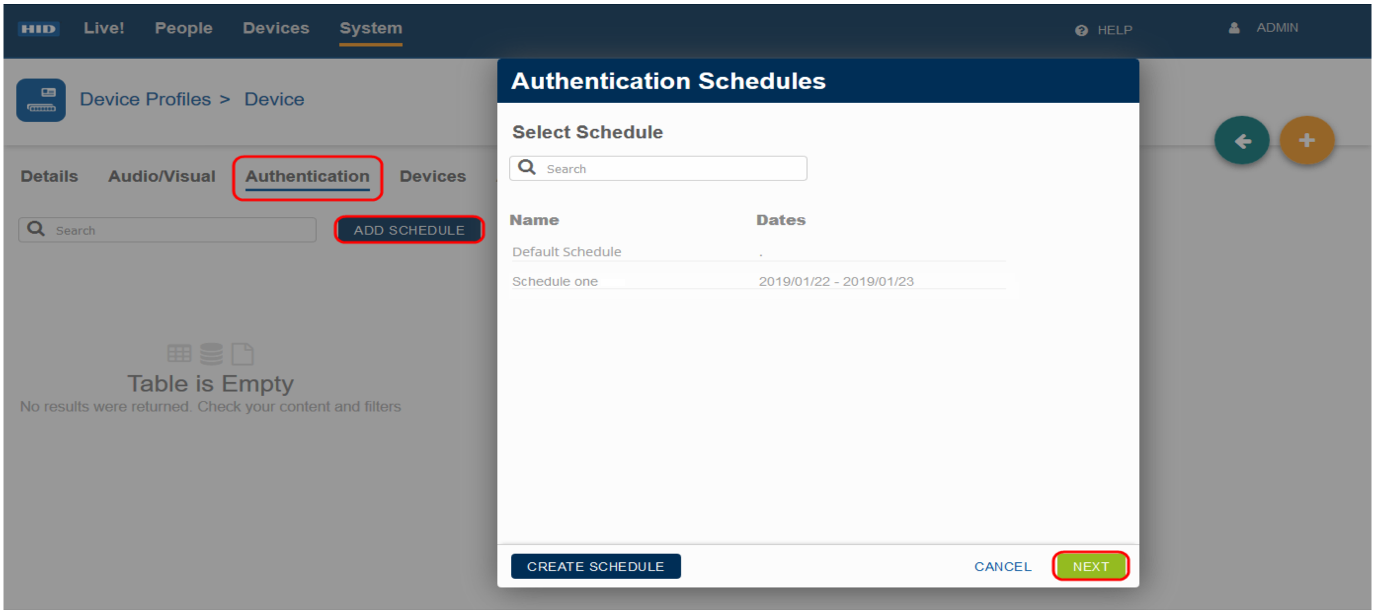
Flashing: On

Beep: Beep Twice

Duration (s): 0.8

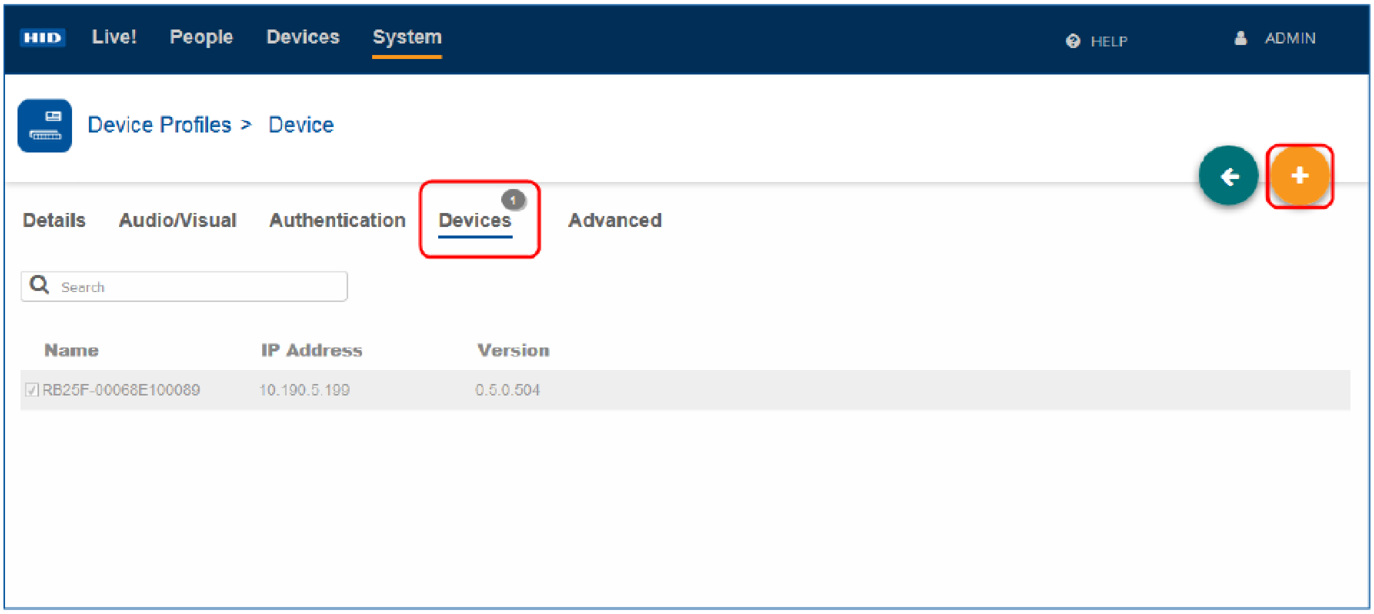
7. On the **Device** screen, select **Authentication**.
8. Click **ADD SCHEDULE** to schedule when a device will operate in a special Authentication Mode. Select a schedule from the list and click **Next**.

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



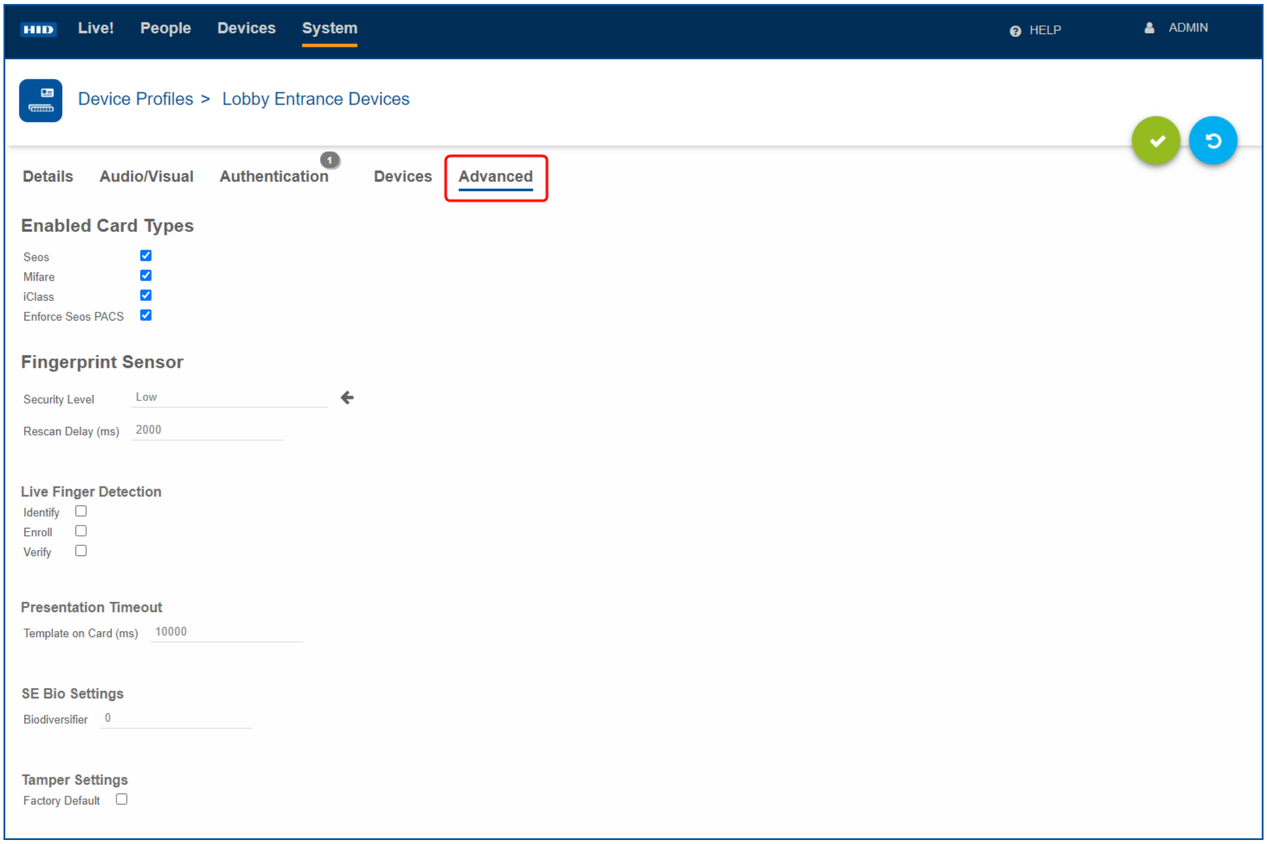
Name	Dates
Default Schedule	-
Schedule one	2019/01/22 - 2019/01/23

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.



Name	IP Address	Version
☑ RB25F-00068E100089	10.190.5.199	0.5.0.504

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.



Device Profiles > Lobby Entrance Devices

Enabled Card Types

- Seos ☑
- Mifare ☑
- iClass ☑
- Enforce Seos PACS ☑

Fingerprint Sensor

- Security Level: Low
- Rescan Delay (ms): 2000

Live Finger Detection

- Identify □
- Enroll □
- Verify □

Presentation Timeout

- Template on Card (ms): 10000

SE Bio Settings

- Biodiversifier: 0

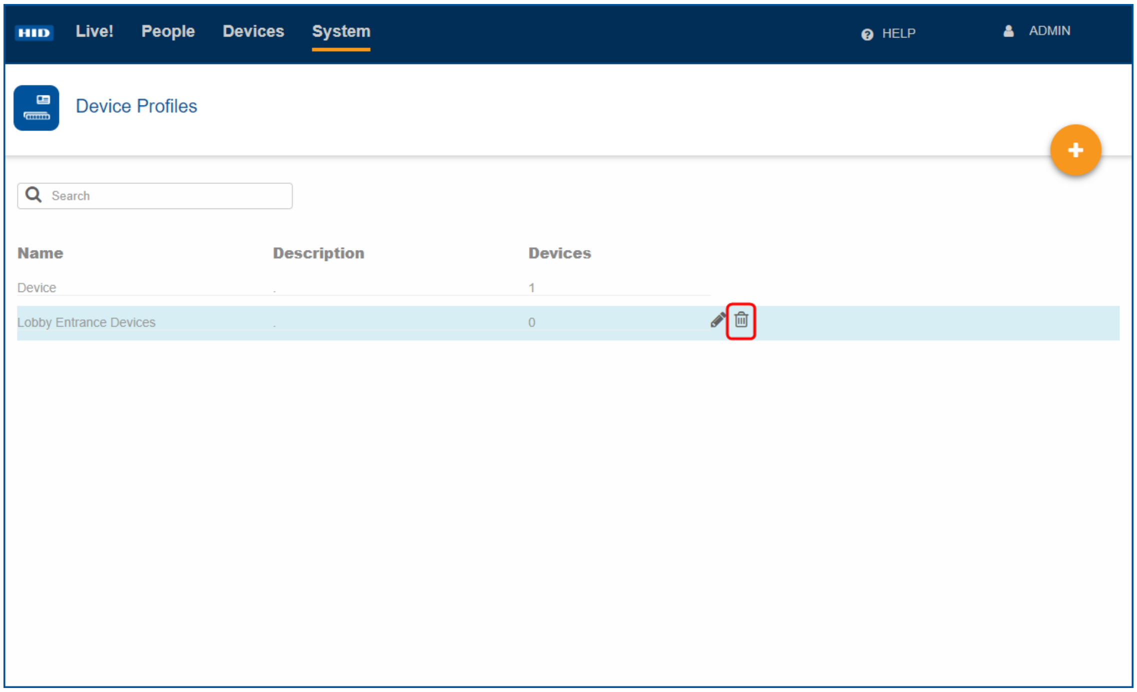
Tamper Settings

- Factory Default □

2.9.3 Delete a device profile

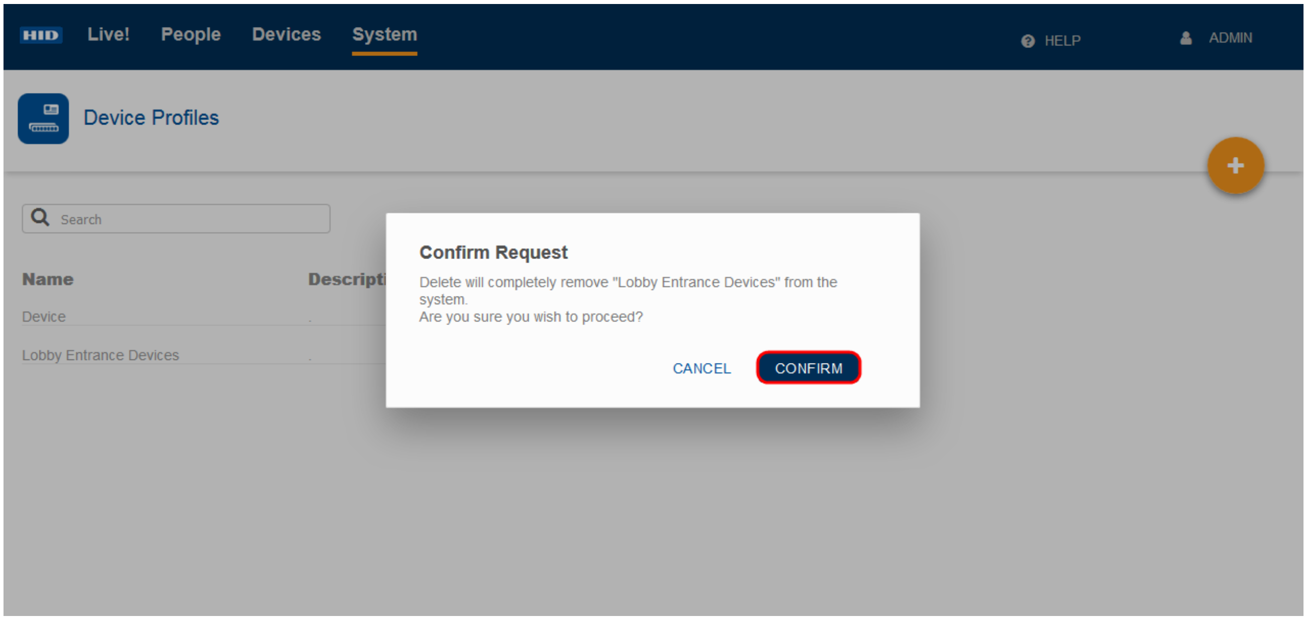
To delete a device profile:

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.



Name	Description	Devices
Device	.	1
Lobby Entrance Devices	.	0

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



Confirm Request

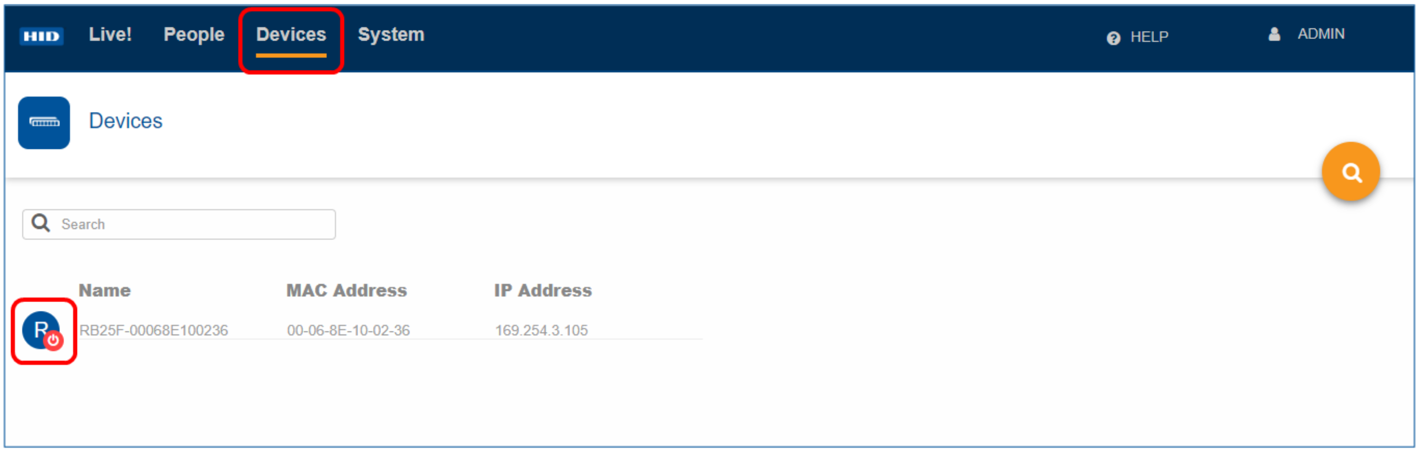
Delete will completely remove "Lobby Entrance Devices" from the system.
Are you sure you wish to proceed?

2.10 Device health indication

HID Biometric Manager displays the health status of connected devices in a live view on the **Device** page. There are four icons that indicate the device health.

Icon	Status	Definition
R 🟢⏻	High level communications in place and device ready.	The device is ready to be used and there are no issues.
R 🟠⏻	Low level communications only and the device can't be used.	The device has power and can be found through LAN or Ethernet but there is an operating error.
R 🔴⏻	No communications with device.	Communication has been lost between the device and HID Biometric Manager. The device has lost power or a tamper event has taken place.
R 🟠⇄	High level communications in place but device is busy.	Communication between the connected devices and HID Biometric Manager is stable but the device is experiencing a high level of usage.

The **Devices** page displays the real-time status for all connected devices.



Name	MAC Address	IP Address
RB25F-00068E100236	00-06-8E-10-02-36	169.254.3.105

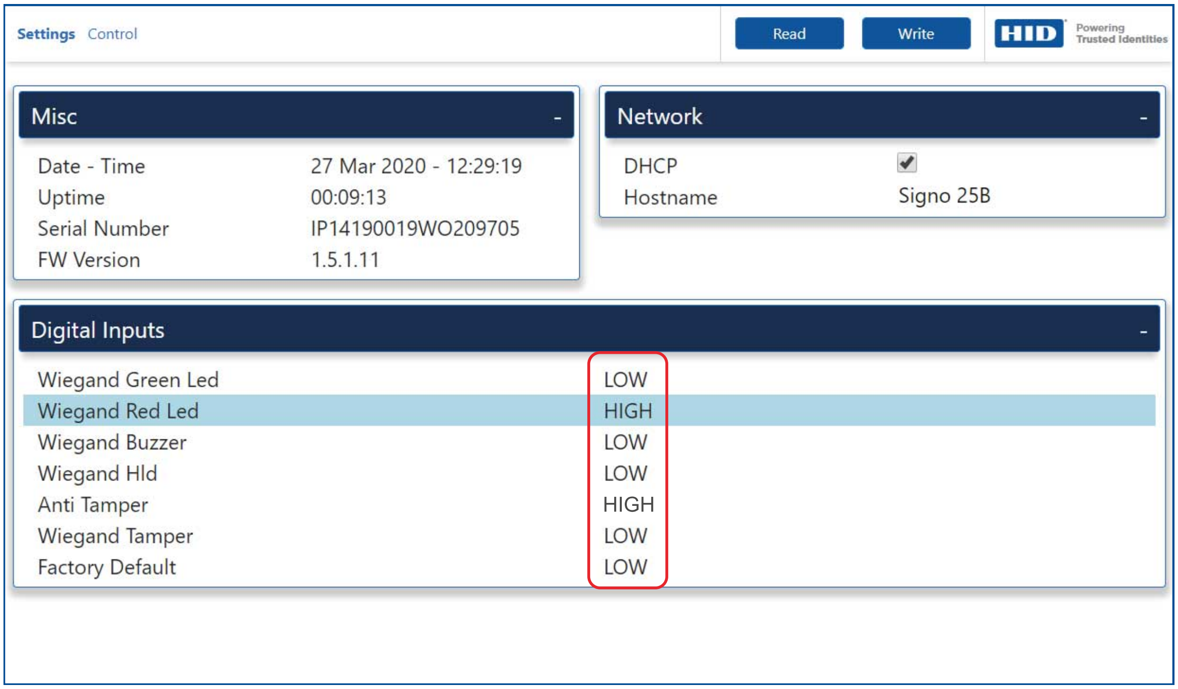
2.11 Device debug page

The device debug page provides a live view of the status of each input for the device and serves as a diagnostic tool during installation and operation.

To access the device debug page, search **http://<Device IP>:8888** in a Web browser.

The **Miscellaneous** window gives device information such as the running time, serial number and firmware version.

The **Digital Inputs** reading of **High** indicates that the input is in use or has been triggered. A short across the terminals on the rear of the device will result in the **Factory Default** input reading **High**.



Misc

Date - Time	27 Mar 2020 - 12:29:19
Uptime	00:09:13
Serial Number	IP14190019WO209705
FW Version	1.5.1.11

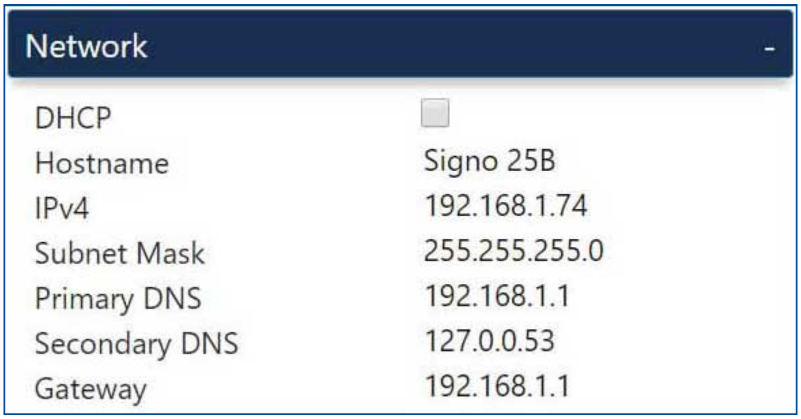
Network

DHCP	☑
Hostname	Signo 25B

Digital Inputs

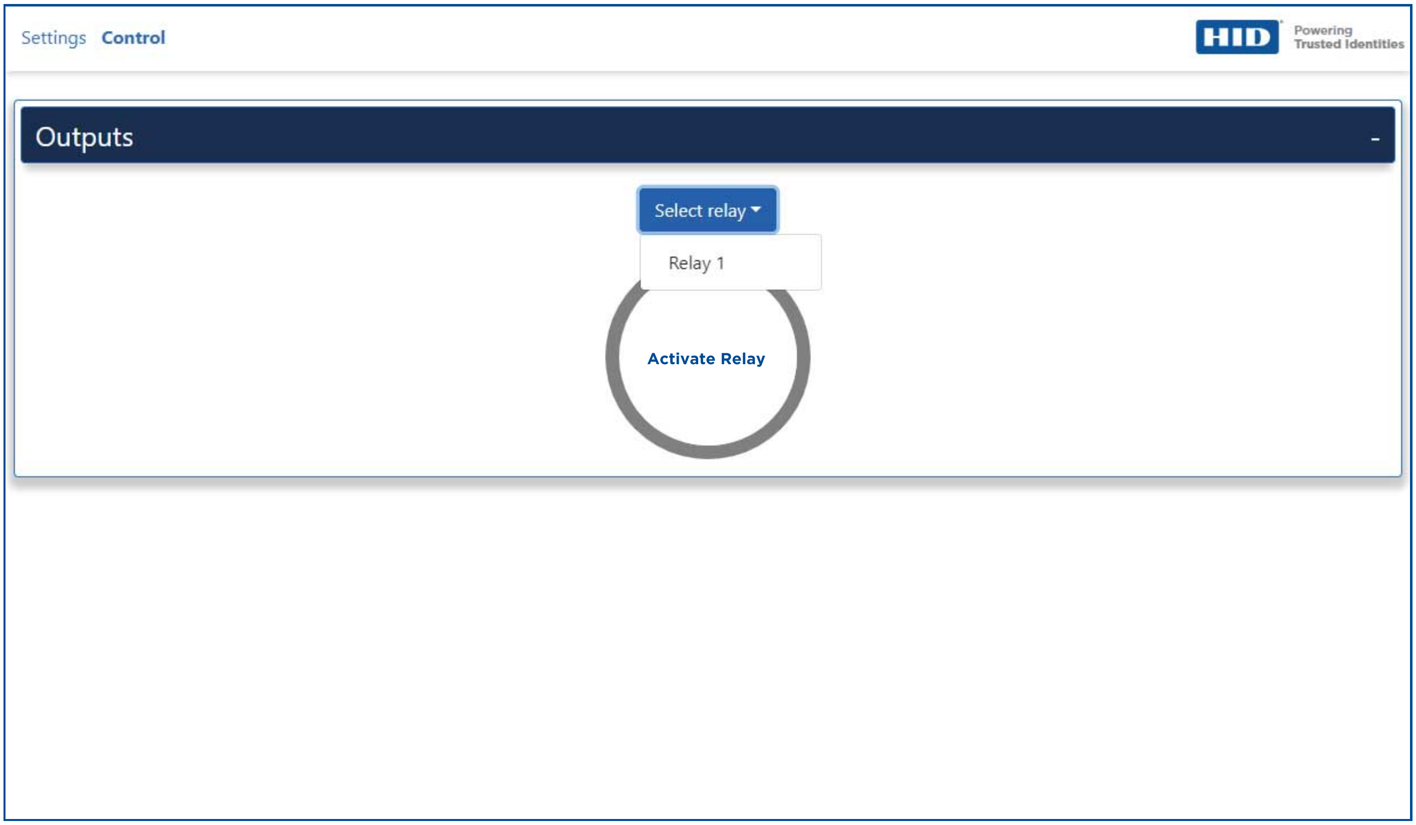
Wiegand Green Led	LOW
Wiegand Red Led	HIGH
Wiegand Buzzer	LOW
Wiegand Hld	LOW
Anti Tamper	HIGH
Wiegand Tamper	LOW
Factory Default	LOW

When the **DHCP** option under the **Network** window is toggled off, the **Network** window will expand. The details can be manually entered to suit the user.


Network

DHCP	☐
Hostname	Signo 25B
IPv4	192.168.1.74
Subnet Mask	255.255.255.0
Primary DNS	192.168.1.1
Secondary DNS	127.0.0.53
Gateway	192.168.1.1

Under the **Control** tab, a relay can be selected and activated to determine a connection through the device debug page. This is useful during the installation of the device. If the door strike is wired to the internal relay, it can be activated to confirm connection.



Note: The internal relay will toggle for 5 seconds.

2.12 Tamper settings

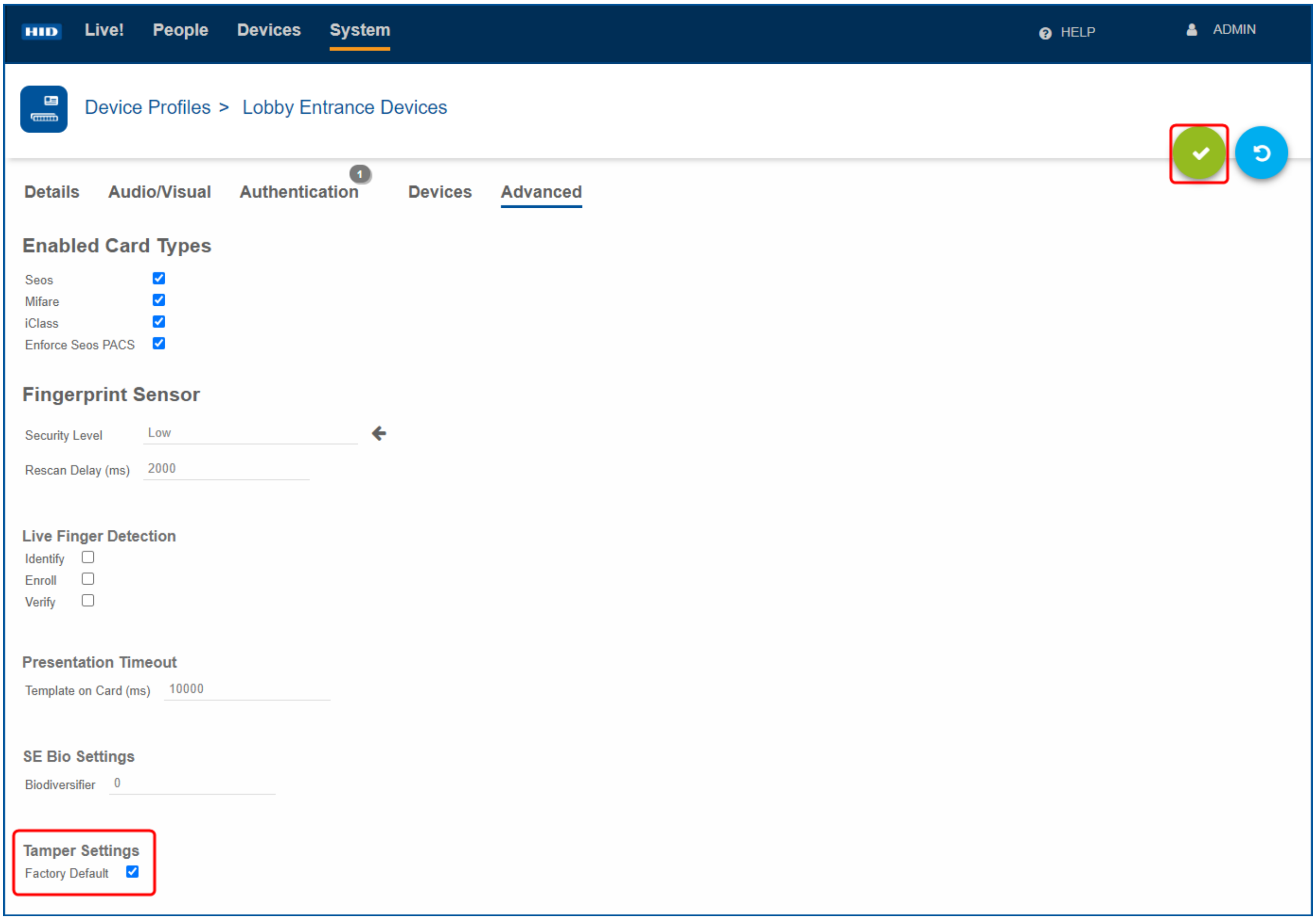
When any of the connected devices are removed from the casing or power is cut to the any of the connected devices, the **Factory Default** feature will trigger, resetting and rebooting to factory settings, clearing the connected devices of any stored Biometric templates and any connected devices configuration settings. The devices will not communicate with the HID Biometric Manager until it has been re-installed.

Note: The **Factory Default** feature is switched off by default.

In the case of an accidental tamper, where the device keeps power, a Tamper event will appear in the **Live!** view. The Device health will now be red.

To restore communications between the Device and HID Biometric Manager, the Device must be uninstalled from HID Biometric Manager and then re-installed.

To toggle the **Factory Default** setting on or off, on the **Device Profile** page and select the **Advanced** tab. Click **Save** to save the changes.



Enabled Card Types

Seos ☑
Mifare ☑
iClass ☑
Enforce Seos PACS ☑

Fingerprint Sensor

Security Level: Low
Rescan Delay (ms): 2000

Live Finger Detection

Identify ☐
Enroll ☐
Verify ☐

Presentation Timeout

Template on Card (ms): 10000

SE Bio Settings

Biodiversifier: 0

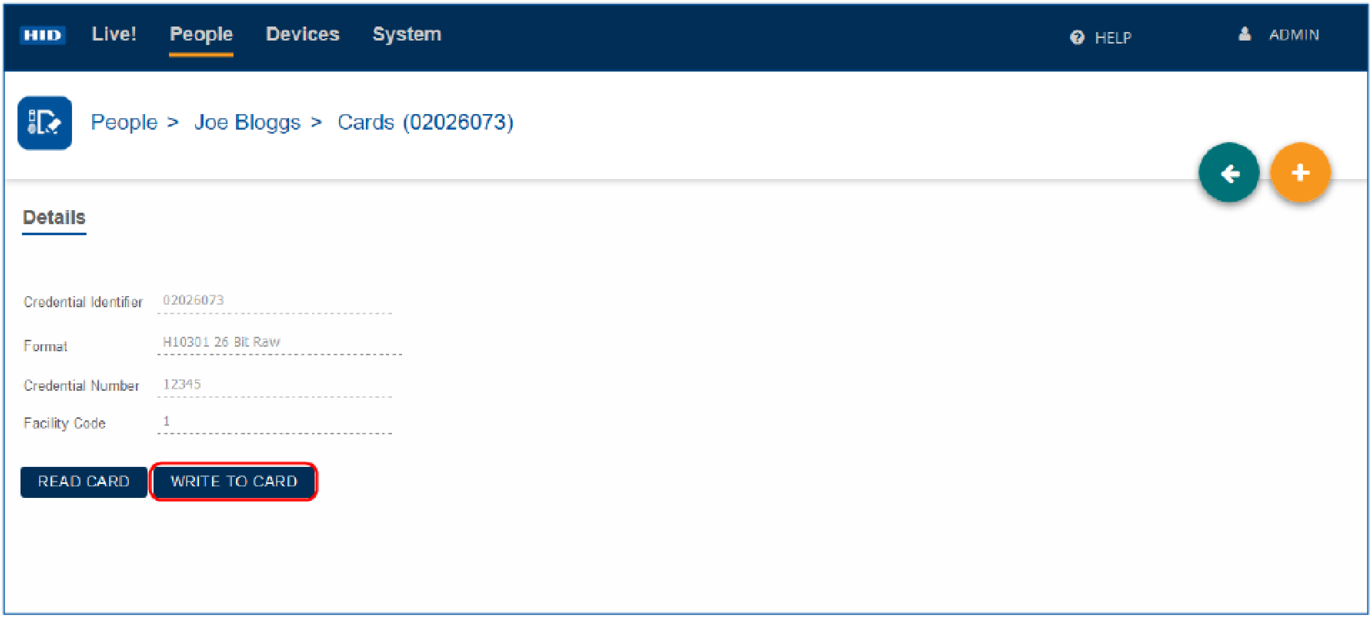
Tamper Settings

Factory Default ☑

2.13 Write fingerprint templates to a card

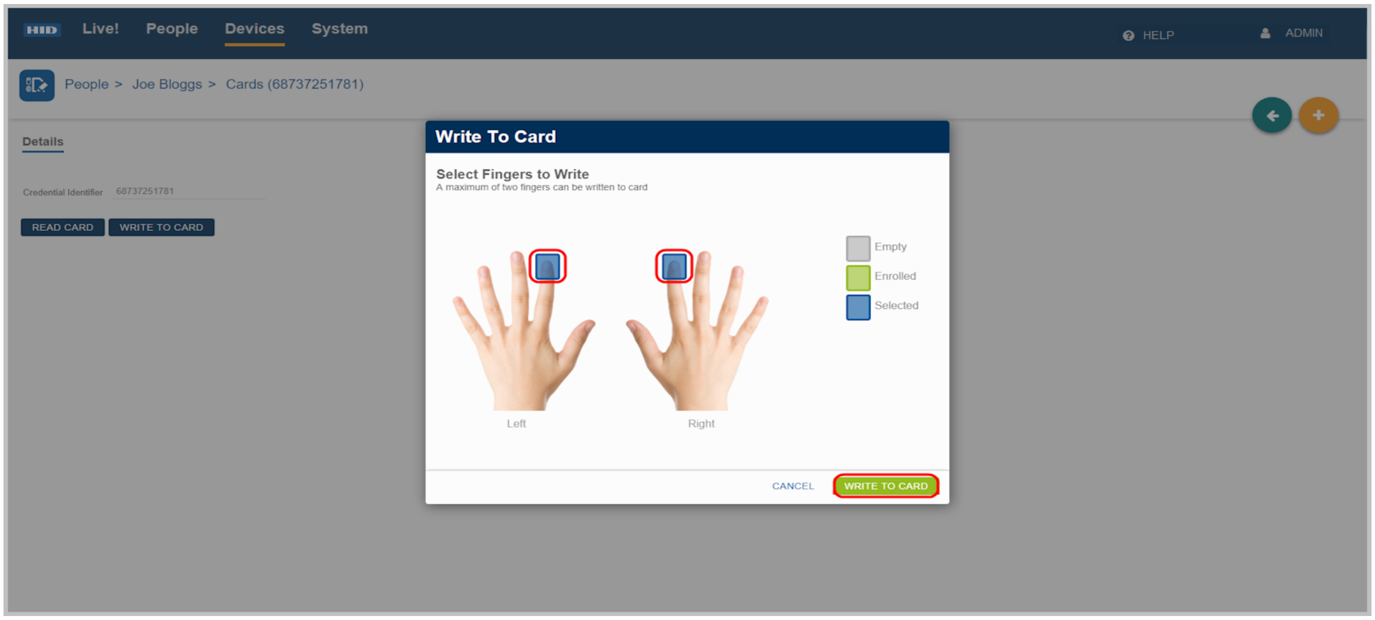
If you intend to make use of the **Template on Card** option as the authentication mode you will only be able to copy two fingerprint templates to the card.

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.



Credential Identifier 02026073
Format H10301 26 Bit Raw
Credential Number 12345
Facility Code 1

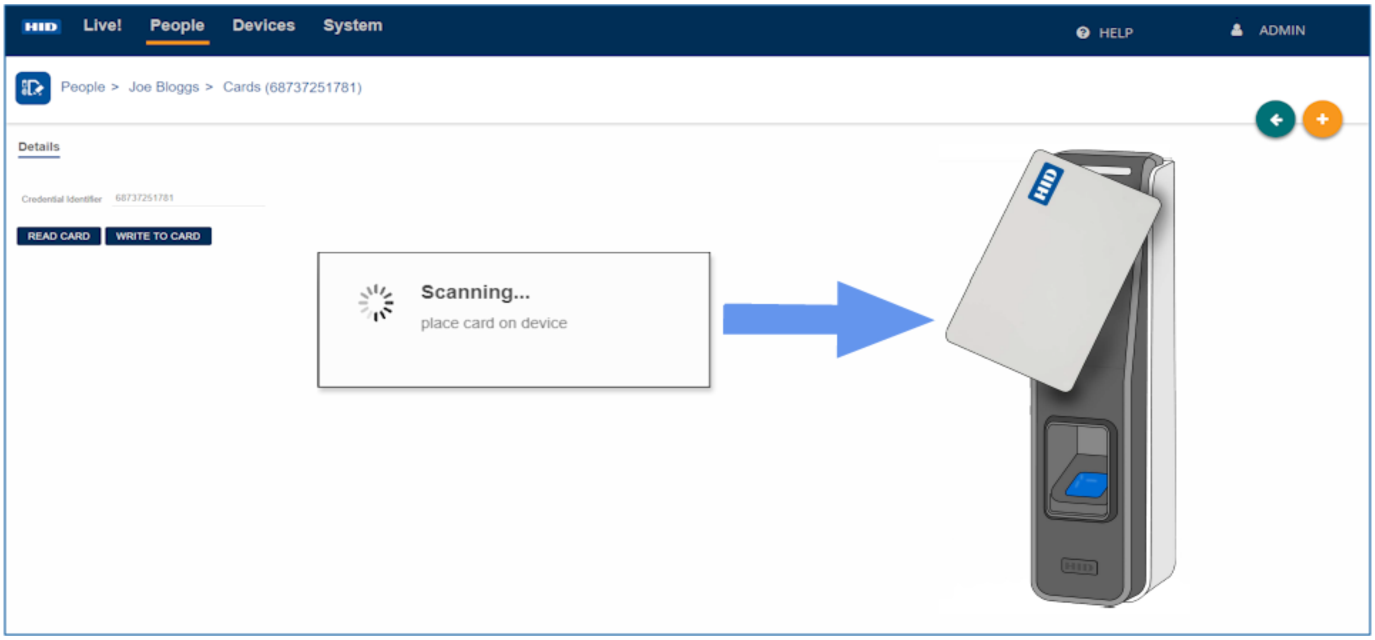
4. Select the fingers (maximum of two) you wish to be written to the card and click **WRITE TO CARD**.



Credential Identifier 68737251781

Select Fingers to Write
A maximum of two fingers can be written 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 it's default color.

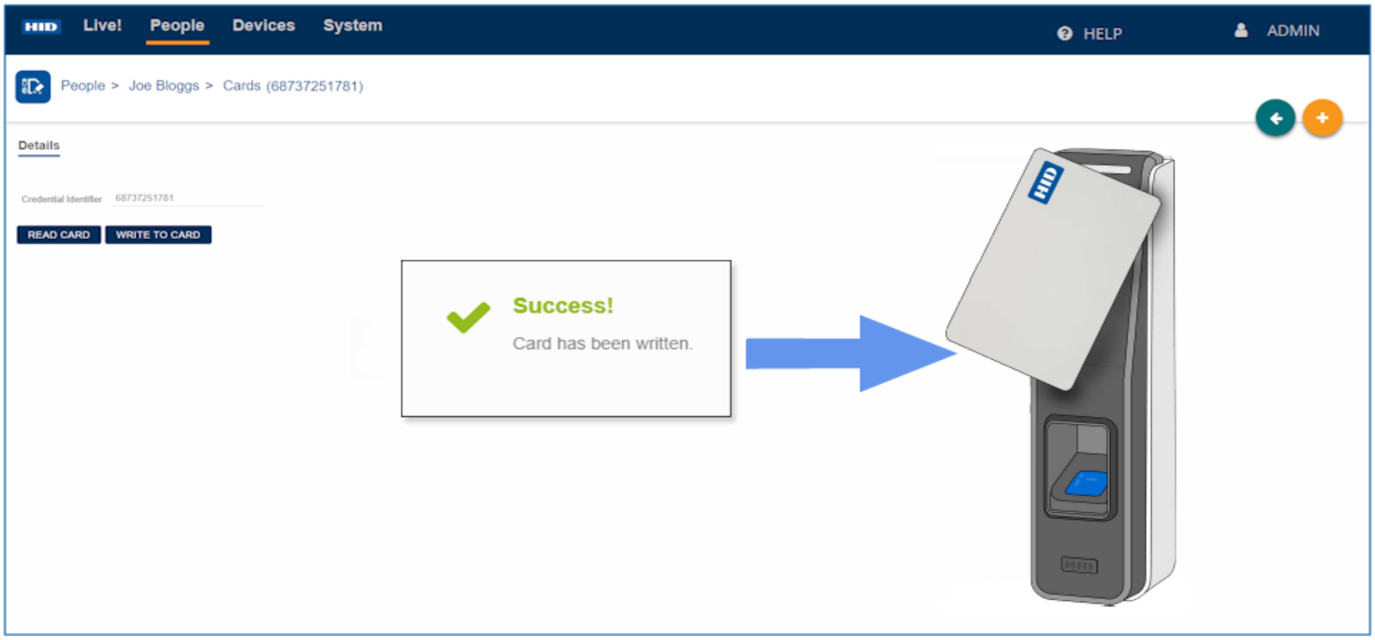


HID
Live!
People
Devices
System
HELP
ADMIN
People > Joe Bloggs > Cards (68737251781)
Details
Credential Identifier 68737251781
READ CARD
WRITE TO CARD
HID

Scanning...

place card on device

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



HID
Live!
People
Devices
System
HELP
ADMIN
People > Joe Bloggs > Cards (68737251781)
Details
Credential Identifier 68737251781
READ CARD
WRITE TO CARD
HID

Success!

Card has been written.

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.

2.14 Backup and recovery

This section explains how to backup the Microsoft SQL local Data Base (DB) used by HID Biometric Manager.

2.14.1 Generate recovery key

This section shows how to generate a recovery key on the original server.

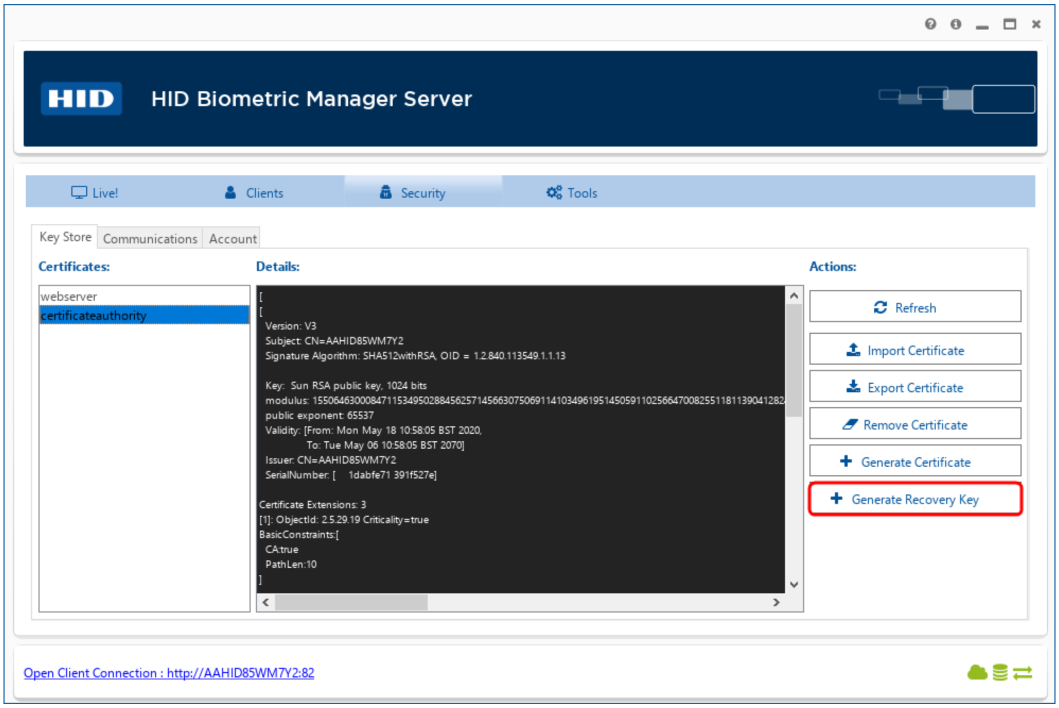
A new key is only required if:

- Clean install is performed
- After updating to SP2.2 and restarting the HBM server

Note: A recovery key only needs to be generated once per database instance.

Before commencing with the first database backup, a recovery key has to be generated as a single use key. To generate a recovery key from the HID Biometric Manager server and copy this to a safe location.

1. Open the **Security** tab and select **+ Generate Recovery Key**.



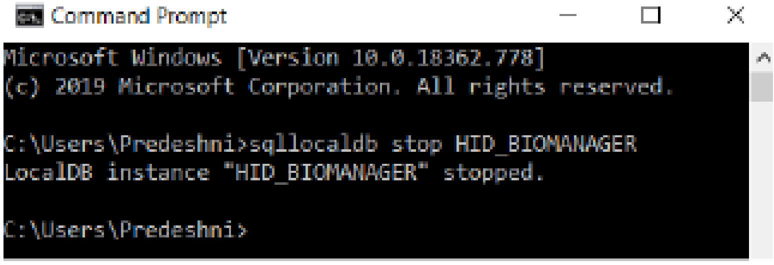
```
[
[
  Version: V3
  Subject: CN=AAHID85WM7Y2
  Signature Algorithm: SHA512withRSA, OID = 1.2.840.113549.1.1.13

  Key:  Sun RSA public key, 1024 bits
  modulus: 15506463000847115349502884562571456630750691141034961951450591102566470082551181139041282
  public exponent: 65537
  Validity: [From: Mon May 18 10:58:05 BST 2020,
               To: Tue May 06 10:58:05 BST 2070]
  Issuer: CN=AAHID85WM7Y2
  SerialNumber: [    1dabfe71 391f527e]

Certificate Extensions: 3
[1]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
  CA:true
  PathLen:10
]
```

2. The **Recovery Key Generator** window is displayed. Click **Generate Key**.
3. Click **OK** once the Recovery Key message appears then close that window.
4. Copy and save the generated recovery key to a text document and save to multiple secure machines or locations other than the HBM server.

2.14.2 Backup procedure

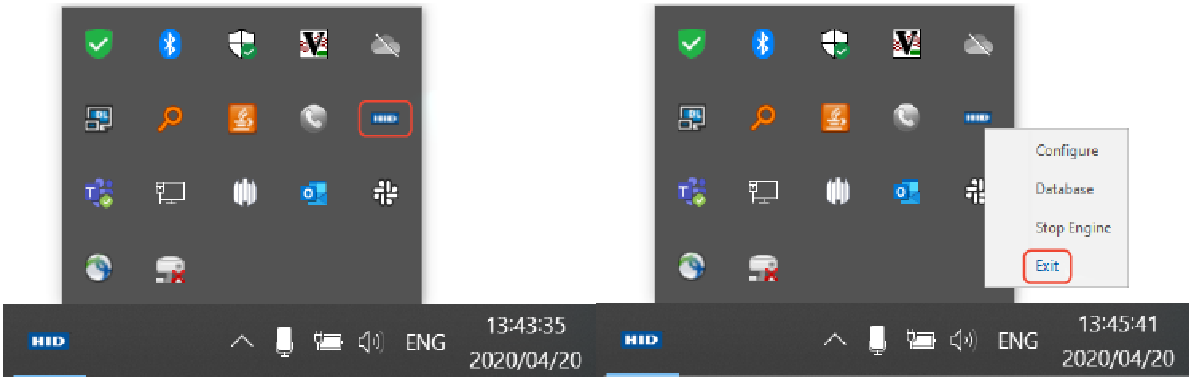
The following shows the backup procedure on the original server.

1. Stop the SQL local database by opening a command prompt and typing **SQLLOCALDB STOP HID_BIOMANAGER**.



```
Microsoft Windows [Version 10.0.18362.778]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\Predeshni>sqllocaldb stop HID_BIOMANAGER
LocalDB instance "HID_BIOMANAGER" stopped.

C:\Users\Predeshni>
```

2. Stop HBM in the Windows system tray.

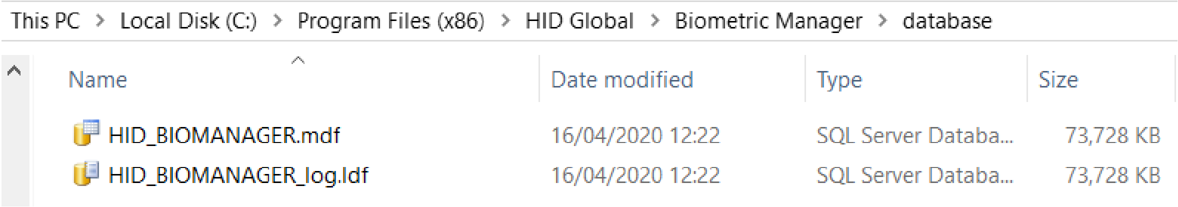


3. Copy the **HID_BIOMANAGER.mdf** and **HIDBIOMANAGER_log.ldf** files from **C:\Program Files (x86)\HID Global\Biometric Manager\database** to a secure location.
   - Backup daily or weekly.
   - Store backups on a secure machine separate to the HBM server.
4. The backup is now complete. It is now safe to start up HBM if no recovery procedure is needed.

2.14.3 Restore procedure

The restore procedure takes place on the recovery server.

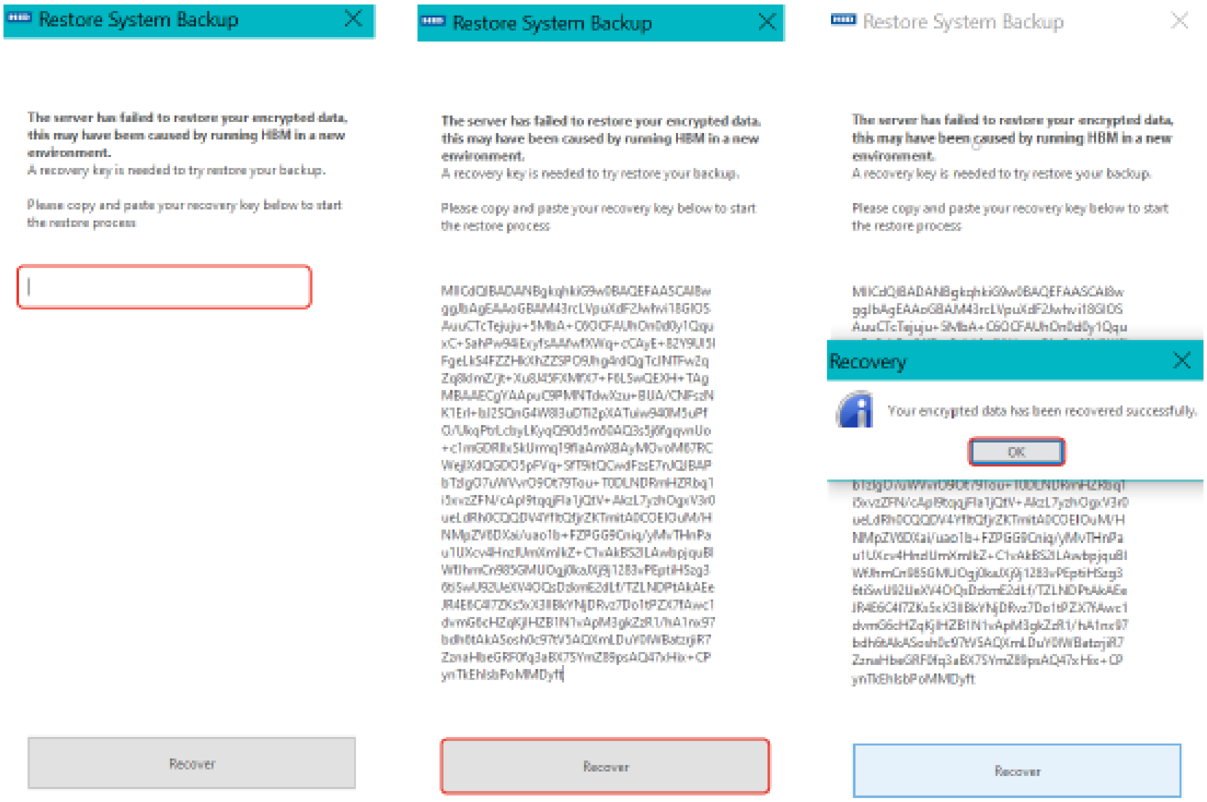
1. Ensure that the original server is not on the network, or that HBM has been uninstalled and is no longer used on the original server.
2. Ensure the SQL server version on the recovery machine is the same or a higher version than the original server. The SQL local database version installed by HBM is based on the current version of SQL server installed.
3. Install HID Biometric Manager but do not start it.
4. Copy and paste the previously back up **.mdf** and **.ldf** files to **C:\Program Files (x86)\HID Global\Biometric Manager\database**.



This PC > Local Disk (C:) > Program Files (x86) > HID Global > Biometric Manager > database

Name	Date modified	Type	Size
HID_BIOMANAGER.mdf	16/04/2020 12:22	SQL Server Databa...	73,728 KB
HID_BIOMANAGER_log.ldf	16/04/2020 12:22	SQL Server Databa...	73,728 KB

5. Launch HBM. The recovery key will need to be entered:
   a. Paste the recovery key in the field
   b. Click **Recover**
   c. On successful recovery, click **OK**



The server has failed to restore your encrypted data, this may have been caused by running HBM in a new environment.

A recovery key is needed to try restore your backup.

Please copy and paste your recovery key below to start the restore process

The server has failed to restore your encrypted data, this may have been caused by running HBM in a new environment.

A recovery key is needed to try restore your backup.

Please copy and paste your recovery key below to start the restore process

MIICdQIBADANBgkqhkiG9w0BAQEFAASCAl8w
ggJbAgEAAoGBAM43rcLVpuXdFZwhvi18GIOS
AuuCTcTejuju+5MbA+C6OCFAUhOn0d0y1Qqu
xC+5ahPw94IExyfsAAfwfXWq+cCAyE+82Y9UI5I
FgeLkS4FZZHkXhZZSPO9Jhg4rdQgTcINTFw2q
Zq8dmZ/jt+Xu8J45FXMfX7+F6L5wQEXH+TAg
MBAAECgYAApuC9PMNTdwXzu+BUA/CNFszN
K1Erl+bI25QnG4W8I3uDTi2pXATuiw940M5uPf
O/UkqPtrLcbyLKyqQ90d5m80AQ3s5j0fgqvnUo
+c1mGDRlIx5kUmq19flaAmXBAyMOvoM67RC
WejIXdQGDO5pFVq+SfT9itQCwdFzsE7nJQJBAP
bTdgO7uWVvrO9Ot79Tou+T0DLNDRmHZRbq1
i5xvzZFN/cApI9tqqjFla1jQtV+AkzL7yzhOgxV3r0
ueLdRh0CQQDV4YftQfjrZKTmitA0COEIOuM/H
NMpZV6DXai/uao1b+FZPGG9Cniq/yMvTHnPa
u1UXcv4HnzlUmXmlkZ+C1vAkBS2lLAwbpjquBI
WtIhmCn98SGMUOgj0kaJXj9j1283vPEptiHSzg3
6tiSwU92UeXV4OQsDdkmE2dLf/TZLNDPtAkAEe
JR4E6C4I7ZKs5xX3IIBkYNjDRvz7Do1tPZX7fAwc1
dvmG6cHZqKjIHZB1N1vApM3gkZzR1/hA1nx97
bdh6tAkASosh0c97tV5AQXmLDuY0WBatzrjR7
ZznaHbeGRF0fq3aBX75YmZ89psAQ47xHix+CP
ynTkEhlsbPoMMDyft

The server has failed to restore your encrypted data, this may have been caused by running HBM in a new environment.

A recovery key is needed to try restore your backup.

Please copy and paste your recovery key below to start the restore process

MIICdQIBADANBgkqhkiG9w0BAQEFAASCAl8w
ggJbAgEAAoGBAM43rcLVpuXdFZwhvi18GIOS
AuuCTcTejuju+5MbA+C6OCFAUhOn0d0y1Qqu
i5xvzZFN/cApI9tqqjFla1jQtV+AkzL7yzhOgxV3r0
ueLdRh0CQQDV4YftQfjrZKTmitA0COEIOuM/H
NMpZV6DXai/uao1b+FZPGG9Cniq/yMvTHnPa
u1UXcv4HnzlUmXmlkZ+C1vAkBS2lLAwbpjquBI
WtIhmCn98SGMUOgj0kaJXj9j1283vPEptiHSzg3
6tiSwU92UeXV4OQsDdkmE2dLf/TZLNDPtAkAEe
JR4E6C4I7ZKs5xX3IIBkYNjDRvz7Do1tPZX7fAwc1
dvmG6cHZqKjIHZB1N1vApM3gkZzR1/hA1nx97
bdh6tAkASosh0c97tV5AQXmLDuY0WBatzrjR7
ZznaHbeGRF0fq3aBX75YmZ89psAQ47xHix+CP
ynTkEhlsbPoMMDyft

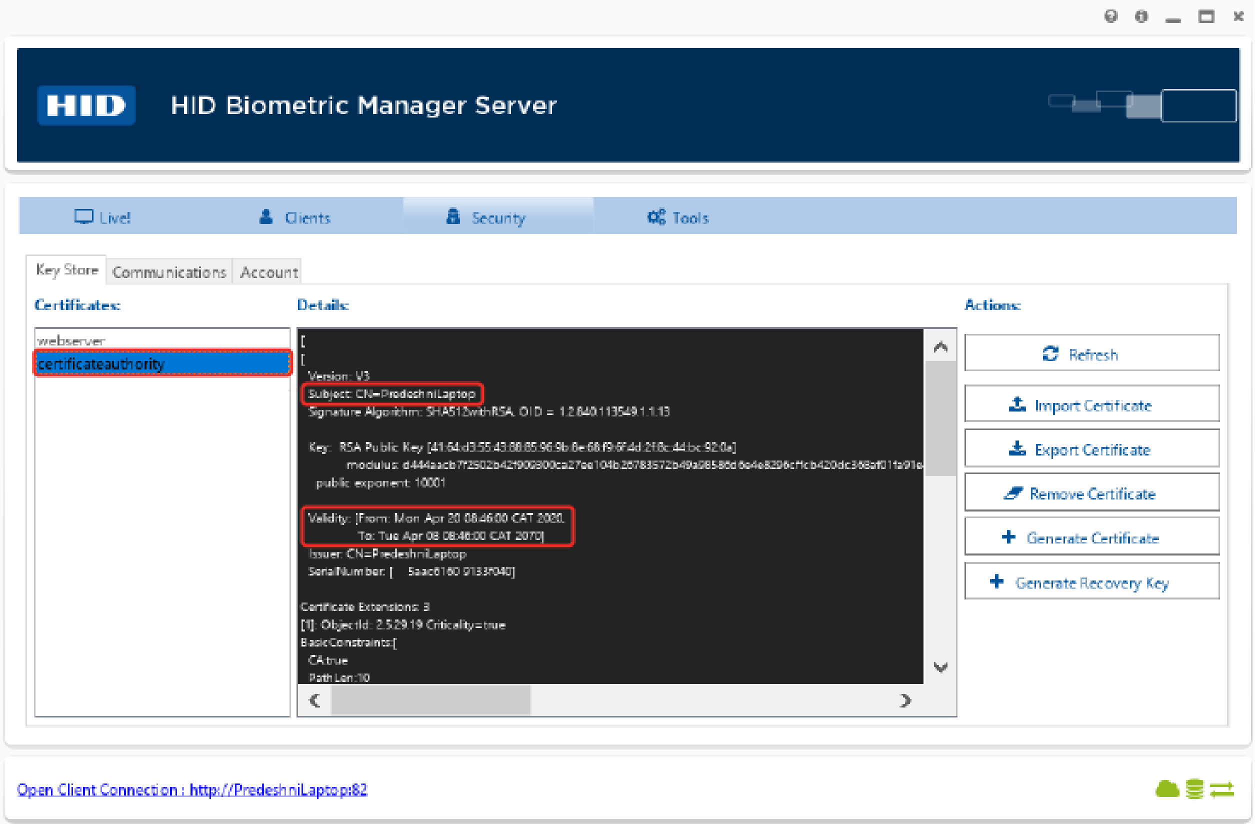
Your encrypted data has been recovered successfully.

6. Once started, check that the recovery process has created a new certificate with the recovery server information and not the original server information. This can be verified through the HID Biometric Manager Server window.

   a. Open the **Security** tab.

   b. Under the **Key Store** tab and select **certificateauthority** and in the **Details** window, verify the following:

- **Subject CN** and **Issuer CN** must be the host name of the recovery server.
- Check the **Validity** field and make sure the date and time reflects the date and time around the current install of HBM on the recovery server .
- Under section **Subject Alternative Name**, make sure the IP addresses belong to the recovery server.



```
[
[
  Version: V3
  Subject: CN=PredeshniLaptop
  Signature Algorithm: SHA512withRSA, OID = 1.2.840.113549.1.1.13

  Key:  RSA Public Key [41:64:d3:55:43:88:85:96:9b:8e:68:f9:6f:4d:21:8c:44:bc:92:0a]
            modulus: d444aacb7f2502b42f909300ca27ee104b26783572b49a98586d6e4e8296cffcb420dc368af01fa91e
    public exponent: 10001

  Validity: [From: Mon Apr 20 08:46:00 CAT 2020,
               To: Tue Apr 08 08:46:00 CAT 2070]
  Issuer: CN=PredeshniLaptop
  SerialNumber: [    5aac6160 9133f040]

Certificate Extensions: 3
[1]: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
  CA:true
  PathLen:10
```

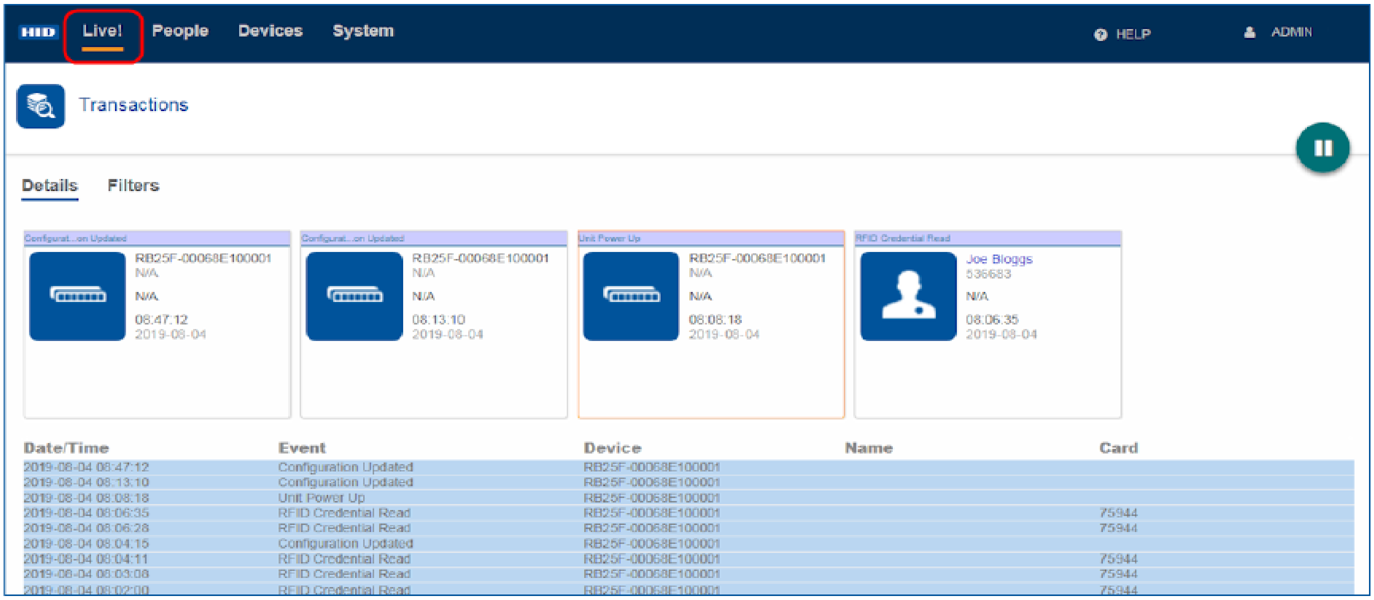
8. Log into HBM and uninstall all connected devices. Do not **Factory Default**.
9. Factory default all devices using the pins on the reverse of the unit, see *HID iCLASS SE RB25F User Guide* (PLT-04900).
10. Wait one minute for devices to reboot after factory default.
11. Re-install all devices within HBM.
12. Test the communication between devices and HBM.

2.15 System monitoring and Reports

2.15.1 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.

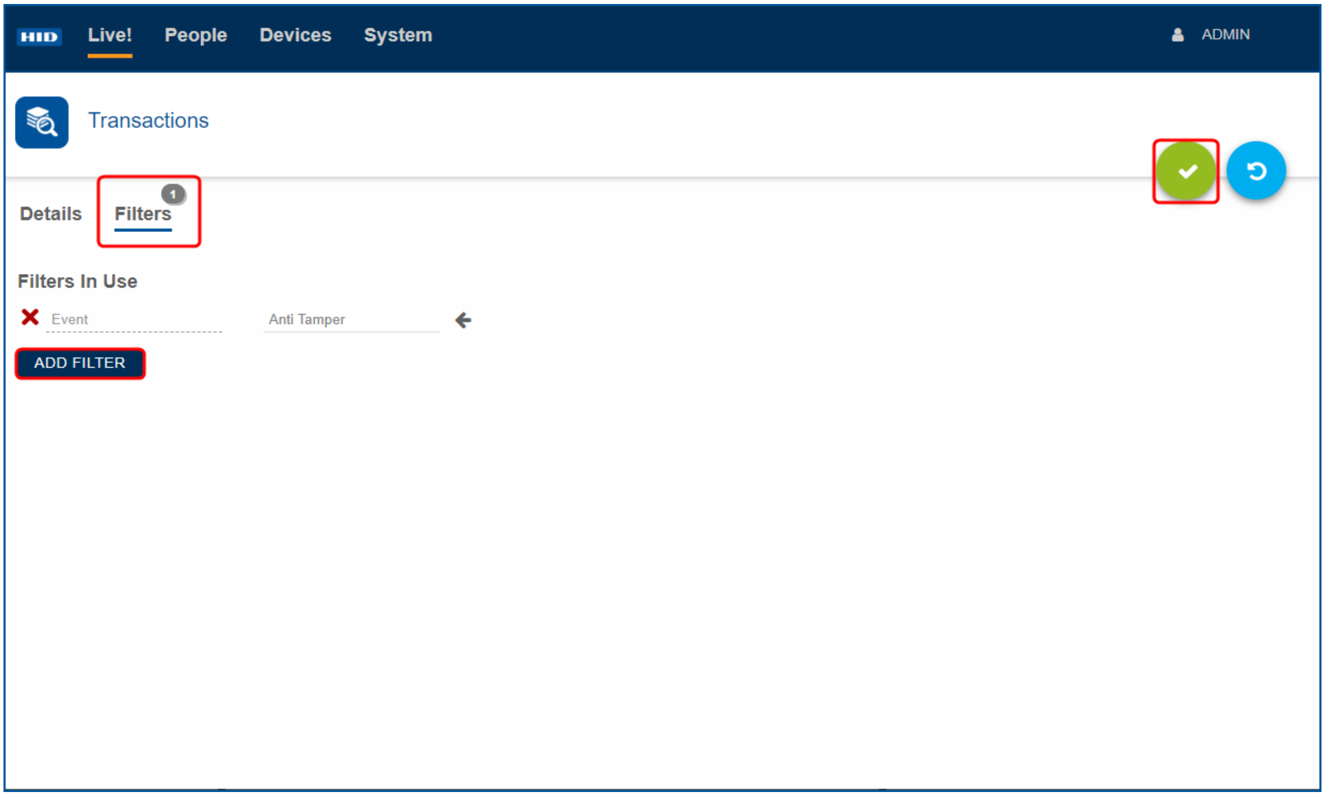
Note: Event information is only displayed after a device has been added.



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		75944
2019-08-04 08:06:28	RFID Credential Read	RB25F-00068E100001		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.

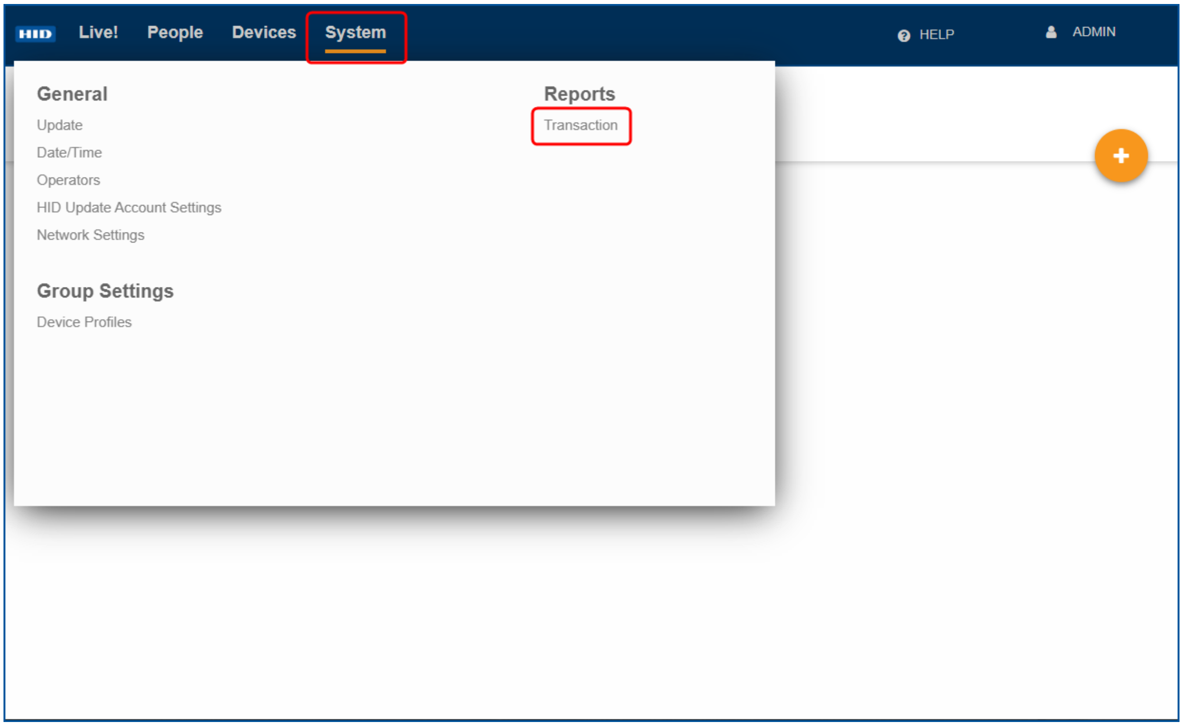


Filters In Use

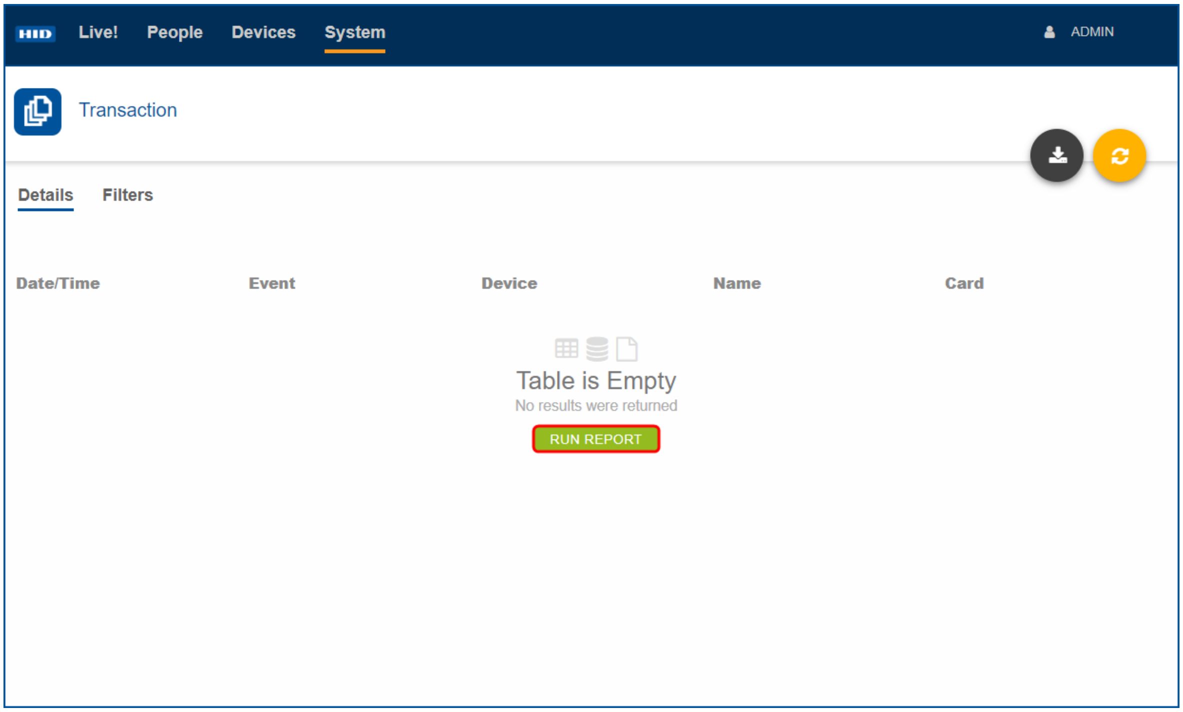
Event Anti Tamper

2.15.2 Transaction Reports

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

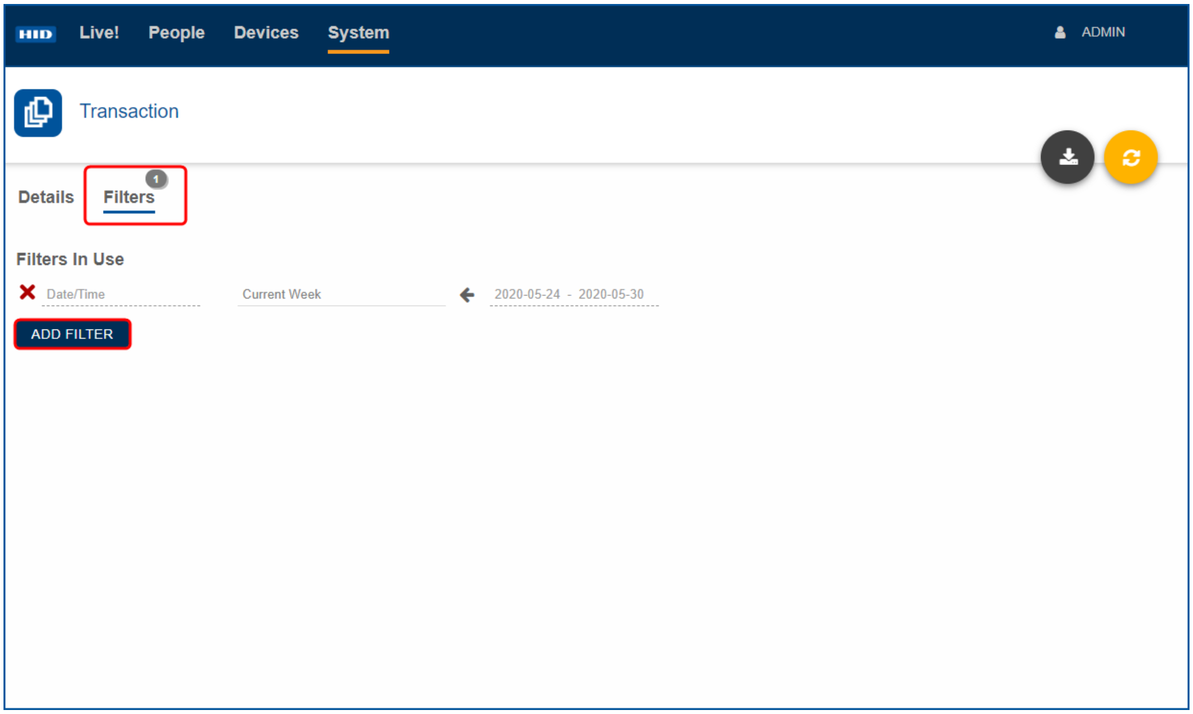


Click **RUN REPORT** to create a report of HID Biometric Manager transactions. Once the report is created click the save report icon [⬇] to save the report to a PDF or CSV file.



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

Biometric Manager Mobile Access setup

Powering
Trusted Identities

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 how to verify HID Reader Manager™ Technician account details in Biometric Manager and how to load HID 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 Origo® Portal HID Mobile Access Portal and creates a primary account administrator. For detailed information on the onboarding process visit the onboarding site at:

https://managedservices.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

At the customers request, 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 Origo Port and 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:

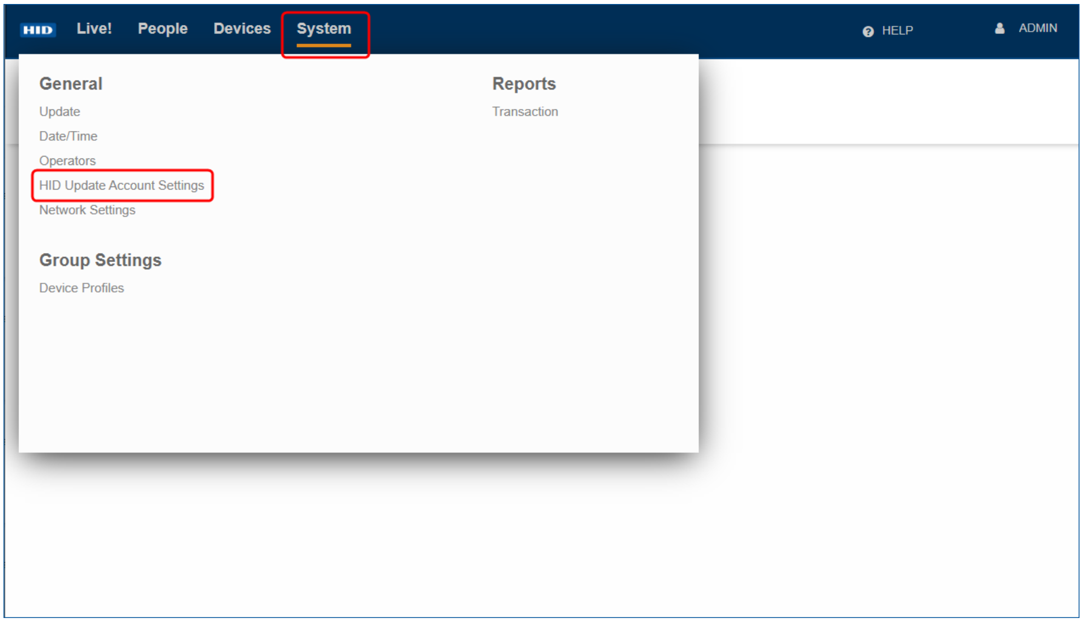
- *HID Mobile Access Frequently Asked Questions* (PLT-02085).
- *HID Mobile Access App User Guide* (PLT-02077).

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

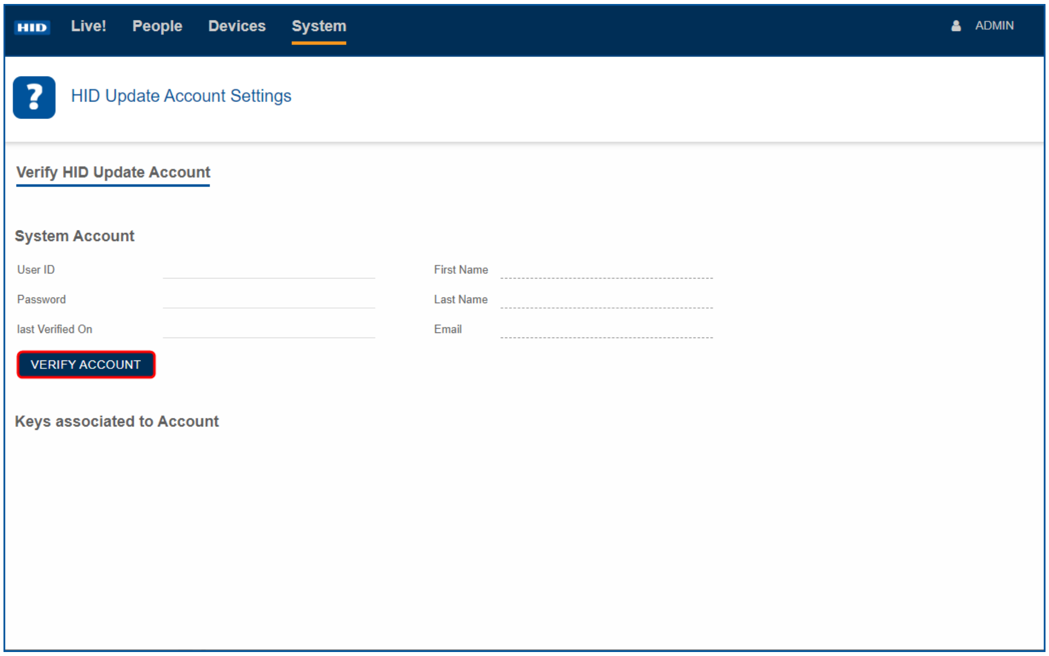
In order to validate a Reader Manager Technician account in HID Biometric Manager an active Reader Manager Technician account must be present, see **HID Reader Manager setup**.

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 Update Account Settings**.



3. On the **HID Update 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**.



HID Update Account Settings

Verify HID Update Account

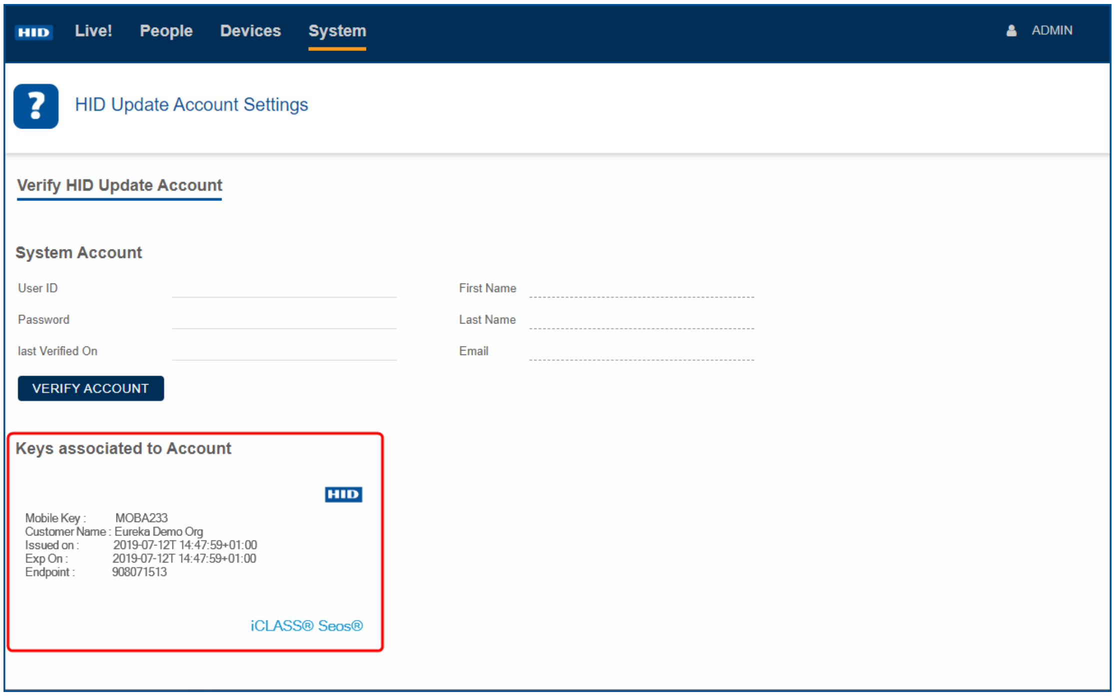
System Account

User ID
Password
last Verified On
First Name
Last Name
Email

VERIFY ACCOUNT

Keys associated to 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 Update Account Settings

Verify HID Update Account

System Account

User ID

Password

last Verified On

First Name

Last Name

Email

Keys associated to Account

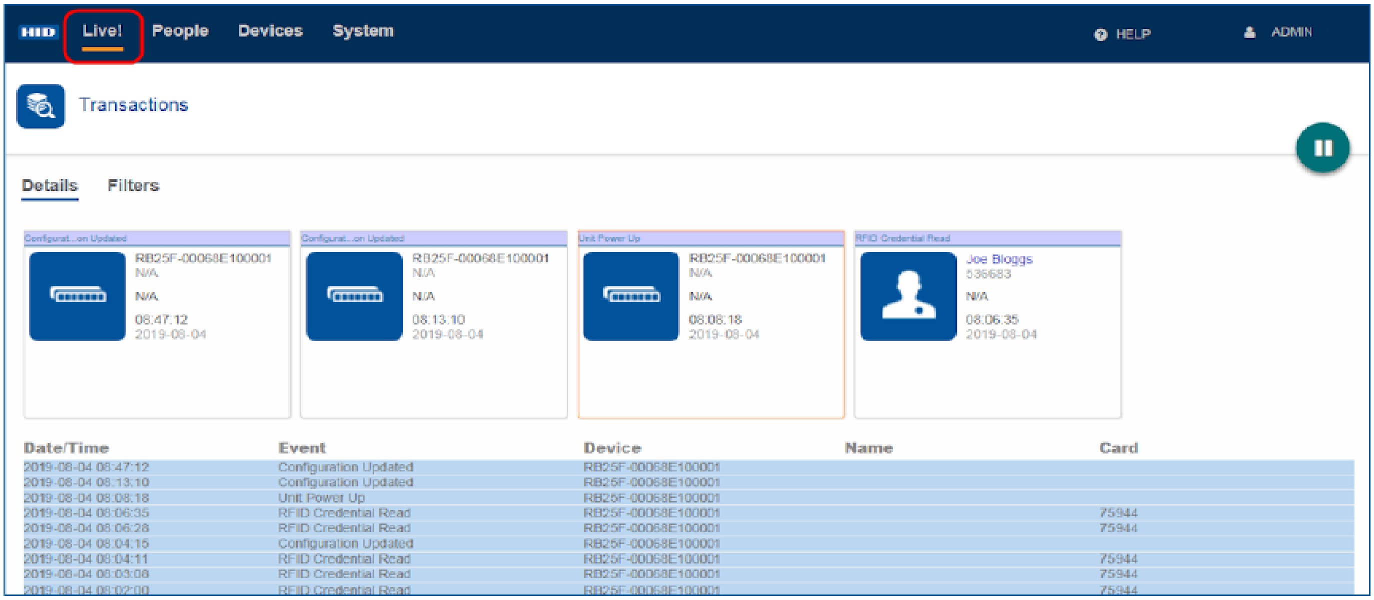
Mobile Key : MOBA233
Customer Name : Eureka Demo Org
Issued on : 2019-07-12T 14:47:59+01:00
Exp On : 2019-07-12T 14:47:59+01:00
Endpoint : 908071513

A.3 Test MOB keys are working correctly

As a prerequisite to test that a MOB key working correctly, the Origo Portal or 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 **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.



Configurat...on Updated
RB25F-00068E100001
N/A
N/A
08:47:12
2019-08-04

Configurat...on Updated
RB25F-00068E100001
N/A
N/A
08:13:10
2019-08-04

Unit Power Up
RB25F-00068E100001
N/A
N/A
08:08:18
2019-08-04

RFID Credential Read
Joe Bloggs
536683
N/A
08:06:35
2019-08-04

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		75944
2019-08-04 08:06:28	RFID Credential Read	RB25F-00068E100001		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**

Fingerprint template encryption

Powering
Trusted Identities

In-field update for existing installations

1. Update the HID Biometric Manager software to software version 1.0.1103.59811.
2. Update the firmware of each RB25F device connected to the HID Biometric Manager.
3. After updating the RB25F devices, each device must be reset to their factory default state. See **Reset a device**
4. Uninstall each RB25F device from within HID Biometric Manager and re-install them.

Note: Steps 3 and 4 ensure a clean move to SP2.1.

Note: The device profile will sync to make sure all the reader configuration is downloaded to the RB25F device after re-installation and once connection has been established with the HID Biometric Manager.

New installations

1. Verify that the HID Biometric Manager software is at version 1.0.1103.59811, and RB25F is at firmware version 1.5.1.22.
2. If required, update the devices firmware and software to the latest version.

Note: As this is a new install, the device configuration can be done after verification. If required, update the device firmware.

Additional information on the RB25F template encryption

- All RB25F units have been shipped with Identrust x509 certificates which are used as part of the Biometric template encryption feature.
- The HID Biometric Manager server application will generate an AES-256 encryption key to be used as part of the template encryption feature.
- There is no need to enter any additional information or setup other than running the update.

After the RB25F has been updated with the new firmware level for SP2.1, and the RB25F has gone through a re-install process, it must connect with the HID Biometric Manager in order for the encryption key to be sent to the RB25F. There are two important points of note:

1. Once the update is complete, the device will only allow **Template on Device Authentication** until the AES-256 encryption keys are sent from the HID Biometric Manager. If the authentication mode was set to **Finger Only** or **Finger + Card** the device will need to make a connection with the HID Biometric Manager to receive the MOB keys before it can become fully operational.
2. As part of SP2.1 the AES-256 encryption keys are not backed up. If the computer that the HID Biometric Manager is running on is destroyed, it is not possible to recover them. This will be addressed in a future update.

Appendix C

Acronyms and terminology

Powering
Trusted Identities

Term	Definition
Authentication Mode (RB25F)	**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. **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. **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). **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). 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.
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.
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

Term	Definition
	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
June 2020	Updates to support HID Biometric Manager Service Pack 2.2 (RB25F Reader Firmware Version 1.5.1.22 and HID Biometric Manager Software Version 1.0.1103.59811)	A.4
December 2019	Updates to support HID Biometric Manager Service Pack 2.1 (RB25F Reader Firmware Version 1.5.0.86 and HID Biometric Manager Software Version 1.0.886.57608)	A.3
September 2019	Updates to support RB25F Service Pack 1 (RB25F Reader Firmware Version 1.5.0.82 and HID Biometric Manager Software Version 1.0.774.56514)	A.2
June 2019	Minor update to Section 3.2.1 HID Biometric Manager software install.	A.1
February 2019	Initial release.	A.0

Powering
Trusted Identities

PLT-04029, A.4

Americas & Corporate
611 Center Ridge Drive
Austin, TX 78758
USA

Support: 866-607-7339
Fax: 949-732-2120

Asia Pacific 19/F
625 King's Road
North Point
Island East
Hong Kong

Support: 852-3160-9833
Fax: 852-3160-4809

Europe, Middle East & Africa
3 Cae Gwyrdd,
Green Meadow Springs,
Cardiff,
United Kingdom,
CF15 7AB
Support: +44 (0) 2920 528 500

Brazil
Condomínio Business Center
Av. Ermano Marchetti, 1435
Galpão A2 - CEP 05038-001
Lapa - São Paulo / SP, Brazil

Phone: +55 11 5514-7100