HID® Biometric Manager™

Administration Guide

PLT-04029, B.2
October 2021

Copyright

Trademarks

Contacts

For technical support, please visit: **https://support.hidglobal.com**.

What's new

Date	Description	Revision
October 2021	Updates to support HID Biometric Manager version 1.0.1550.62511.	B.2

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

Section 01

Introduction

1.1 Document purpose

The document provides procedures for administrations to install and setup HID® Biometric Manager™ and procedures for HID Biometric Manager (HBM) operators to carry out tasks associated with HID® Signo™ Biometric Reader and Controller 25B installation, people enrollment, and credential/biometric data management.

HID Global is bringing the iCLASS SE® RB25F into the Signo™ family of readers and rebranding it as the HID Signo Biometric Reader 25B.

The Signo Biometric Reader 25B is launched with HBM version 1.0.1212.60729 and is available as an update for iCLASS SE RB25F customers.

Note: Unless specified, all HBM version 1.0.1103.59811 features are available for iCLASS SE RB25F customers. The features not compatible with the iCLASS SE RB25F will be called out explicitly throughout the document.

For more information on the Signo Biometric Reader 25B device, refer to *HID Signo Biometric Reader 25B 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 Signo Biometric Reader 25B devices, enroll people in the system, add credentials and biometric data.
- **HID Signo Biometric Reader 25B Biometric Reader installers:** The document provides information relating to the Signo Biometric Reader 25B, including the wiring specification and wiring options.

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 App User Guide (PLT-02077)	Installation, configuration, and use of the HID Mobile Access App for iOS and Android devices.

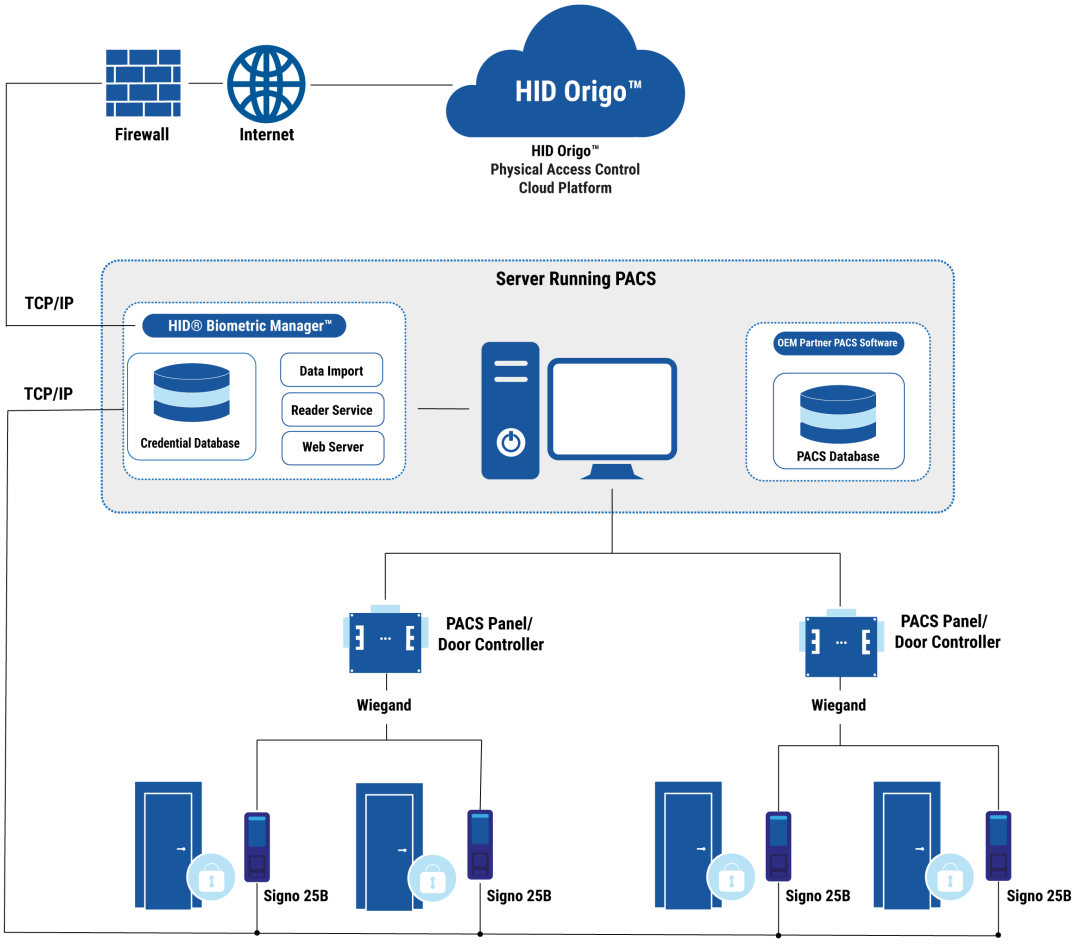
1.4 Physical Access Control System overview

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 Signo Biometric Reader 25B 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 Signo Biometric Reader 25B 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 deployed in 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 Signo Biometric Reader 25B devices and PACS Panel/Door Controllers can be added. HID Biometric Manager can control up to 2,000 Signo Biometric Reader 25B devices.



1.5 HID Biometric Manager server application

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

The web server allows you to configure Signo Biometric Reader 25B 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 Signo Biometric Reader 25B.

1.5.1 System requirements

HID Biometric Manager system requirements:

- Intel i5 2.3 GHz
- RAM 8 GB
- Available disk space 20 GB
- Windows operating system. Windows 10, Windows server 2016, Windows server 2019.

1.5.2 Credential Database

The Credential Database is a SQL database that HBM services uses to store the credential data that has been gathered through manual registration or **1.5.4 Data Import**. It also stores configuration data and transaction logs for all installed Signo Biometric Reader 25B devices.

1.5.3 Reader Service

The Reader Service runs in the background and automatically synchronizes data between the HID Biometric Manager and the Signo Biometric Reader 25B devices.

1.5.4 Data Import

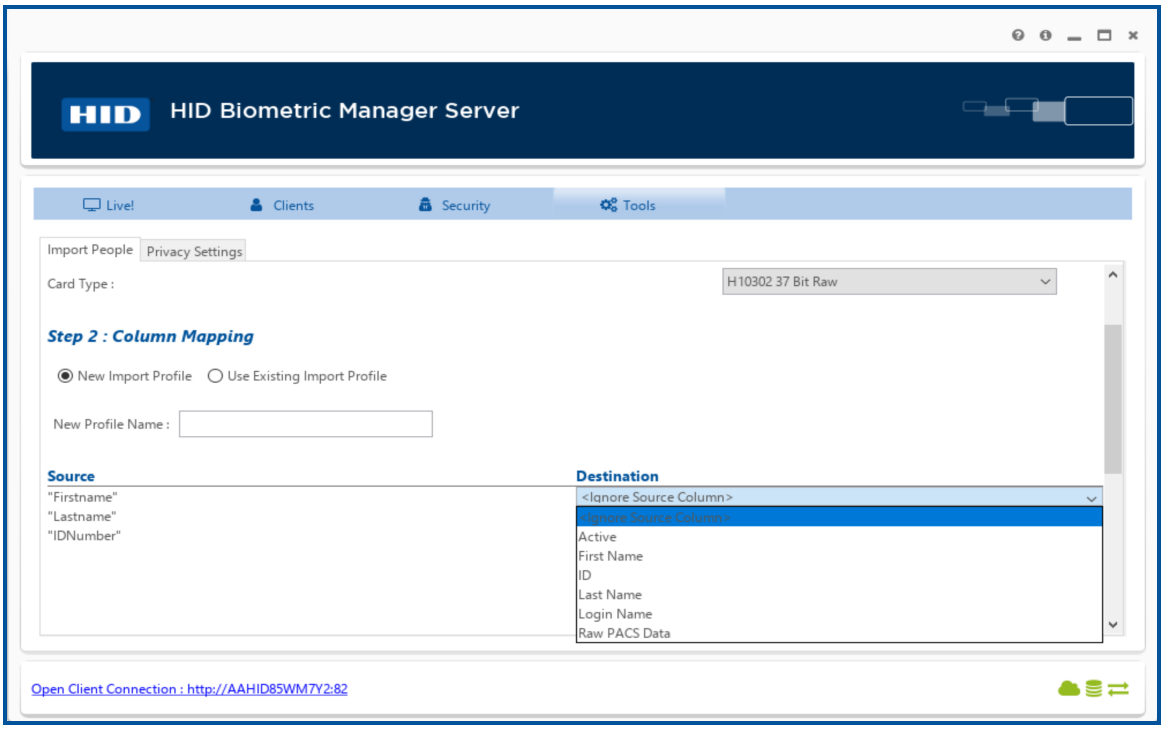
The HID Biometric Manager Data Import component allows credential and credential holder information to be imported into the HID Biometric Manager database from a third party PACS headend. This ensures that the output of the Signo Biometric Reader 25B matches the expected input of the third party controller.

People and credentials can be imported into the system using an Excel or CSV file. Each column needs a header row containing the criteria that populates the **Source** column and the data for each criteria below in the data rows as shown:

Header Row	"Firstname"	"Lastname"	"IDNumber"
Data Rows	"James"	"Code"	"007"
	"Jane"	"Code"	"006"

Note: Up to 250,000 people and credentials can be imported at a time.

After a file is imported, the **Source** column values need to be mapped to the **Destination** column values in the drop down menu.



1.5.5 HID Biometric Manager Server Window Icons

Icon	Description	Status
	Webserver	 - Initial state  - Ready  - Busy with startup  - Failed to start
	Database	 - Initial state  - Ready  - Busy with startup  - Failed to start
	Engine	 - Initial state  - Ready  - Busy with startup  - Failed to start

1.6 HID Biometric Manager Web UI

The HID Biometric Manager provides a web server which supplies content to any device on the network. HBM is compatible with the following browsers:

- Chrome version 73.0.3683.86 and later.
- Firefox Quantum 64-bit.
- Microsoft Edge

This interface is used to install and configure Signo Biometric Reader 25B readers. It is also used to perform user registration including fingerprint enrollment. Any connected Signo Biometric Reader 25B device, or SIGNO-B-USB can be selected as the enrollment 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 Signo Biometric Reader 25B device firmware.

1.7 Signo Biometric Reader 25B

The Signo Biometric Reader 25B is a biometric card and fingerprint reader. It authenticates users according to one of four modes:

- Fingerprint only
- Card only
- Two variations of card with finger:
  - Fingerprint data stored to card
  - Fingerprint data stored to device

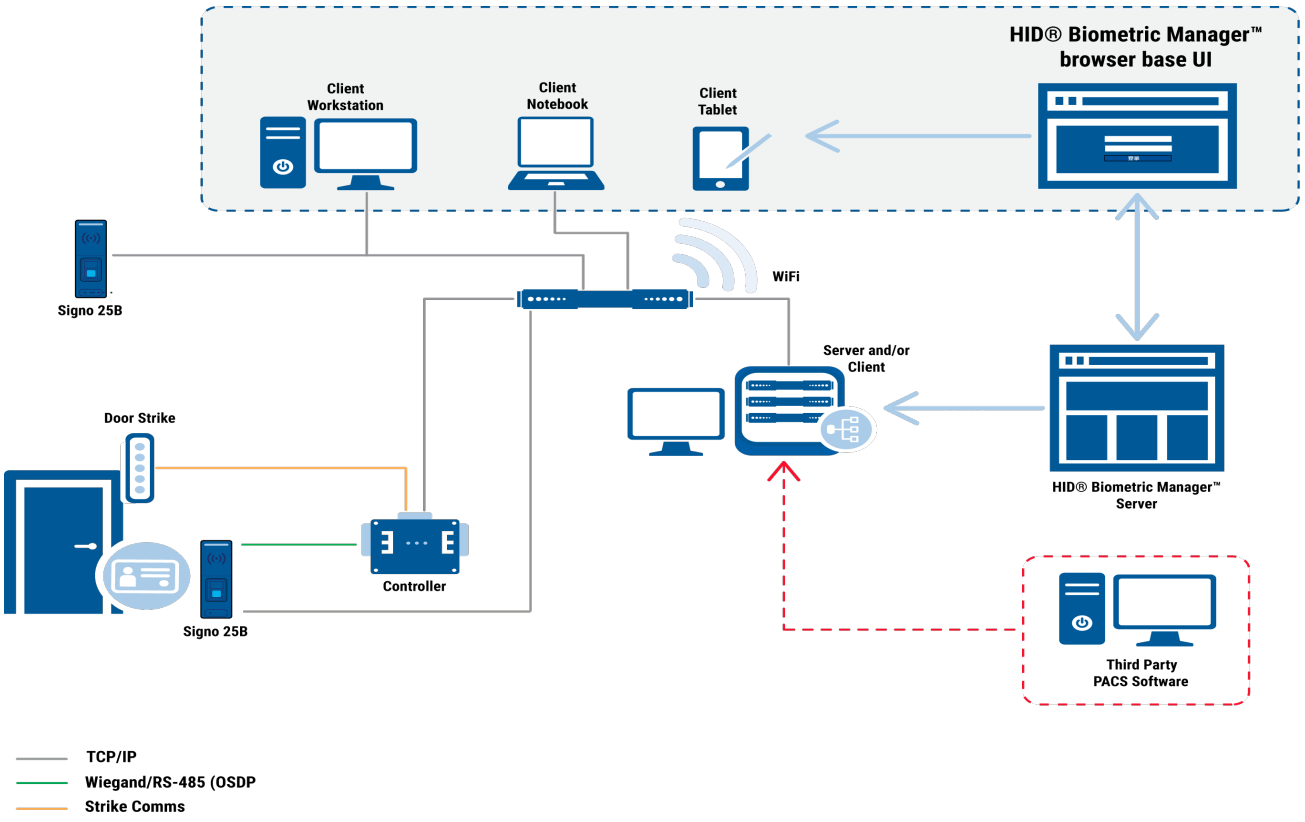
See **Authentication Mode (Signo Biometric Reader 25B)** for more information. When the credential holder is authenticated, the data is output to a third party controller.

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 Signo Biometric Reader 25B which ensures the credential is authentic.

The following diagram shows an example of the system.

- The entire system is located inside the firewall.
- Multiple Signo Biometric Reader 25B devices and PACS Panel/Door Controllers can be added. HID Biometric Manager can control up to 2,000 Signo Biometric Reader 25B devices.



1.9 Network setups examples

The HID Biometric Manager installation wizard manages the majority of network configurations. When using HID Biometric Manager during discovery and installation of Signo Biometric Reader 25B devices, it defaults to hostname Signo Biometric Reader 25B Server.

Note: Switching between DHCP and Static IP will cause the certificates to no longer work. To resolve this, re-install the unit with the target settings set in HBM.

Scenario 1 - DHCP network, Signo Biometric Reader 25B 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.

Signo Biometric Reader 25B devices have an Ethernet connection on the same LAN as the server running HID Biometric Manager. The network is configured so that the DCHP server dynamically assigns IPs (which may have a limited lease time) to Signo Biometric Reader 25B.

Scenario 2 - DHCP network, Signo Biometric Reader 25B devices have dynamic IP, Server has a dynamic IP

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

Signo Biometric Reader 25B devices have an Ethernet connection on the same LAN as the server running HID 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 Signo Biometric Reader 25B devices in HID 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 - HID Biometric Manager installed on a Server and connects to DHCP network

This is the same as Scenario 2 except HID Biometric Manager is running on a Server. This means that it is likely that HID Biometric Manager will not be running all the time. When HID Biometric Manager is not running, Signo Biometric Reader 25B 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

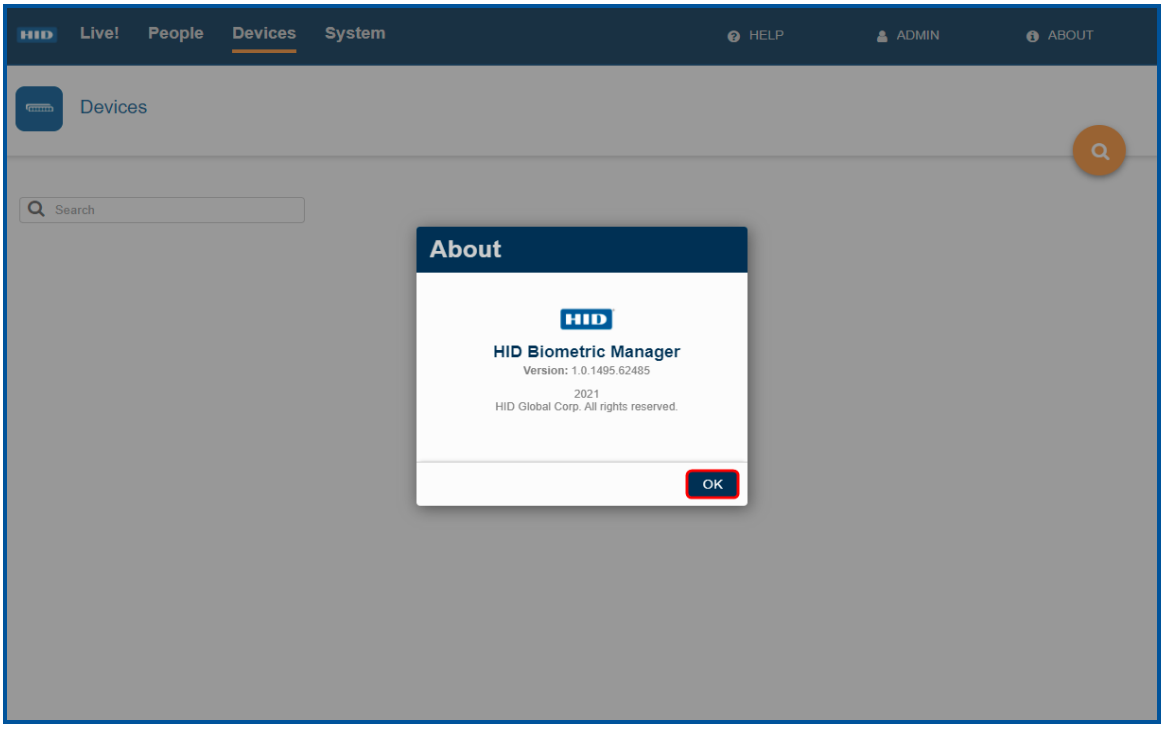
2.1 Overview

HID® Biometric Manager™ is a web application that streamlines the management and configuration of Signo Biometric Reader 25B 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 HID Biometric Manager software, and creates/administers operator roles within the application see **2.4 HID Biometric Manager initial setup**.
- **Administrator:** This operator role has full access to HID Biometric Manager web application with functions to install and manage Signo Biometric Reader 25B devices see **2.6 Device installation and configuration** and enroll people in the system, add credentials, collect and store associated biometric data see **2.9 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 Signo Biometric Reader 25B. This operator role has limited access to user information.
- **Enrollment:** This operator role has full access to HID 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 **2.9 Enrollment**.

2.2 About Section in the UI

Selecting the **ABOUT** button creates a pop-up window showing the HBM version number.



Click **OK** to close the pop-up window.

2.3 Network usage

This table shows the HID Biometric Manager network usage.

Protocol	Port	Source	Destination	Direction	Comment
ICMP		Server	Device	Outgoing	
TCP	22	Server	Device	Outgoing	SSH for firmware update.
TCP	82	Client	Server	Outgoing	Client Server Outgoing HTTP from browser client to server.
TCP	443	Client	Server	Outgoing	Client Server Outgoing HTTPS from browser client to server.
TCP	443	Server	Internet	Outgoing	Connection to Azure.https://hidbiomanager.azurewebsites.net/ Used for FW update.
TCP	443	Server	Internet	Outgoing	RCAM[1] connection to Origo. • https://prod-rfp.firebaseio.com/ • https://prod-readermanager.hidglobal.com/ Used to roll to Elite and for FW update.
TCP	1819	Server	Server	-	RCAM to HBM. This all happens on the same physical computer.
TCP	3000	Server	Device	Outgoing	One time use (per device) for install. Server needs to tell device about MQTT settings to talk to it.
TCP	8883	Device	Server	Outgoing	MQTT
UDP	10500	Server	Device	Outgoing/Incoming	Device Discovery and Device Network Settings.

1. Reader Configuration and Management (RCAM)

2.4 HID Biometric Manager initial setup

2.4.1 HID Biometric Manager software install

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

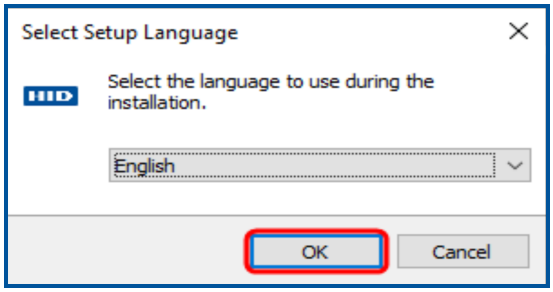
Note: The user installing the HID Biometric Manager software needs to be logged in on the server as a Windows Administrator.

1. Download the **HID Biometric Manager.exe** file from the download site to your server: https://www.hidglobal.com/signo25b
2. Double click on the downloaded **.exe** file to launch the installation wizard.

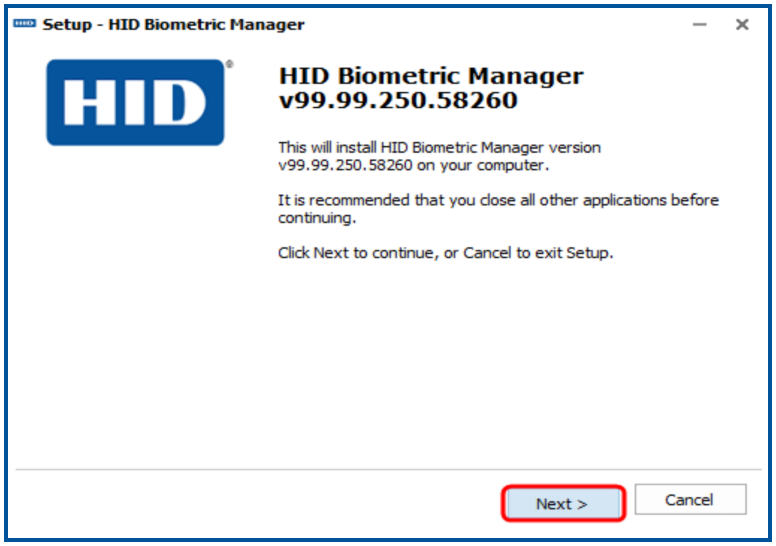
   Note: If the server system language is configured to one of the supported languages then the install wizard instructions and HID Biometric Manager will automatically default to the server system language. Supported languages:

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

3. Select the required language and click **OK**.

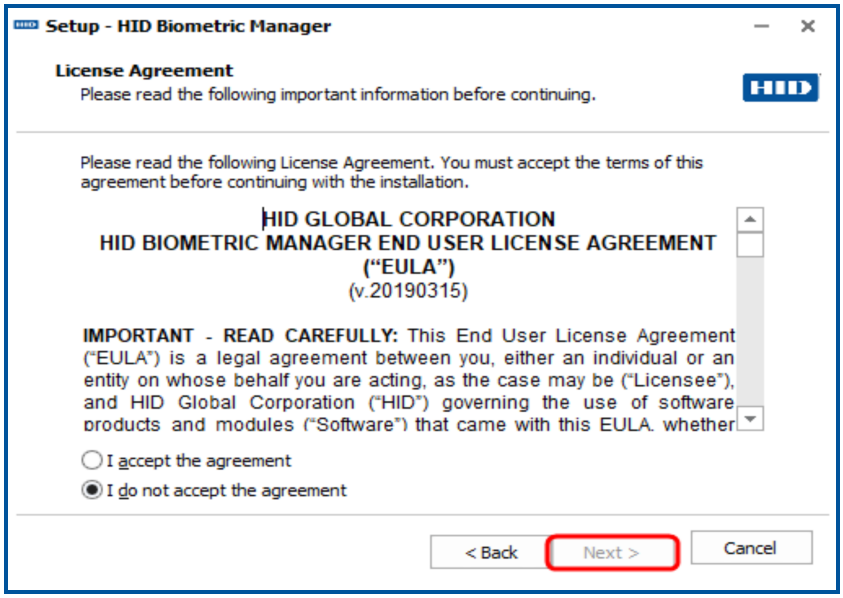


4. Click **Next** on the initial installation wizard screen.

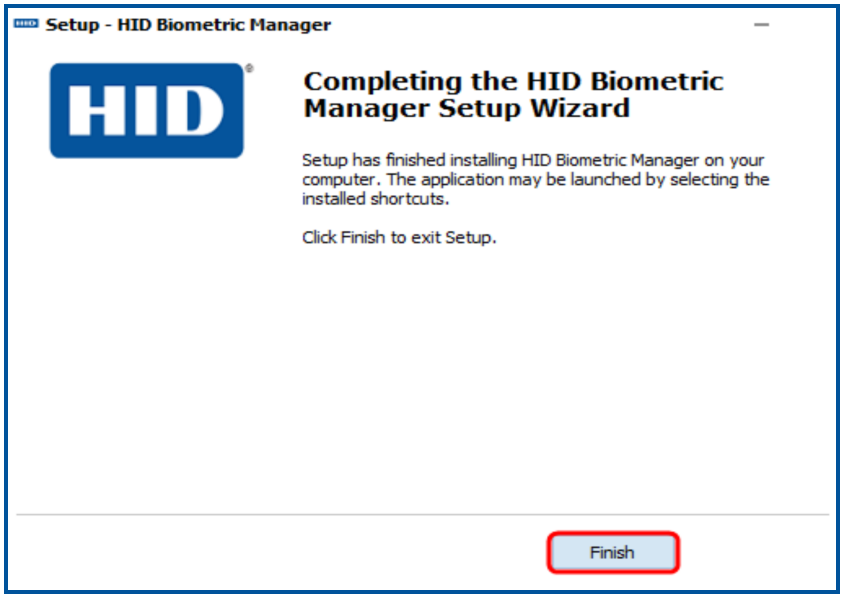


5. Read the License Agreement. Select **I accept the agreement**, and click **Next**.

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



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



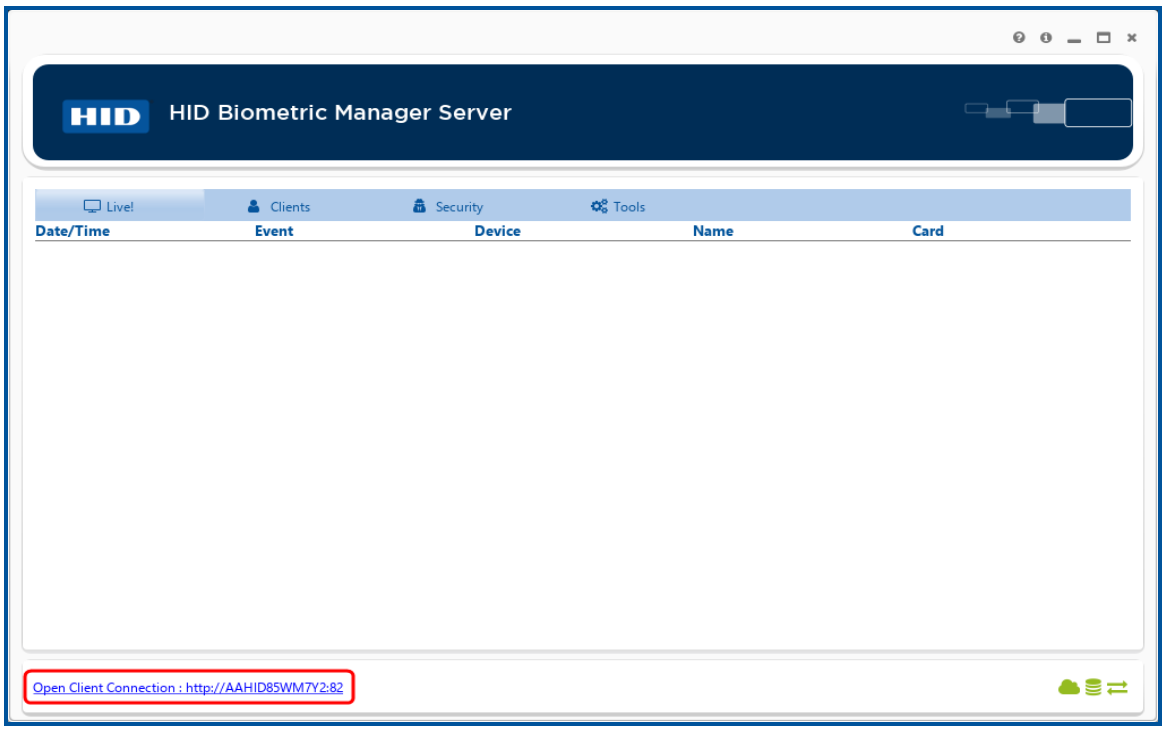
2.4.2 HID Biometric Manager initial login

On the server where HID Biometric Manager has been installed:

1. Double-click 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 the **HID Biometric Manager.exe** file.

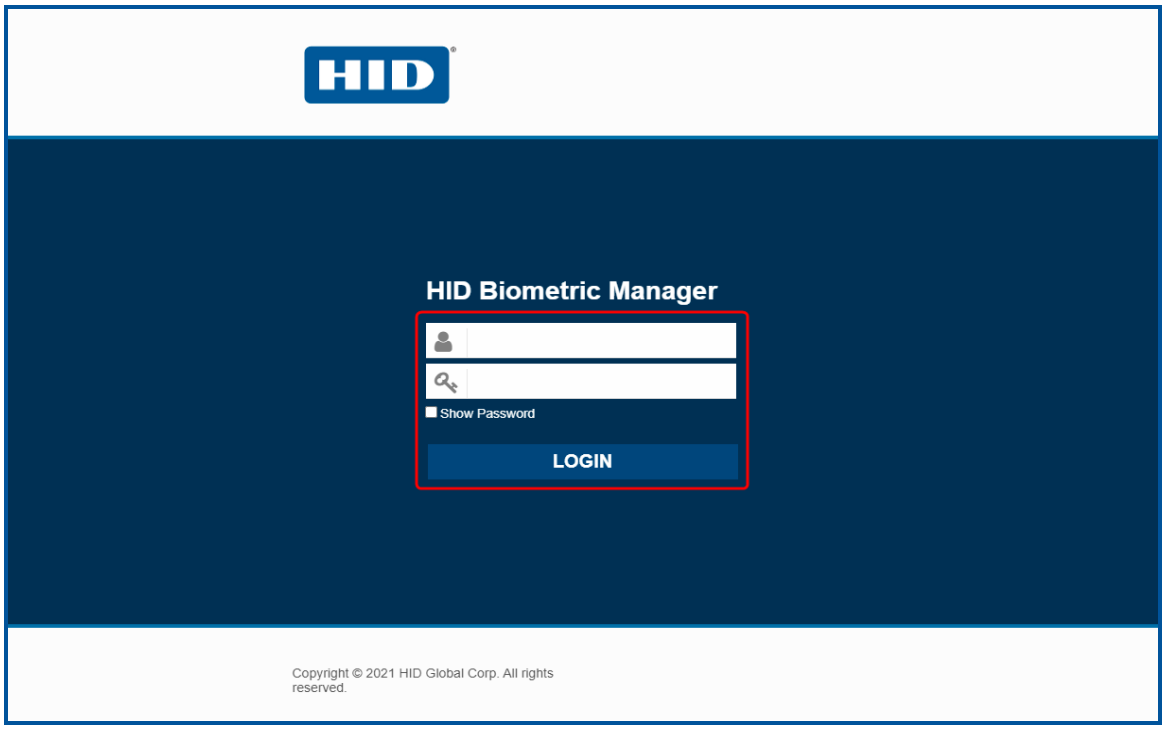
   Note: The size of the database may impact how long it takes the HID Biometric Manager application to launch. Start up feedback is indicated with an on screen progress bar.
2. On the HID Biometric Manager Server application screen, click the **Open Client Connection** link to access the HID Biometric Manager application login screen. Record the **Client Connection** 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** URL fails to connect to HID Biometric Manager due to a port issue, change the default port number (443) in the URL to:**http://hostname:82/HIDBiometric/HIDBiometricManager.html**

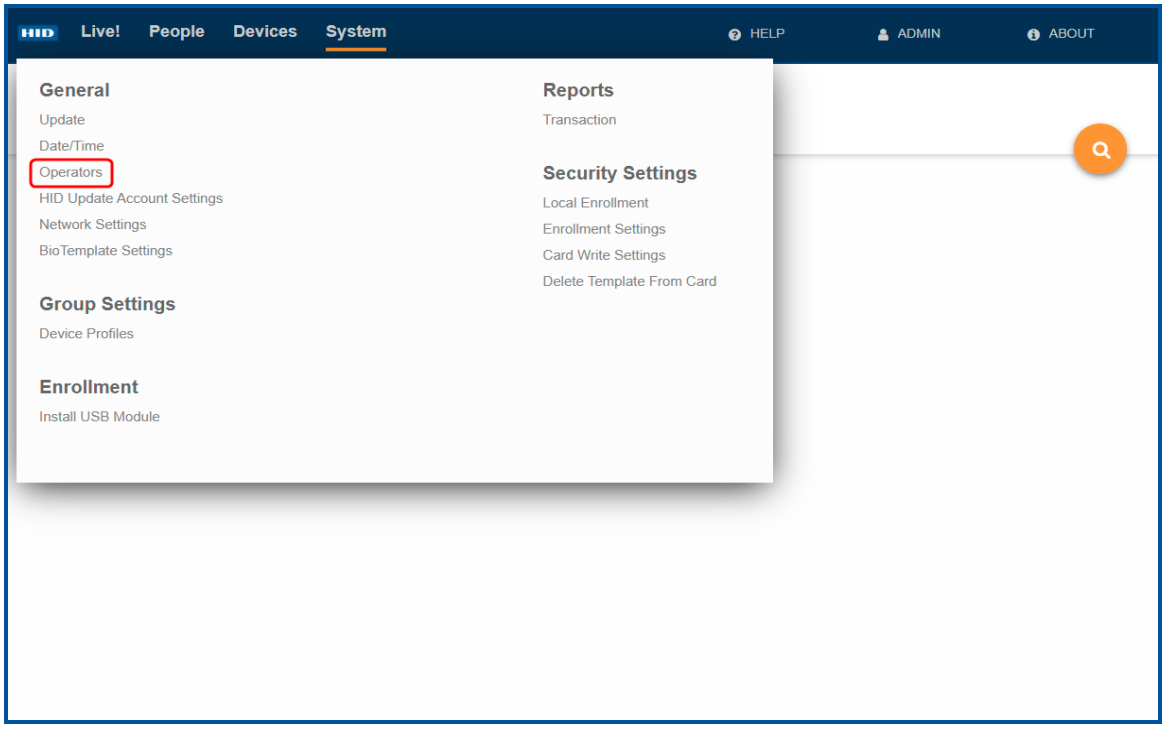


3. Enter the initial default admin User Name (**admin**) and Password (**password**) and click **LOGIN**.

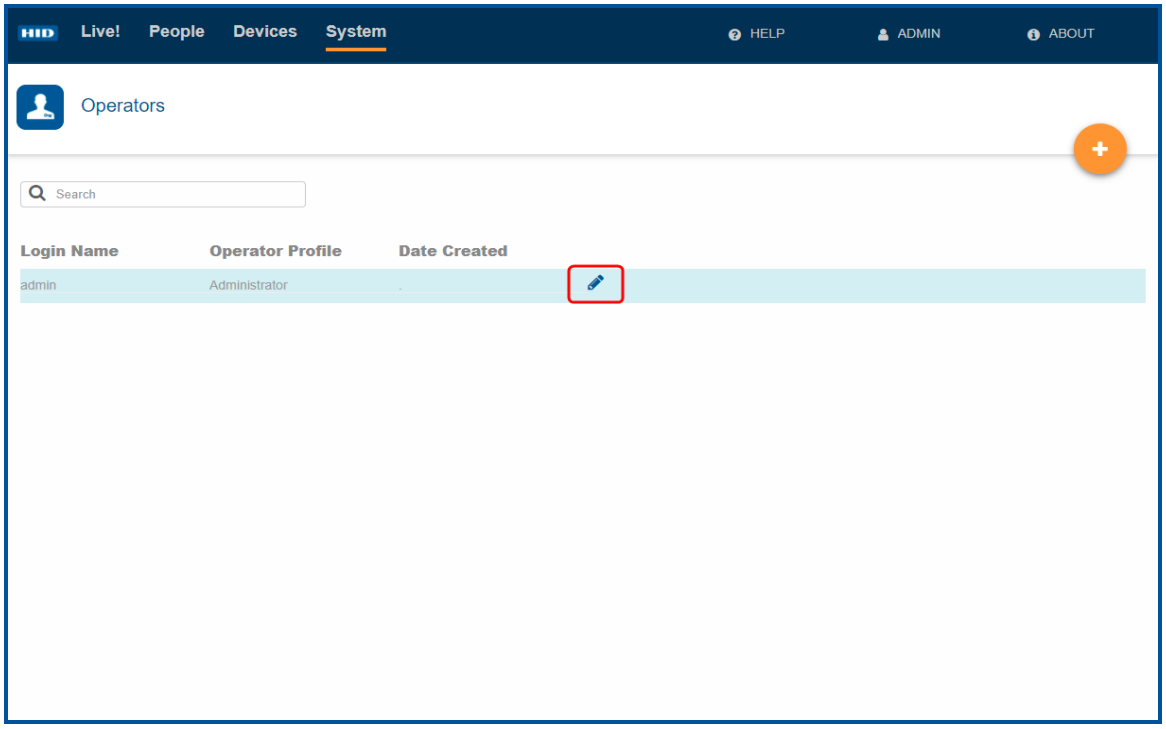
   Note: A pop-up window containing the EULA will open after the initial login, this needs to be accepted.



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



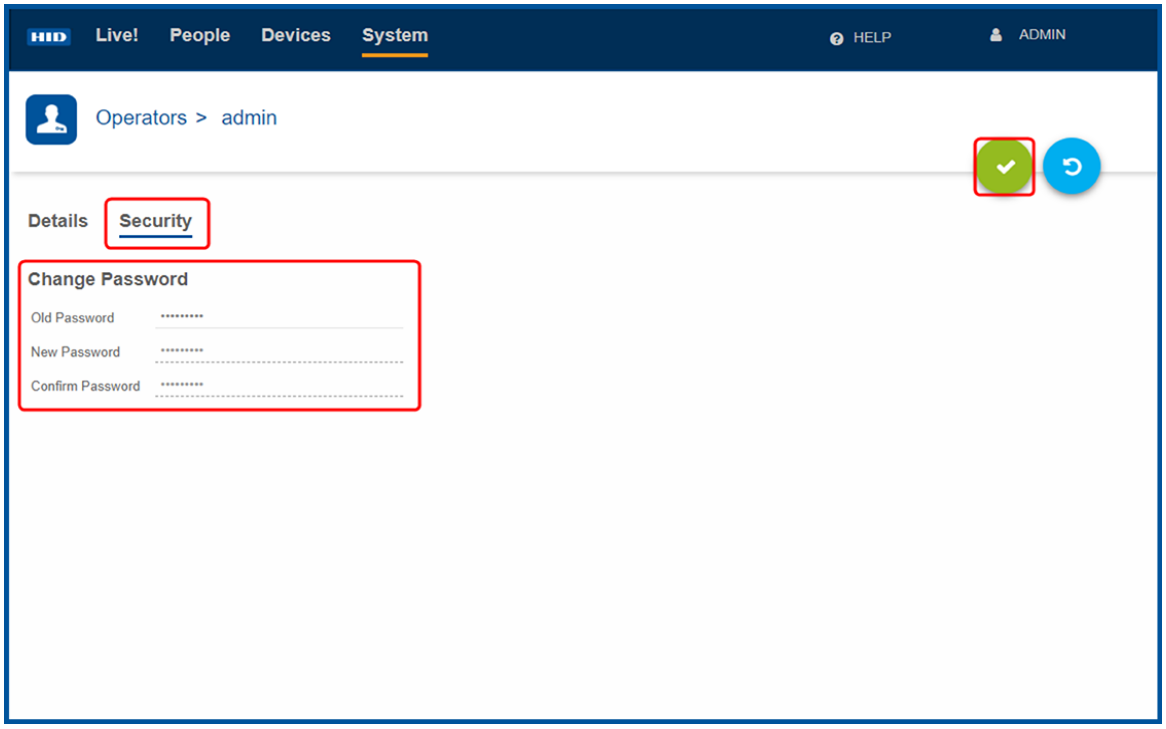
5. Click the **Edit** icon [ ] associated with the displayed system admin user.



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.

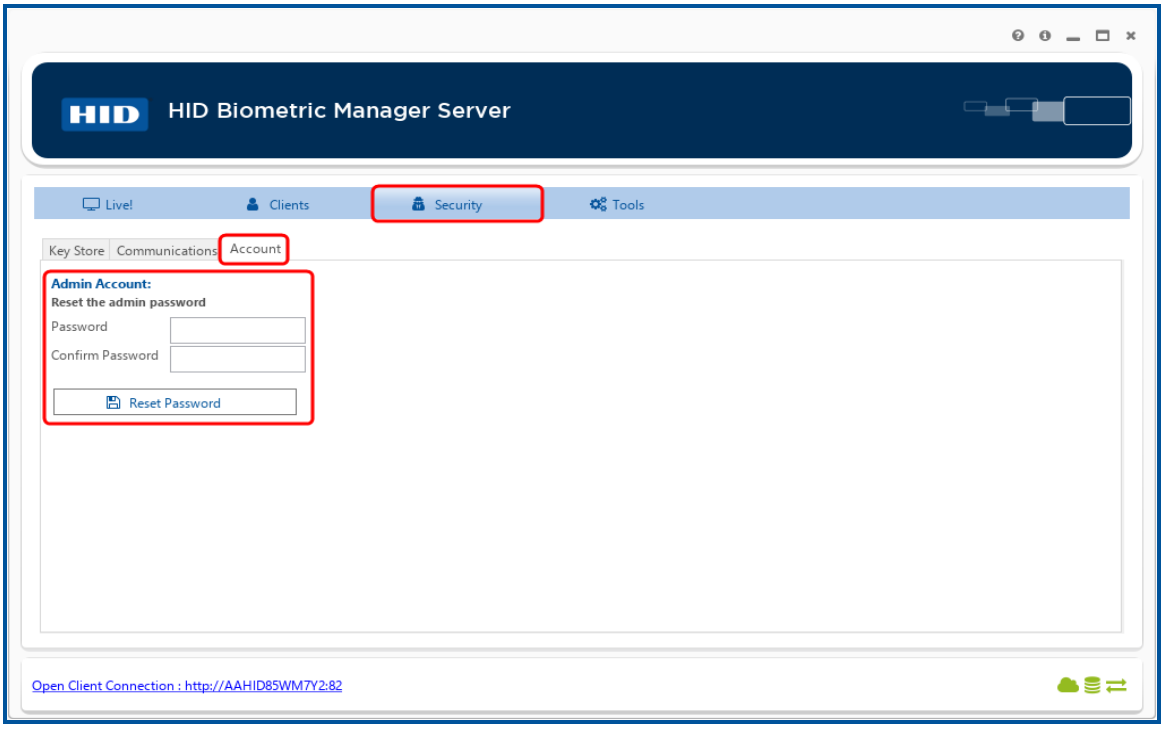
7. Click to save this new password. A notification will appear confirming that all changes have been saved at the bottom of the window.



8. Close the HBM browser window and login again using the default username (**admin**) and new password.

2.5 Resetting administration password

You can reset the administrator password in the **HID Biometric Manager Server** under **Security** > **Account** before log in.



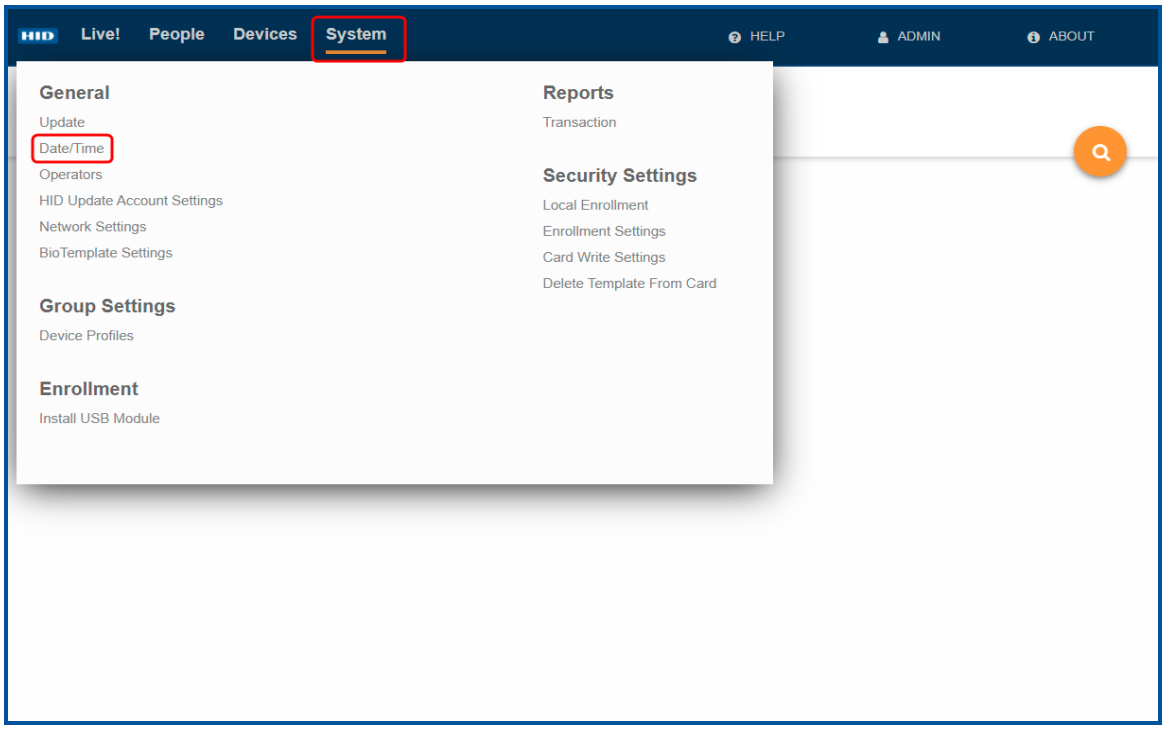
This method can be used to change the administrator password, as shown in **2.4.2 HID Biometric Manager initial login**

Note: The new password created is used to log in to HBM.

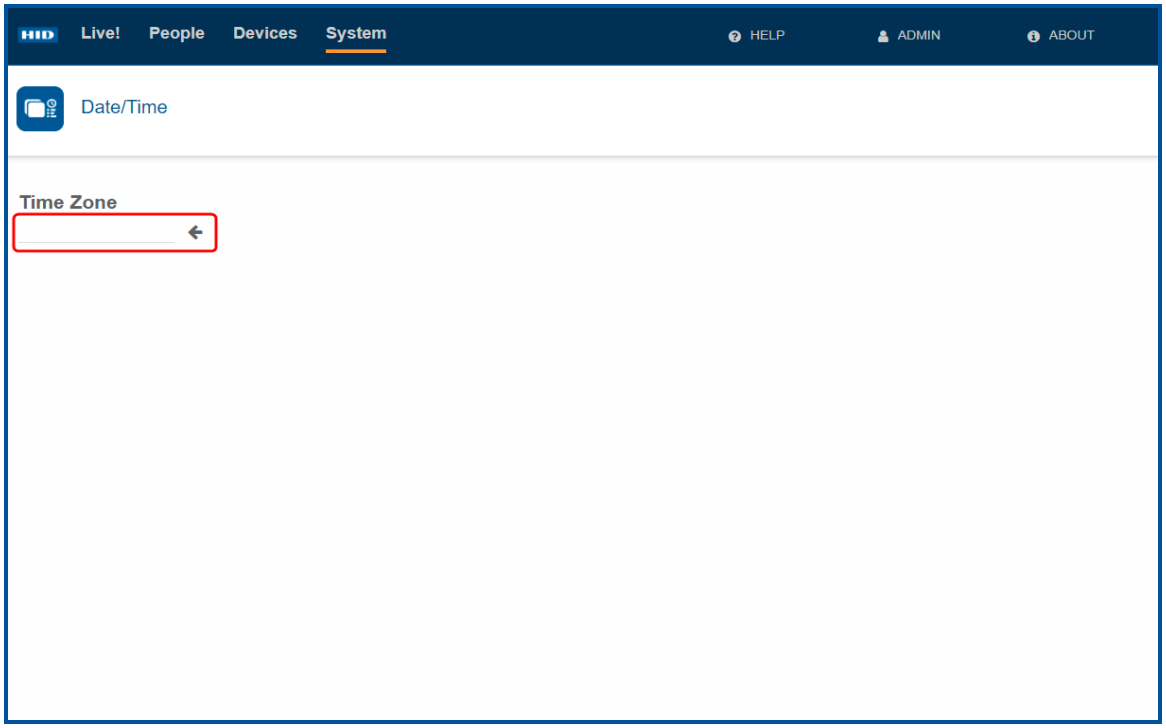
2.5.1 Configure time zone setting

Setting the time zone configures the time zone for the instance of HID Biometric Manager running on the server.

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

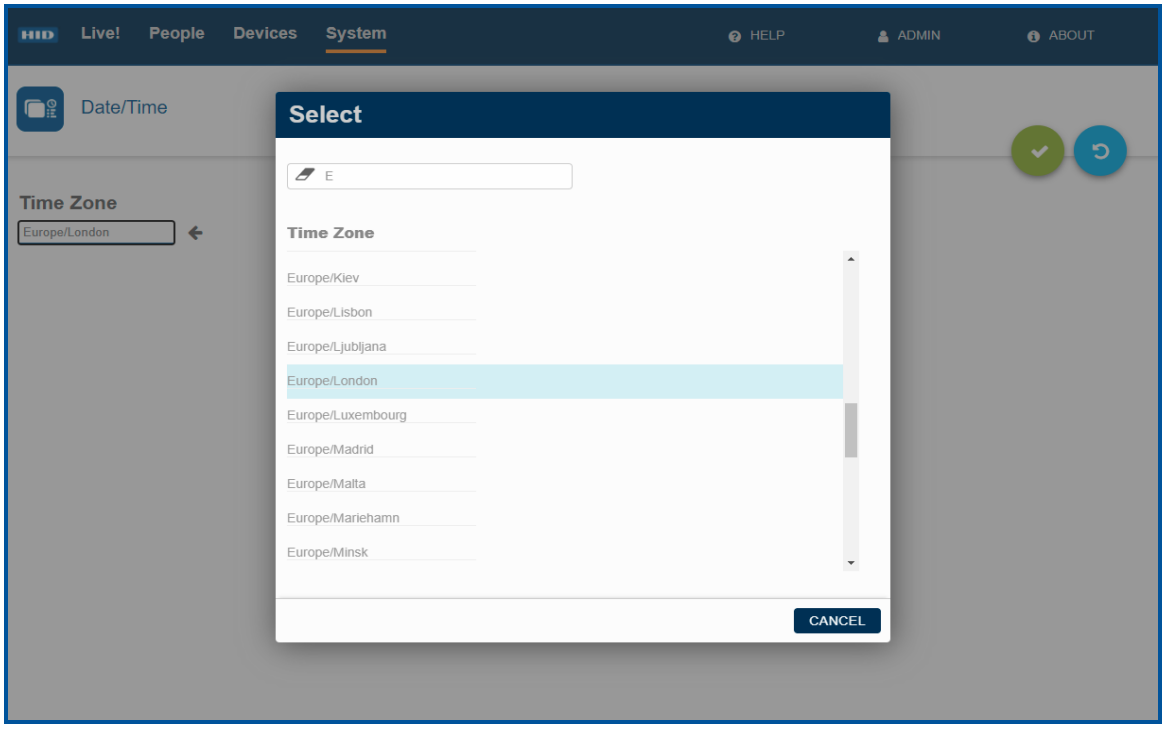


3. Click the **Time Zone** arrow icon to access a list of selectable regions and countries.

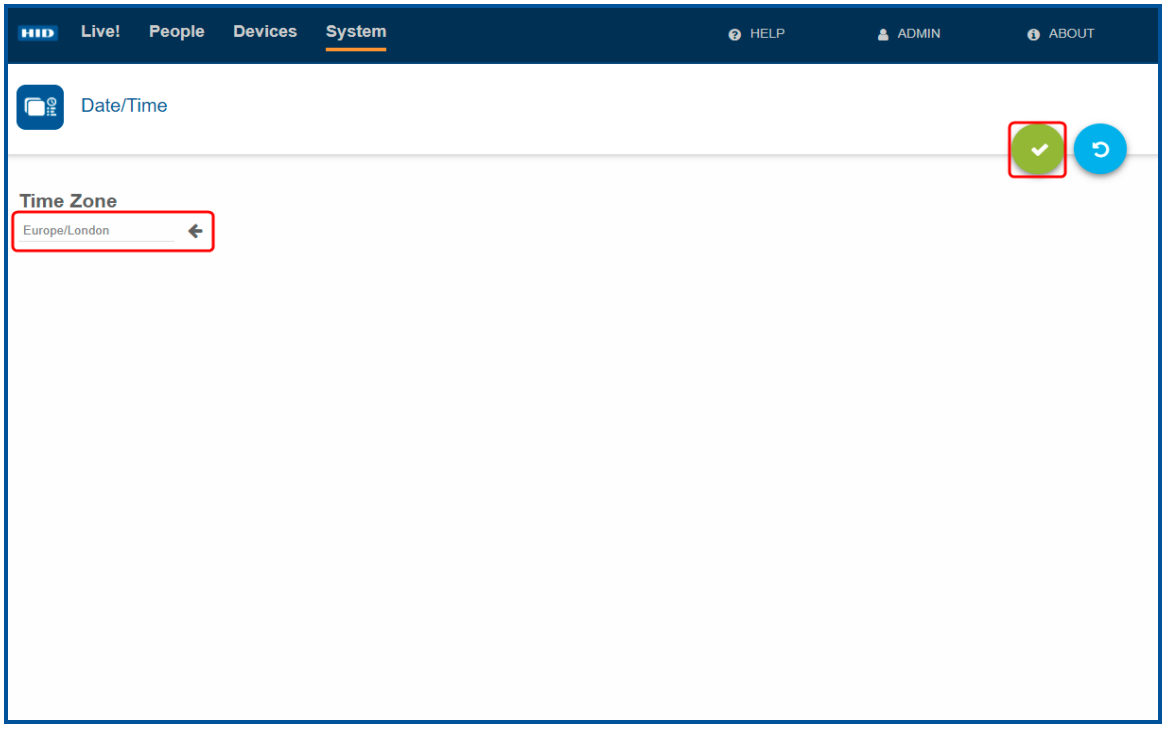


4. Select the required country or region from the displayed list.

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



5. Click .

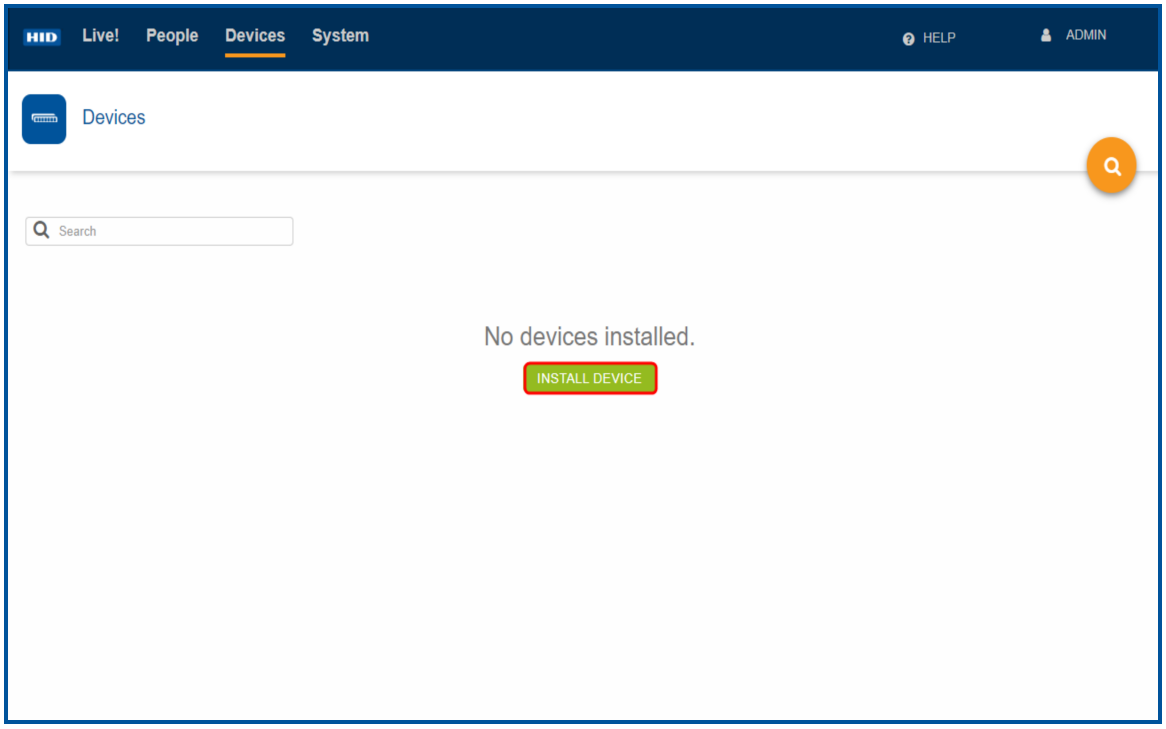


2.6 Device installation and configuration

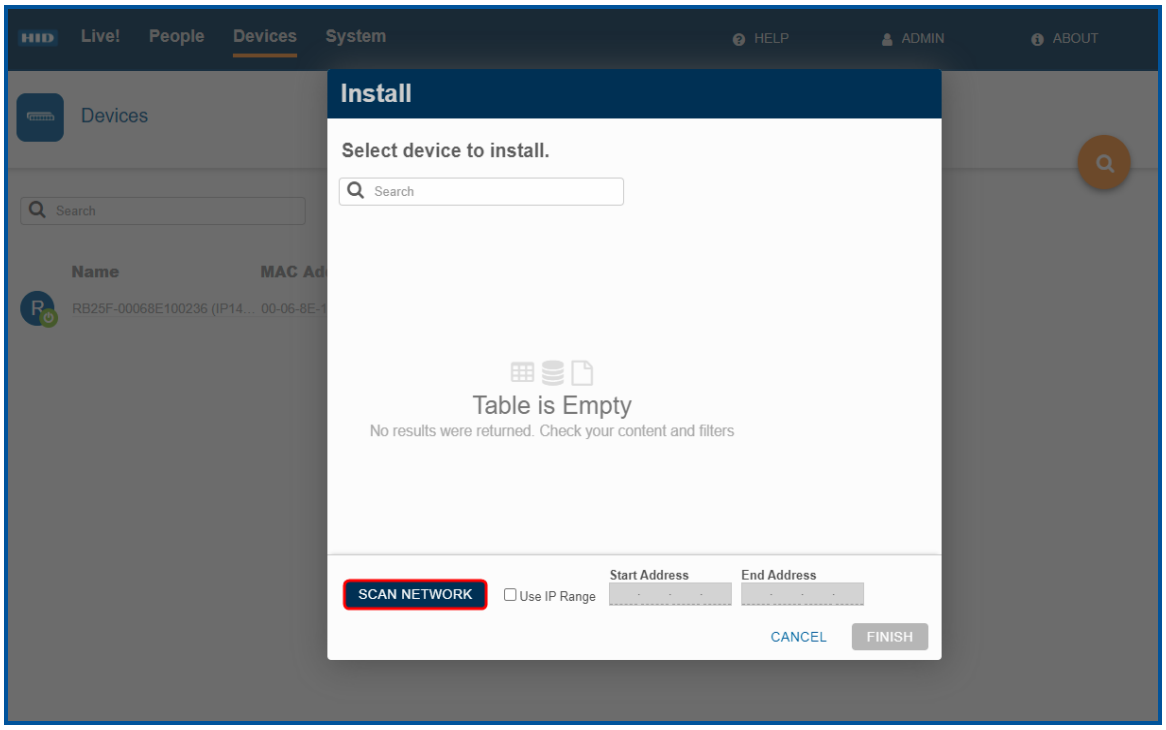
Device installation and configuration with HID Biometric Manager can only be carried out by the Administrator or Device Administrator role. For initial configuration or when no devices are installed, HID Biometric Manager opens on the **Devices** screen with the option to install a device. If devices are already installed Biometric Manager opens on the **People** screen, see **2.9 Enrollment**.

2.6.1 Perform network scan:

1. Launch HID Biometric Manager and login as an **Administrator** or **Device Administrator** operator.
2. To initially install a device, on the **Devices** screen, click **INSTALL DEVICE**.
   Note: If devices are already installed, to add additional devices click the Install icon [].

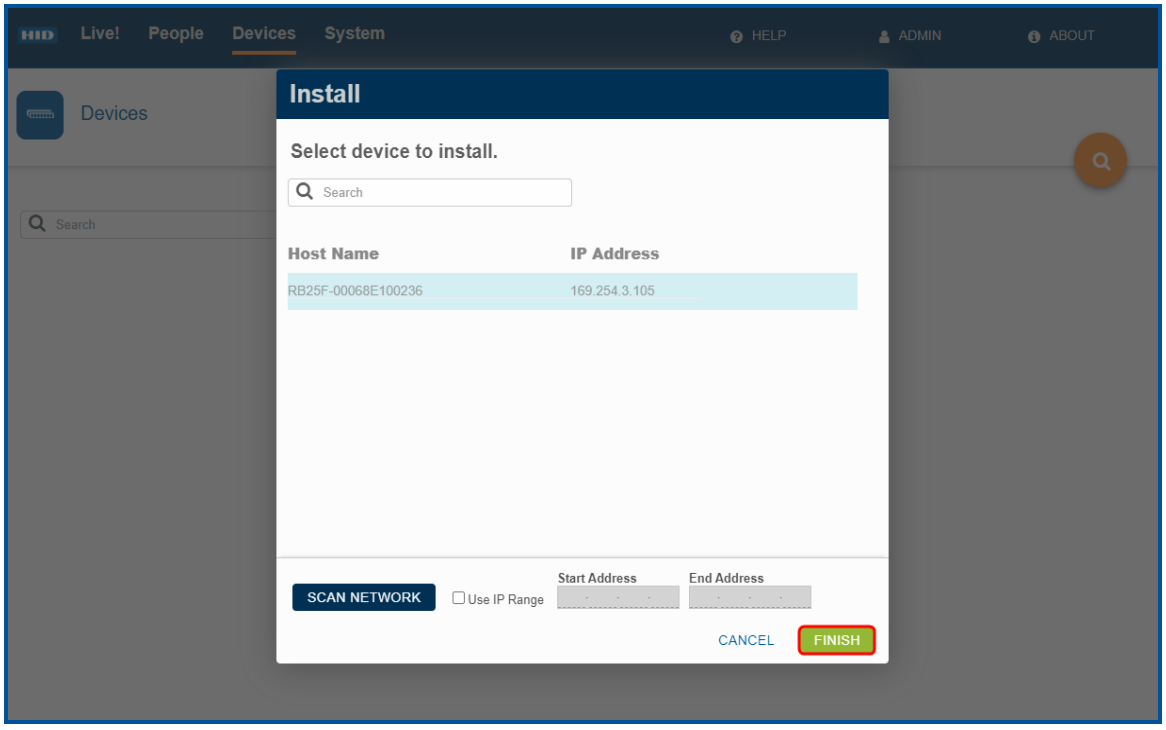


3. Click **SCAN NETWORK** to view the complete list of available devices.
   Note: If no devices are found check the ports listed in **2.3 Network usage** are open within any firewall applications running on the computer or server. The **Search** function can be used to search the list of displayed devices.



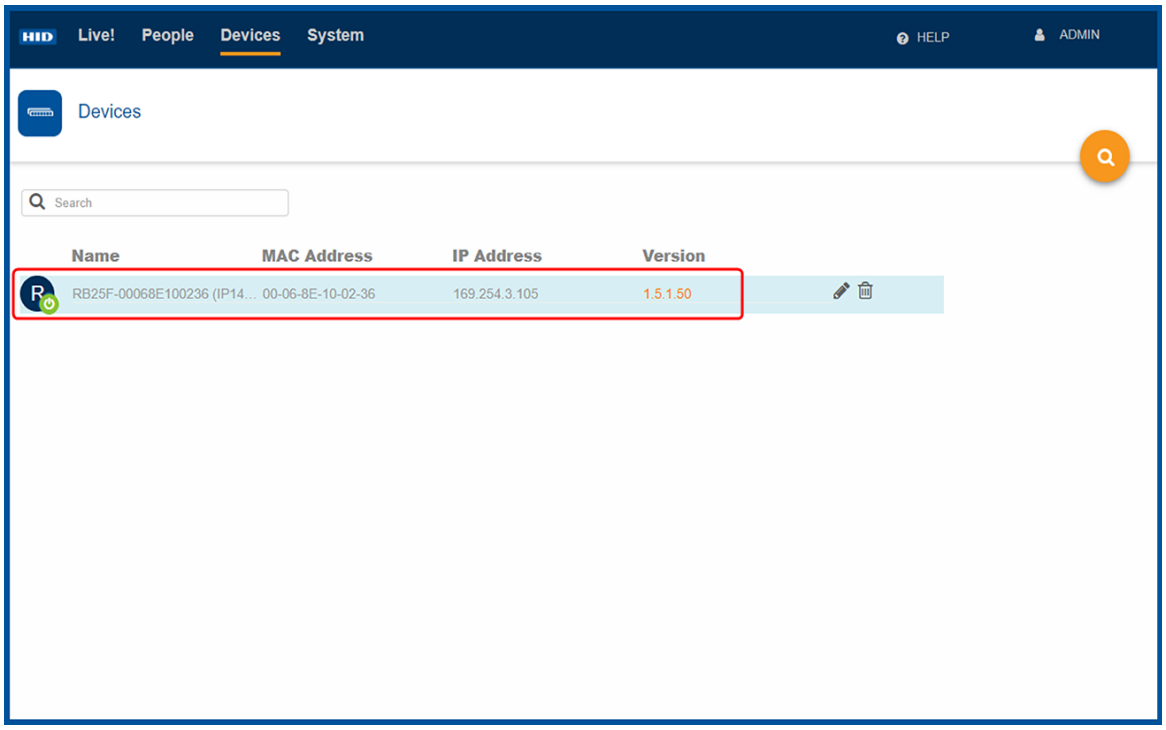
4. Select a device from the displayed list and click **FINISH**.

   Note: The **Host Name** should not include any underscores.



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.

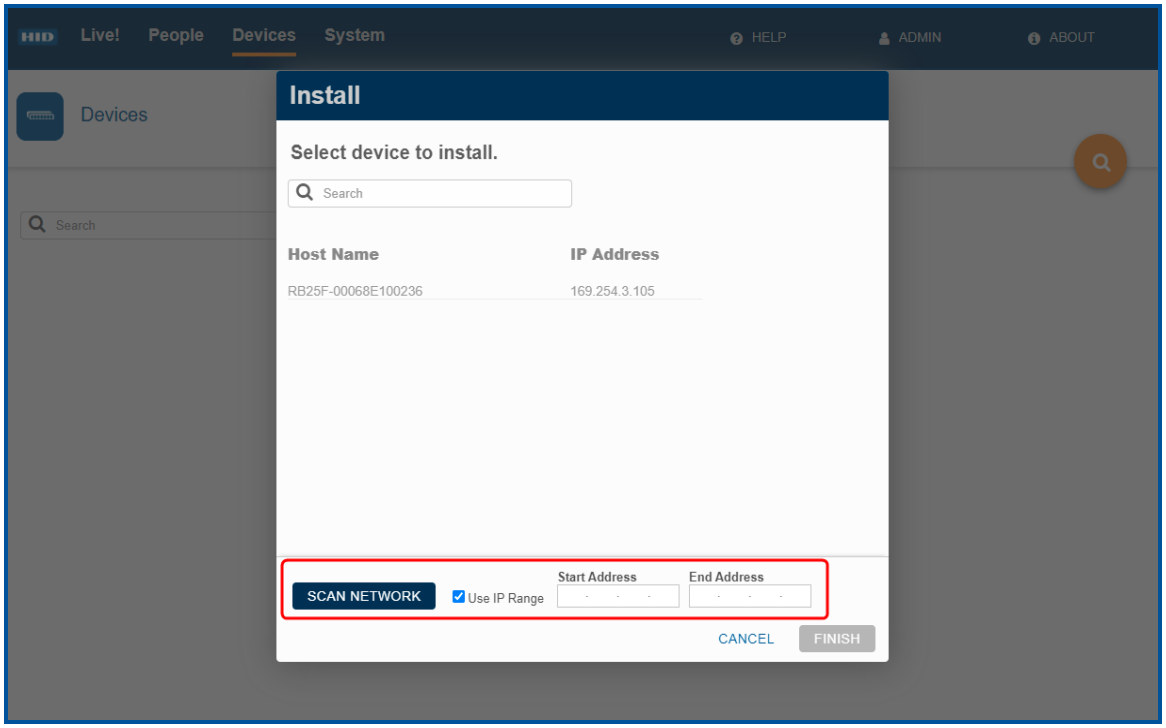


Note: To uninstall a device, see **2.6.7 Uninstall a device**.

2.6.2 Scan network using an IP range

When devices are installed in a virtual LAN setting, HBM allows you to scan for devices over a specific subnet using start and end IP addresses.

1. Select the **Use IP Range** box.

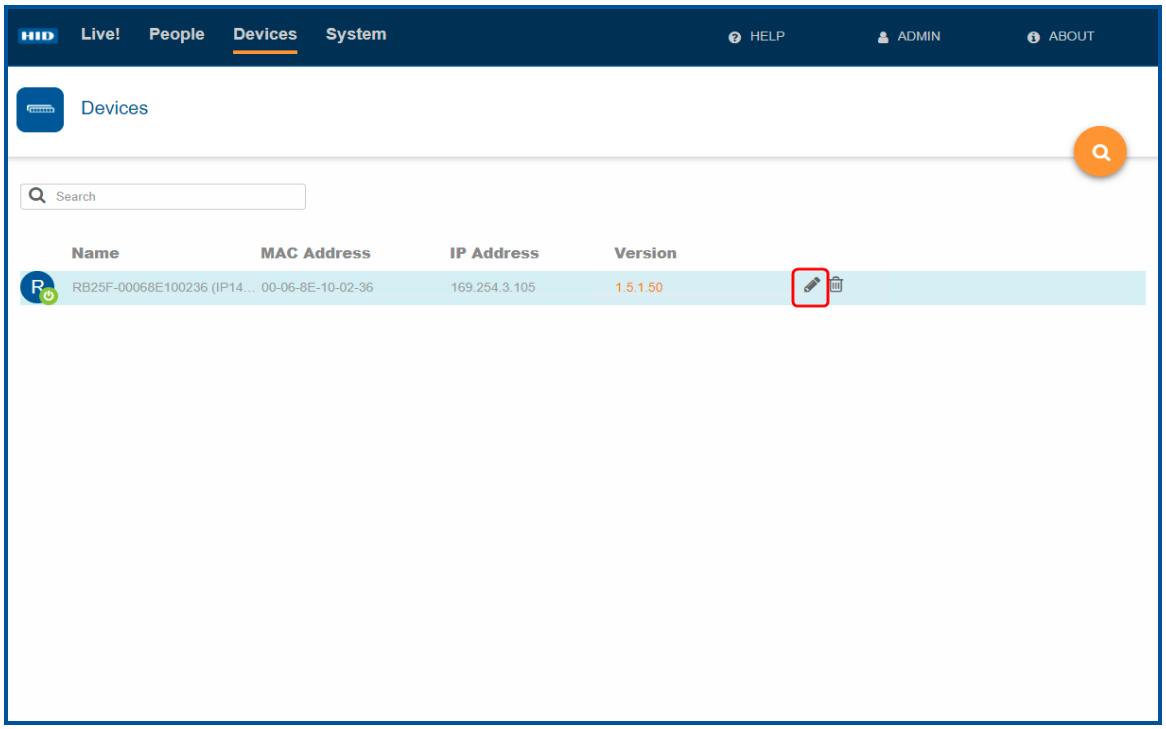


2. Enter the **Start Address** and **End Address**.
3. Click **SCAN NETWORK**.
4. Select a device to install.
5. Click **FINISH**.

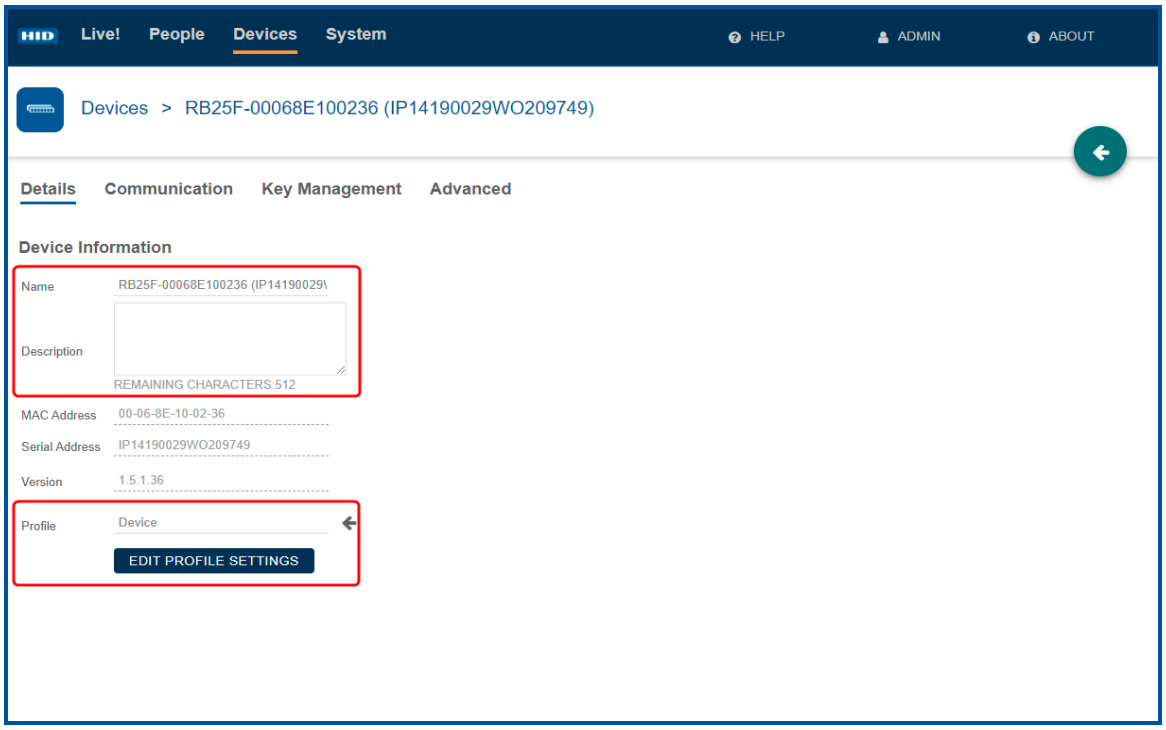
2.6.3 Configure device settings

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 [ ] to access the device settings screen.



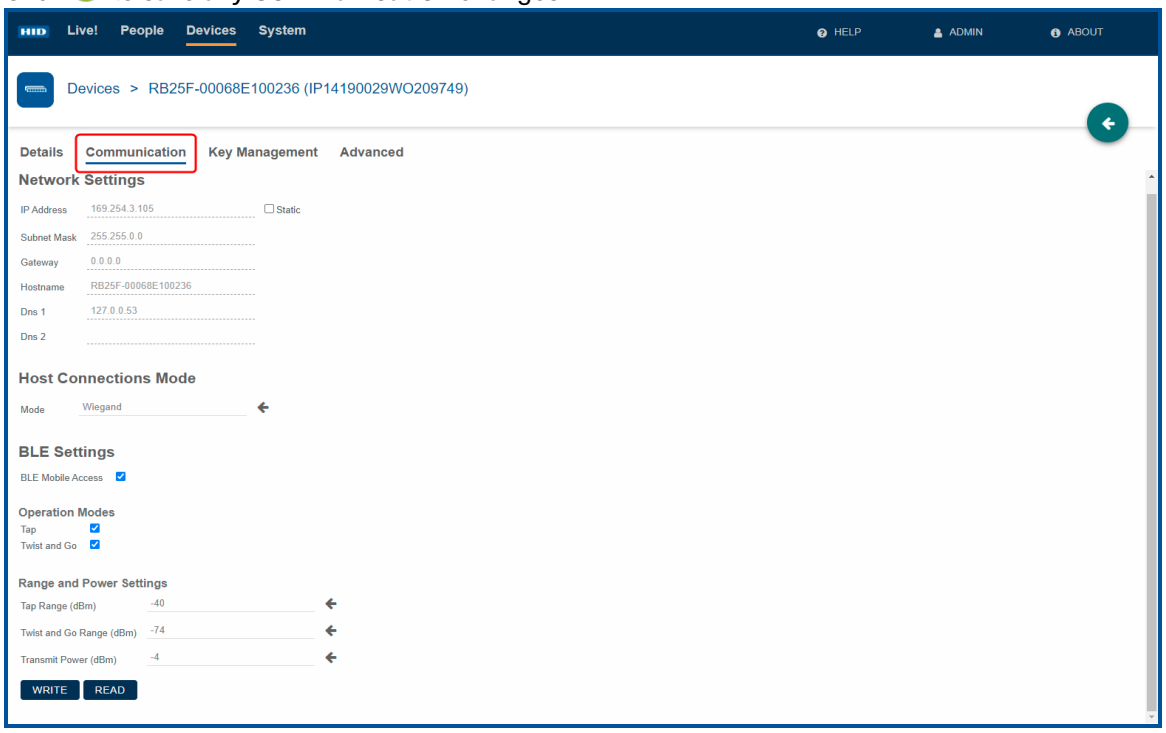
3. Click the **Details** tab on the device screen.
4. Under **Device Information** you can edit the following:
   - **Name/Description:** Enter a logical name for the device. As an option enter a description for the device.
   - **Profile:** Click the arrow icon to select a device profile. Click **EDIT PROFILE SETTINGS** to configure the settings for the displayed device profile, see **2.21.2 Edit a device profile**.



5. Click the **Communication** tab.
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) together with the Subnet Mask and Gateway.
   - **Host Connections Mode:** Set as **Wiegand** (default).
     Note: This refers to output to PACS panel - Wiegand or OSDP)
   - **BLE Settings:** Enable/disable **BLE Mobile Access**.
     - **Operation Modes:** Select the required 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**.
   - **READ:** Read mobile keys from the device.
   - **WRITE:** Write mobile keys to the device. Before mobile keys can be written to the device they must be loaded onto HID Biometric Manager, see **HID Origo set up**.

   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. Click to save any **Communication** changes.

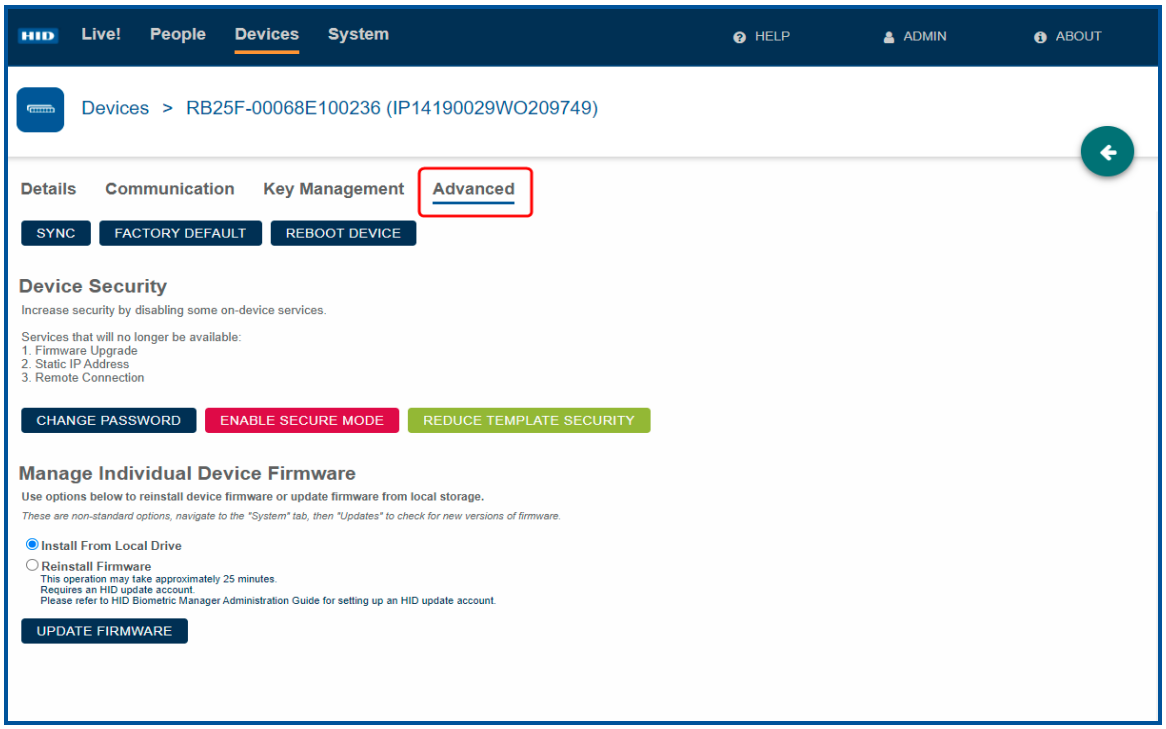


8. Click the **Advanced** tab. On the **Advanced** screen you have options to:
   - **SYNC:** Syncs all device settings in HID Biometric Manager to the device.
   - **FACTORY DEFAULT:** Restores all device settings to the original factory defaults, see **2.6.6 Reset a device**.
   - **REBOOT DEVICE:** Reboots the device.

     Note: The **Live!** tab will show the power down/up for clarification that the device has rebooted.
   - **UPDATE FIRMWARE:** Allow you to update device firmware through HBM or from a local file.
   - **CHANGE PASSWORD:** Allows you to 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:** Allows you to configure the security settings for device communication.

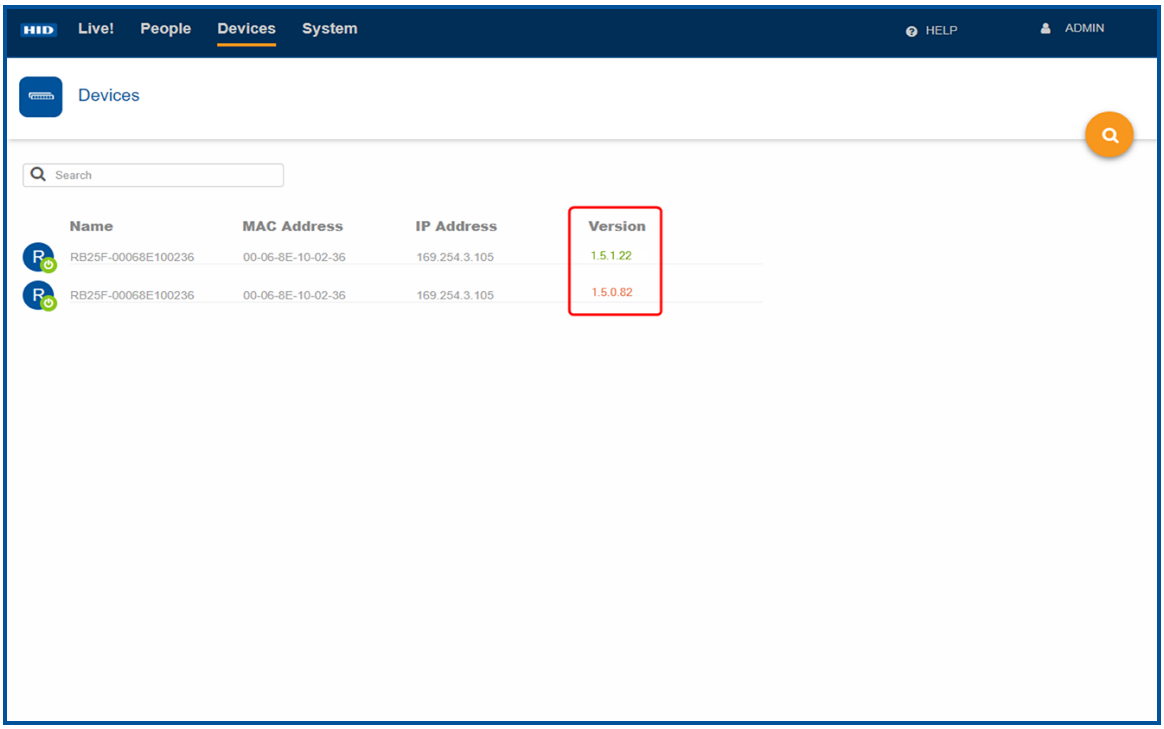
     Note: Firmware upgrades and device network settings are unavailable with secure mode disabled.

9. Click **SYNC**. All settings are copied from HID Biometric Manager to the selected Signo Biometric Reader 25B.



2.6.4 Device firmware update

When a device firmware update is available, the version number will be displayed in red. If the version number is displayed in green the firmware of that device is up to date.

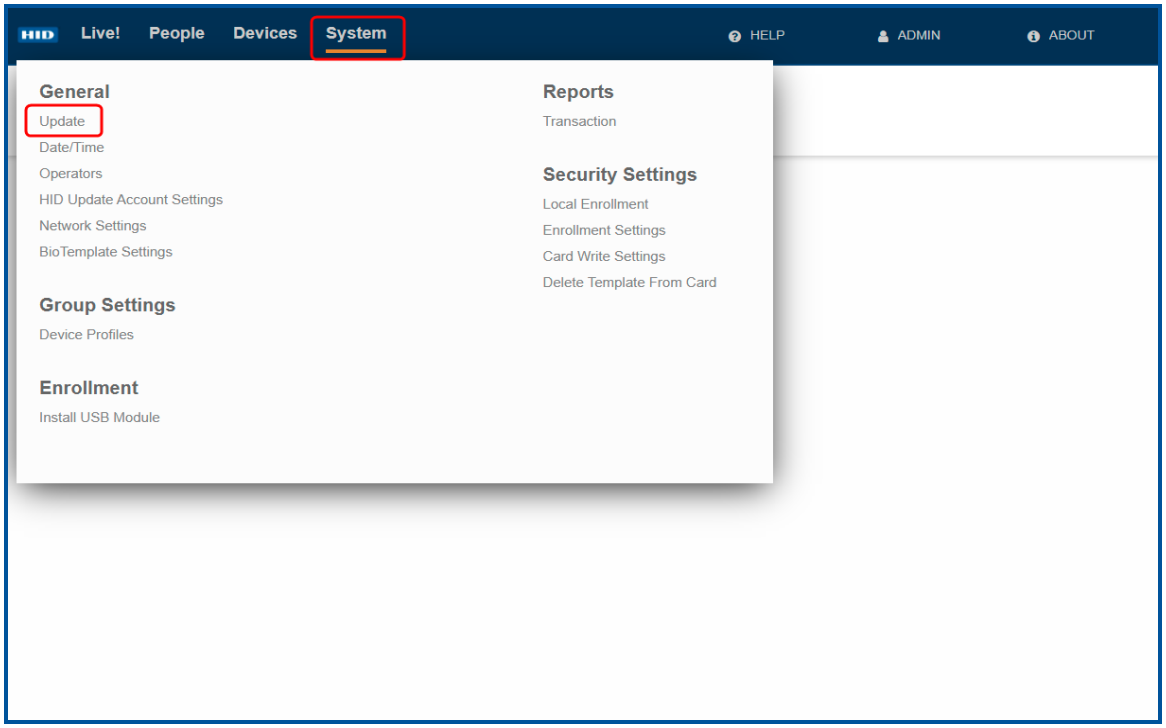


Device firmware updates can take approximately 25 minutes per device, including updates of the reader board. Updates may complete faster depending on the HID Origo™ connection and the number of uninterrupted updates.

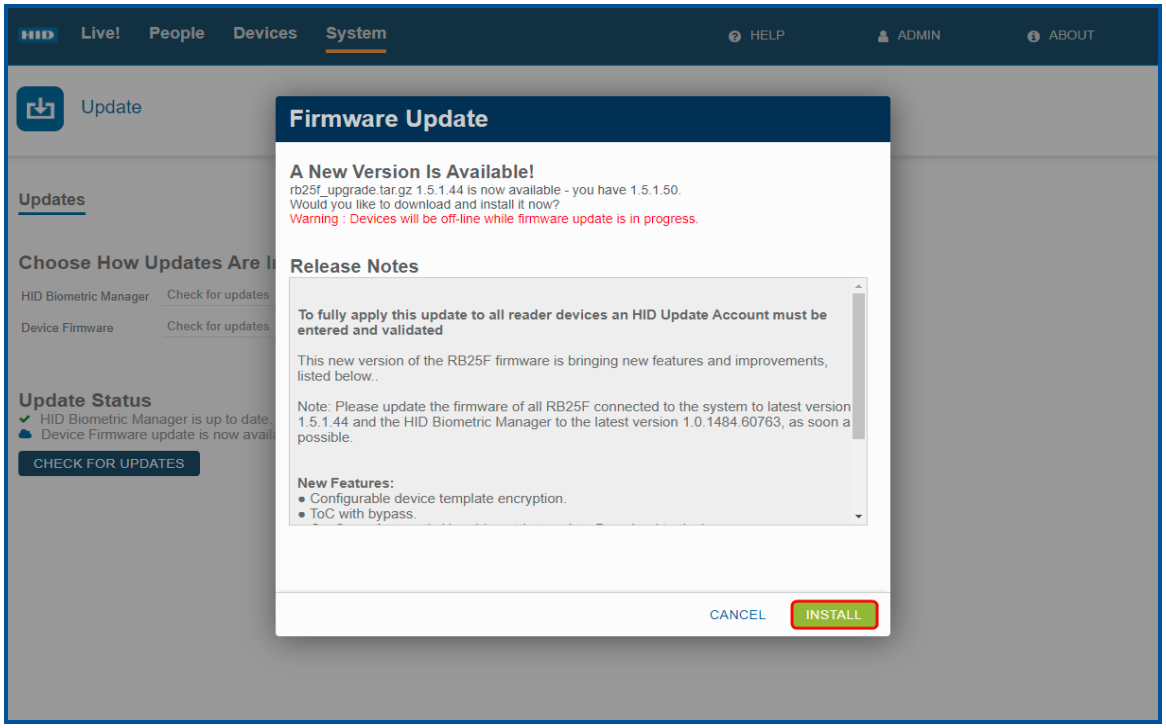
Important: It is recommended that device firmware updates should be carefully scheduled as all devices are updated and will be unavailable for use during the firmware update period.

To update device firmware:

1. Click **System** > **Update**.

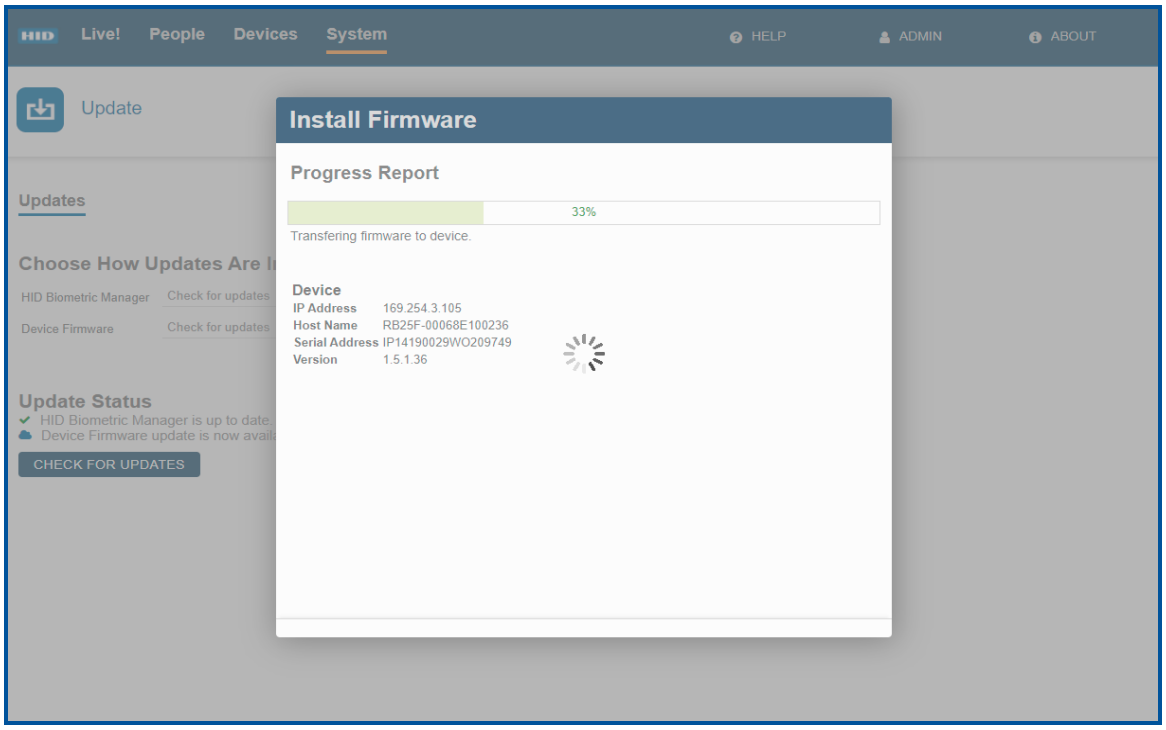


2. Click **CHECK FOR UPDATES**. Review the displayed firmware update information and click **Install** to start the firmware update process.



3. An indication of the firmware update progress is displayed in a pop-up window.

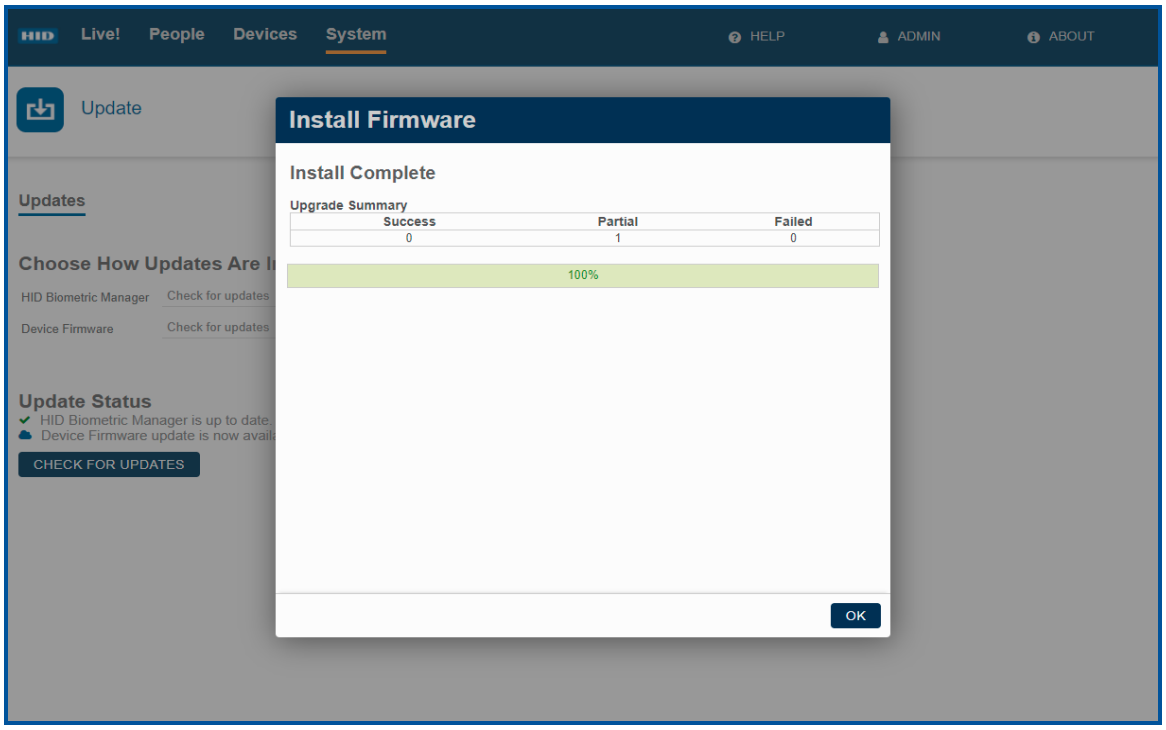
Note: The **Progress Report** bar indicates firmware update progress against total devices. For example, if two devices are being updated then 50% progress indicates one device updated out of two devices. Devices are updated in series with information displayed on the current device being updated.



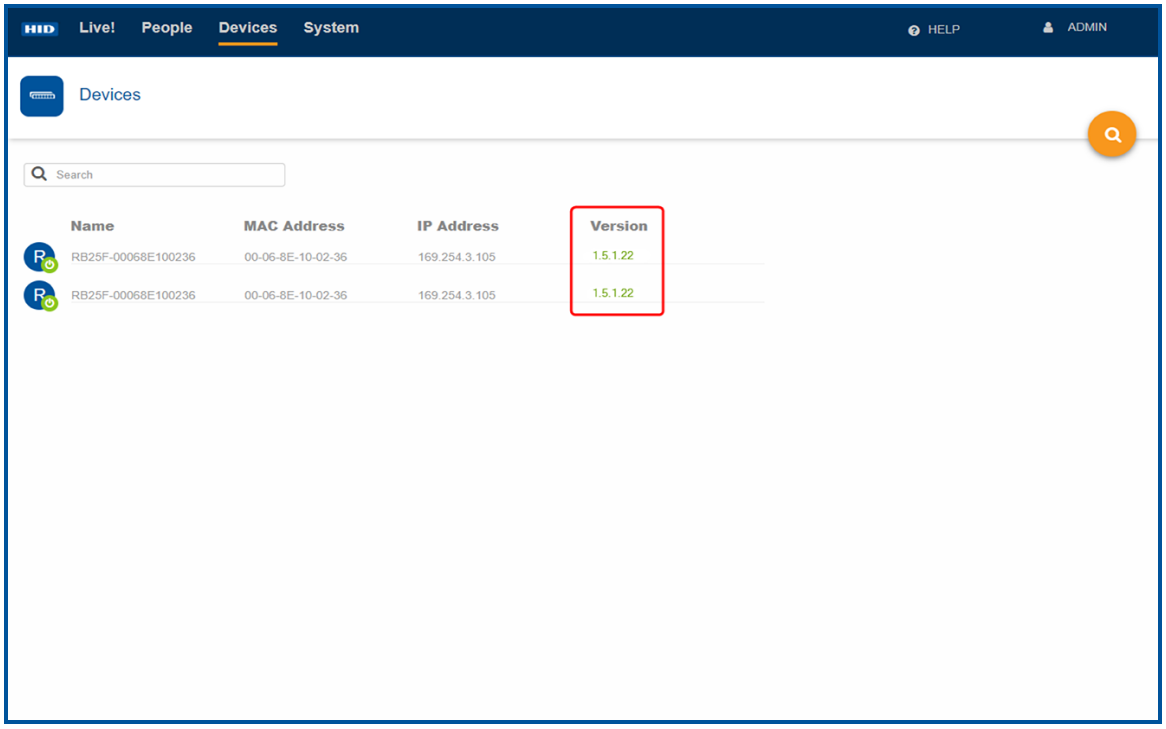
4. Click **OK** when the firmware update is complete.

   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 Origo not being setup (see **HID Origo set up**) 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.



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

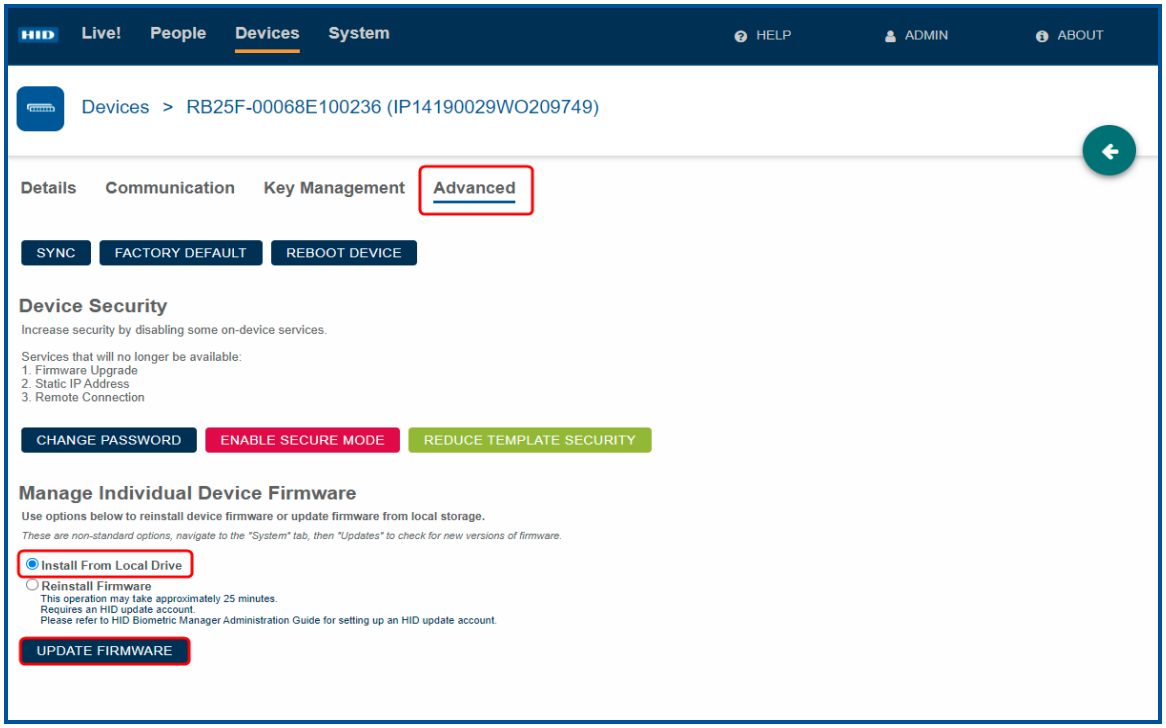


2.6.5 Individual device firmware update

This feature gives the option to install a firmware update from a local file, or reinstall the latest firmware version to a specific or individual device.

Install a firmware update from a local file

1. Click **Advanced**.
2. Select the check box for **Install From Local Drive**.
3. Click **UPDATE FIRMWARE**.



4. Click **CONFIRM** in the pop-up window and then select the update file from your local file system to begin the update.
5. Click **OK** when the update is complete.

Reinstall firmware

1. Click **Advanced**.
2. Select the check box for **Reinstall Firmware**.
3. Click **UPDATE FIRMWARE**.
4. Click **CONFIRM** in the pop-up window.

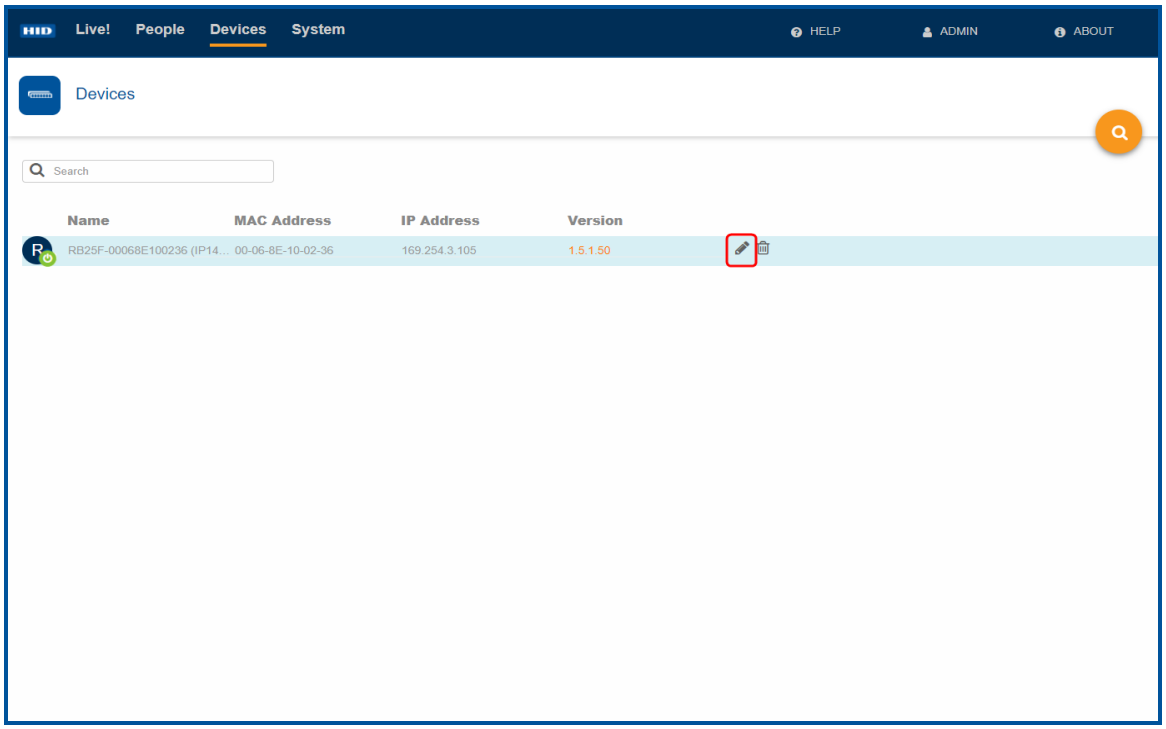
   Note: This operation will take around 25 minutes to complete.
5. Click **OK** when the update is complete.

Important: The device will be offline while the firmware update is in progress.

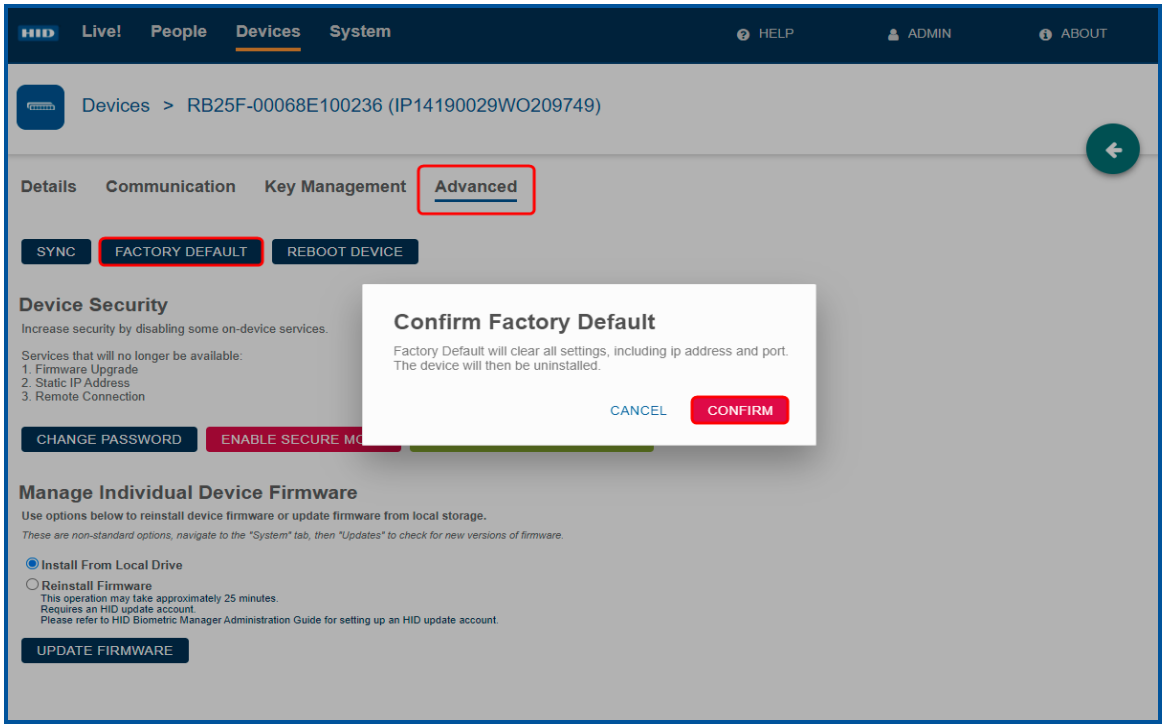
2.6.6 Reset a device

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 [ ] to access the device settings screen.



3. Click the **Advanced** tab and click **FACTORY DEFAULT**.
4. Click **CONFIRM**.

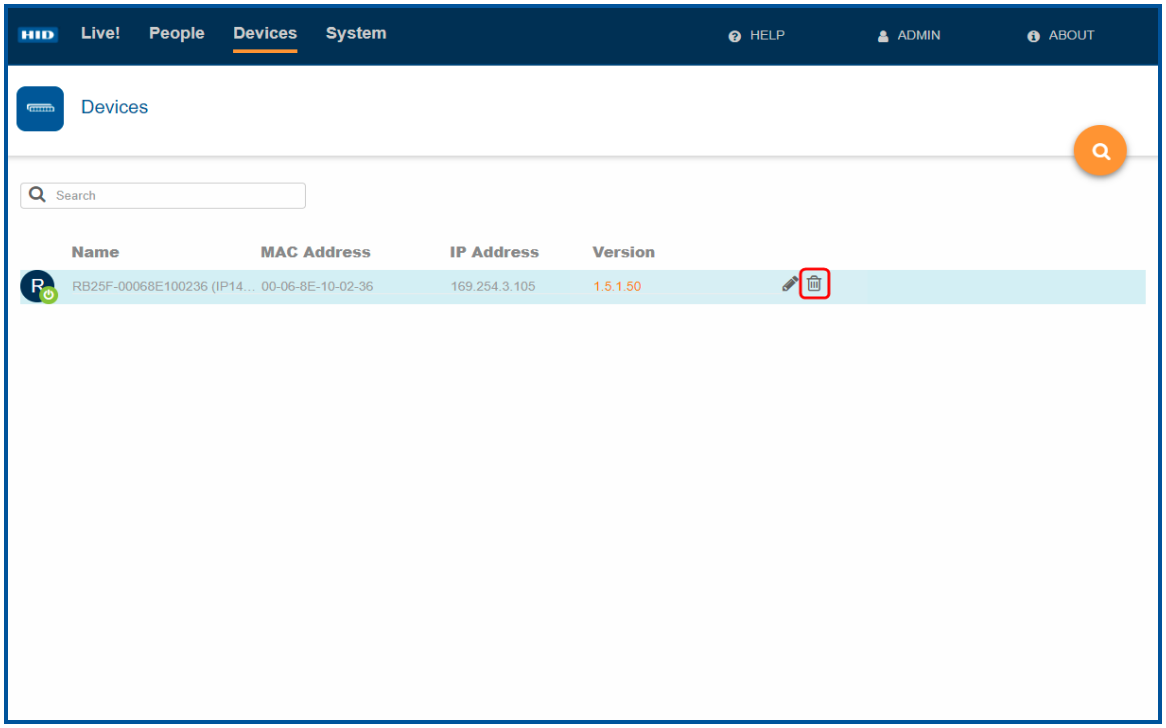


Note: Where communication between HID Biometric Manager and the Signo Biometric Reader 25B is not possible, factory default reset can be carried out at the reader, see *HID Signo Biometric Reader 25B User Guide* (PLT-04900).

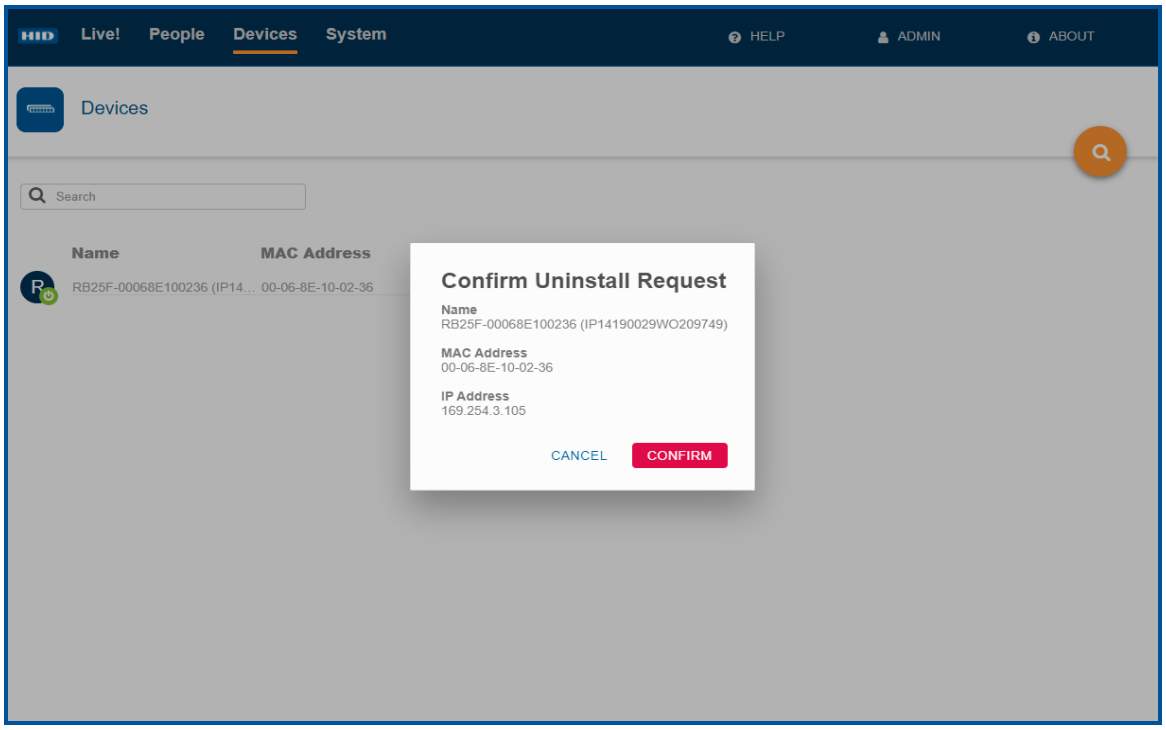
2.6.7 Uninstall a device

To uninstall a device (possibly as a means to resolving issues by removing the device from the server 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 [ ] associated with the device you want to uninstall.



3. Click **CONFIRM**.



4. Click **OK**.

Note: If all devices have been uninstalled in HID Biometric Manager, you will have the option to install a devices on the **Devices** screen, see **2.6 Device installation and configuration**.

2.7 Setting static IP for HBM network

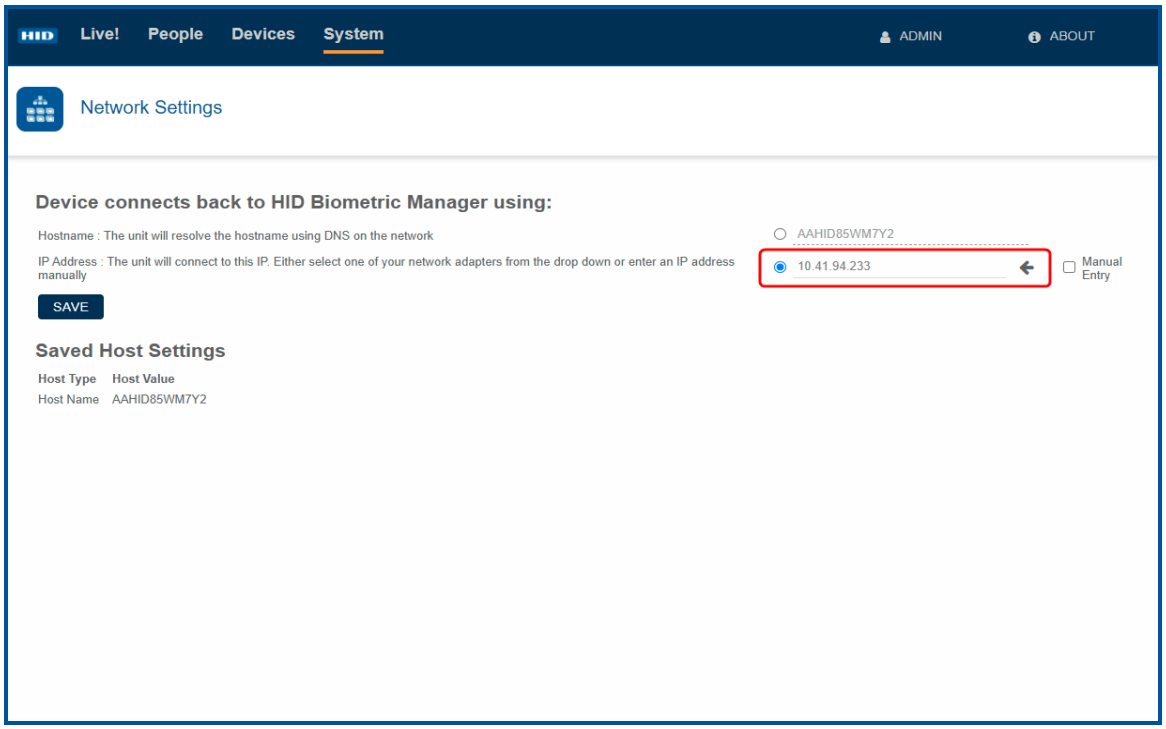
HID Biometric Manager has a feature that allows each device and the HBM network to have a static IP address. When all connected devices and the HBM network are configured with the correct static IP settings, the system continues to operate if the DHCP server is turned off.

Note: This must be set before installing any devices. If this is changed after device installation, devices must be re-installed.

Note: For all network setting changes, make sure that the Signo Biometric Reader 25B stays connected to the HBM server that it was configured to.

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: Select the **Manual Entry** check box to manually enter the IP Address.

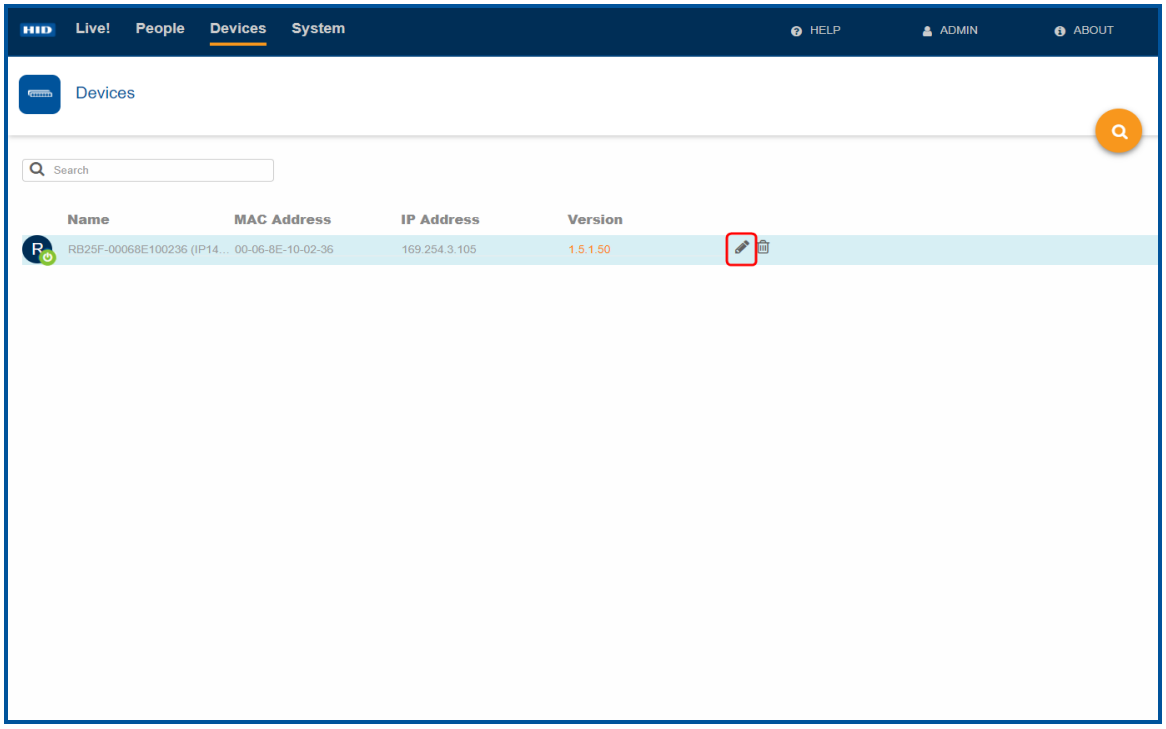


3. Click **SAVE**.

2.8 Setting static IP for a specific device

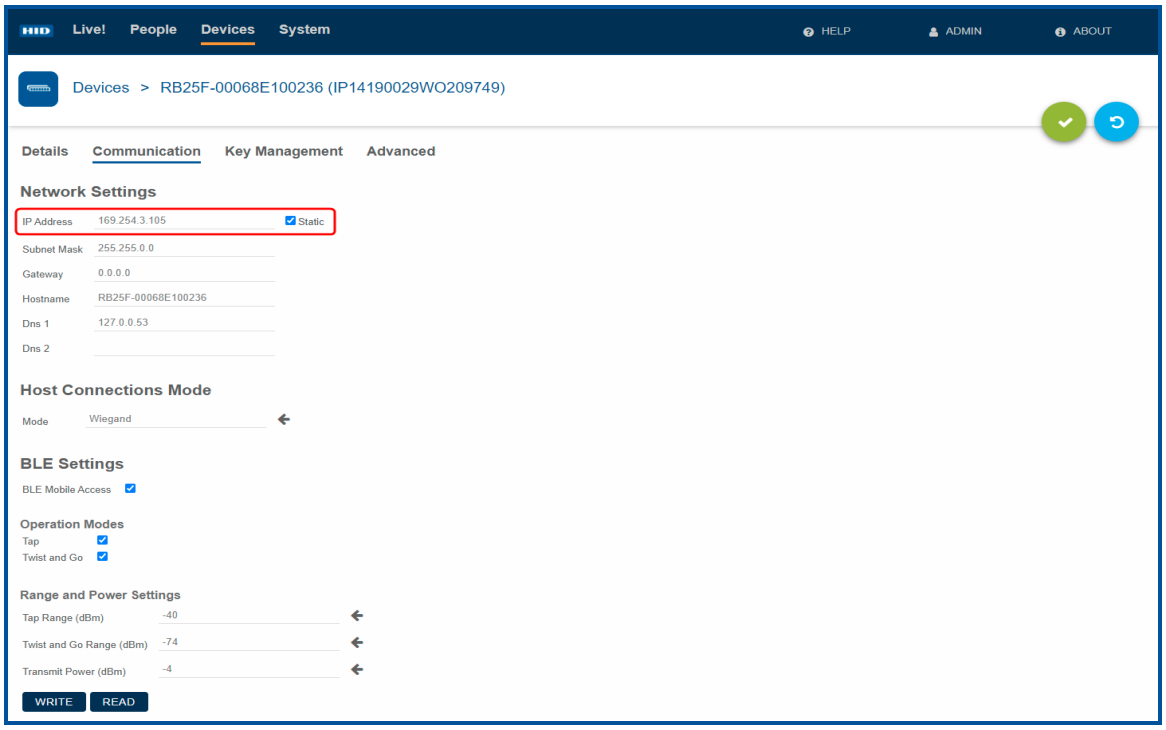
To set the static IP for an individual device:

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



3. On the **Device** page, select the **Communication** tab.
4. Select the **Static** check box to set the static IP address.

   Note: The IP address can also be changed to a user selected value.


Live!
People
Devices
System
HELP
ADMIN
ABOUT
Devices > RB25F-00068E100236 (IP14190029WO209749)
Details
Communication
Key Management
Advanced
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
WRITE
READ

5. Click .

2.9 Enrollment

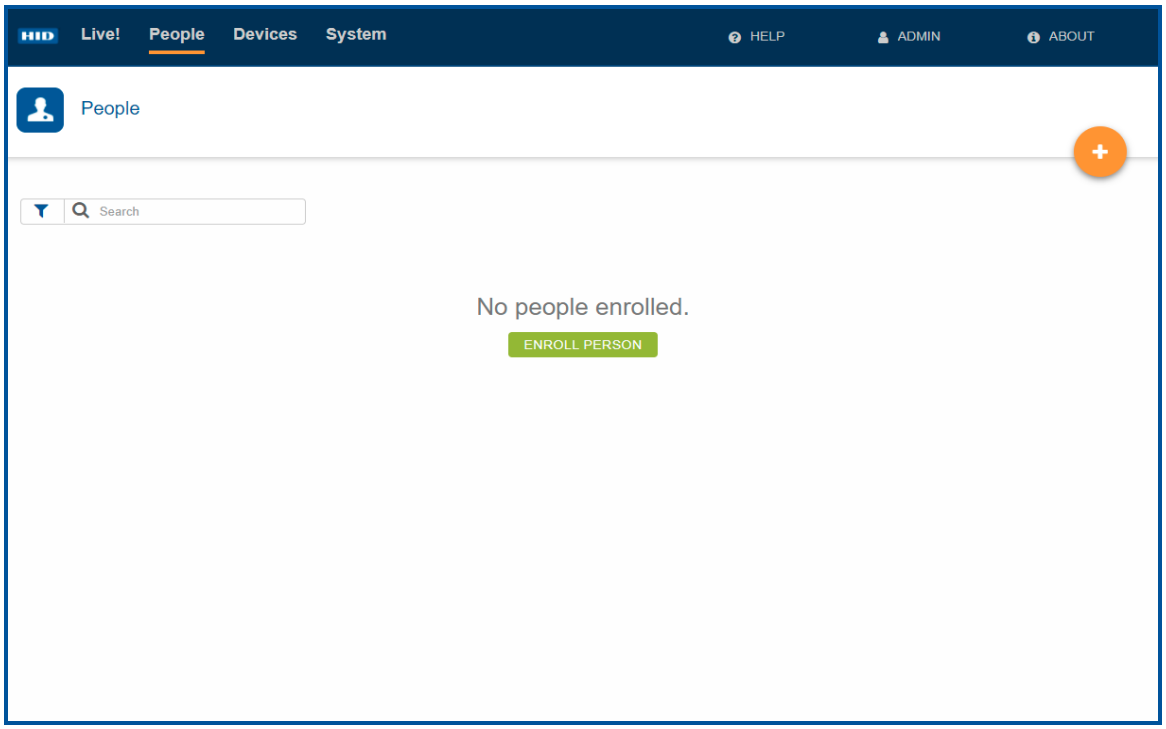
Enrolling people in the system, adding credentials, and collecting associated biometric data can be carried out by an **Administrator** operator or an **Enrollment** operator.

Note: Make sure your firmware is up to date before enrollment.

2.9.1 Enroll people

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

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

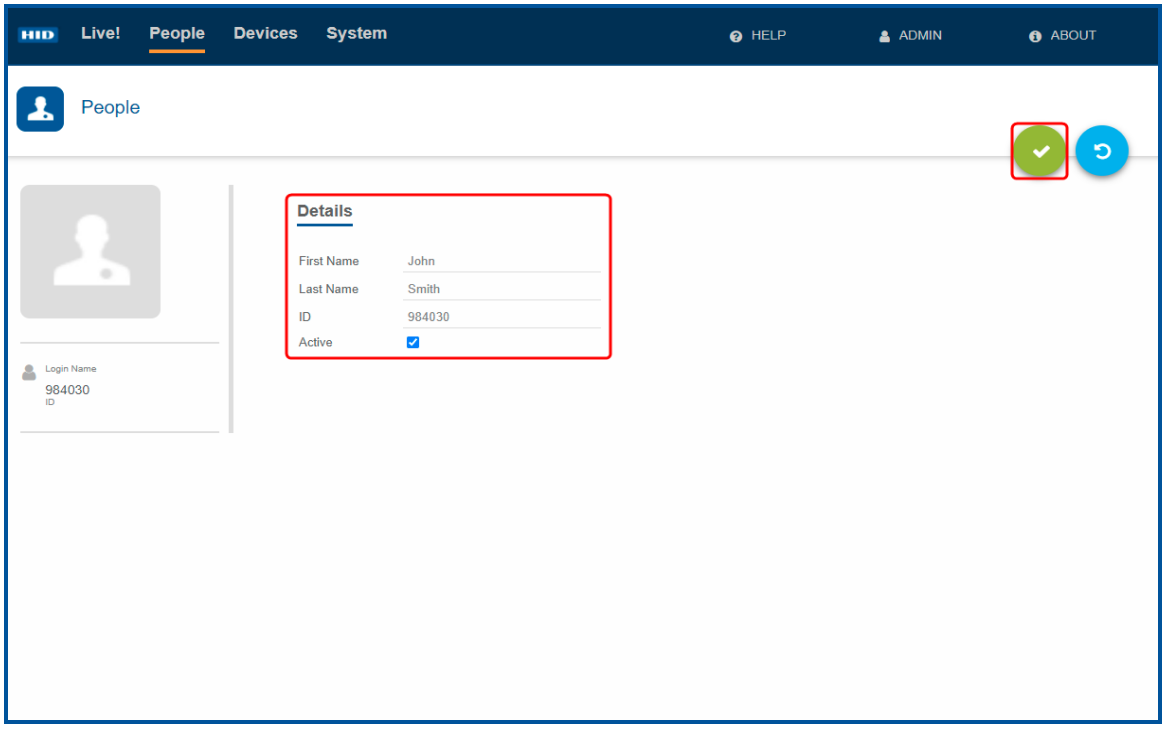


4. Enter the persons details (**First Name/Last Name**) and an **ID** number.

   Note: An **ID** number is sent when an enrolled finger is presented without a card set up.
5. Select **Active** to make this enrolled person active in the system.

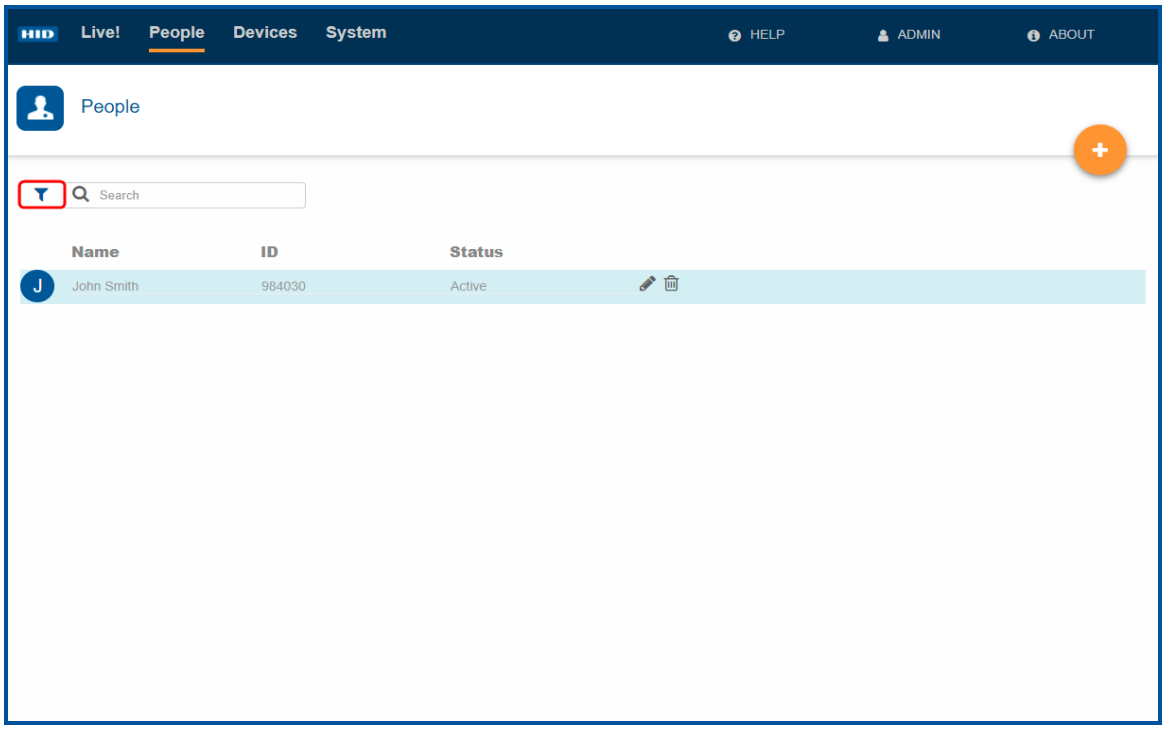
   Note: If **Active** is deselected the enrolled person will have an inactive status in the system and the person's record is not displayed on the **People** screen.

6. Click .



7. The enrolled person record is displayed on the **People** screen. To add additional people, click 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.



2.9.2 Enroll Cards

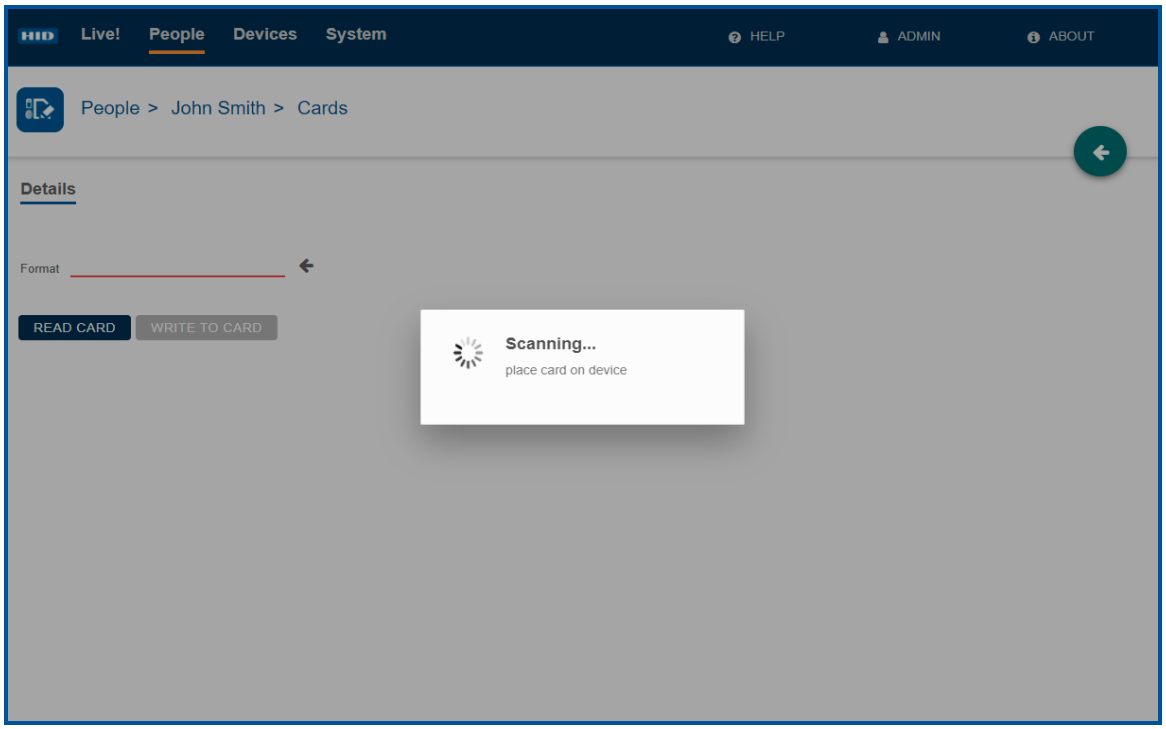
1. On the **People** screen select a displayed person record.
2. On the **Cards** screen click **ADD CARD**.
3. At this point on the **Details** screen you can either scan a card to obtain the card details or, if no card is available, manually enter card details.

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.

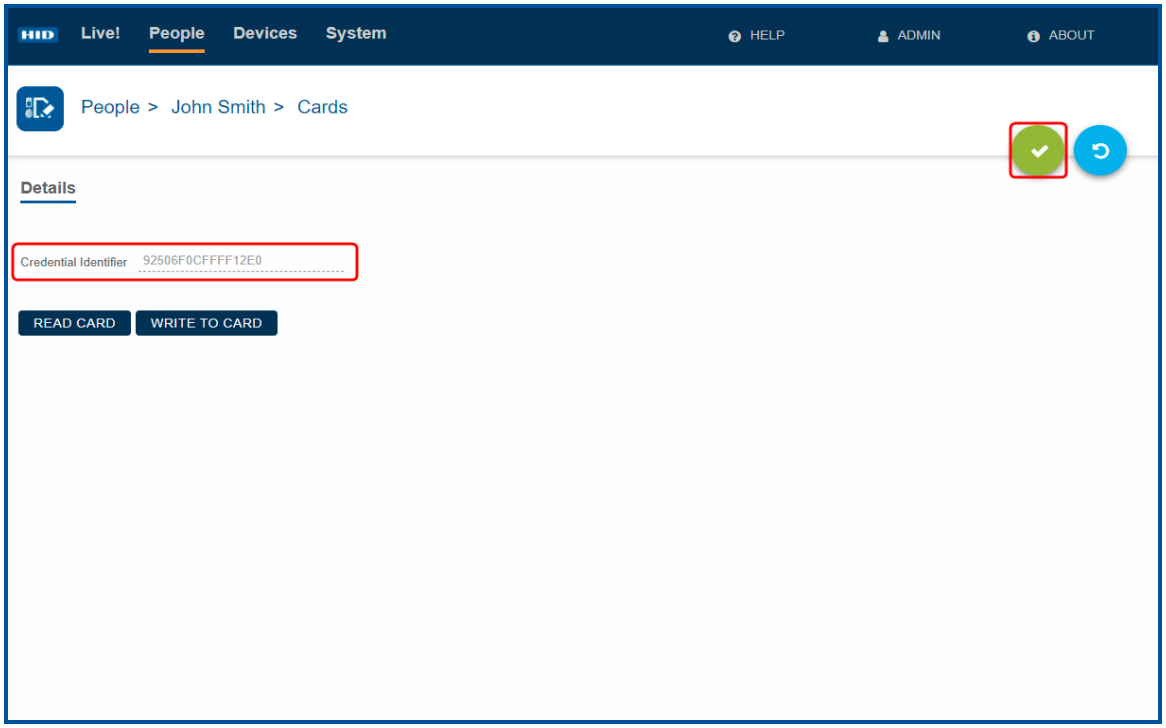
2. Within five seconds, present a card to the Signo Biometric Reader 25B device.

   Note: The card types supported by the device is configured in the device profile settings, see **2.21.2 Edit a device profile**.



3. Click .

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

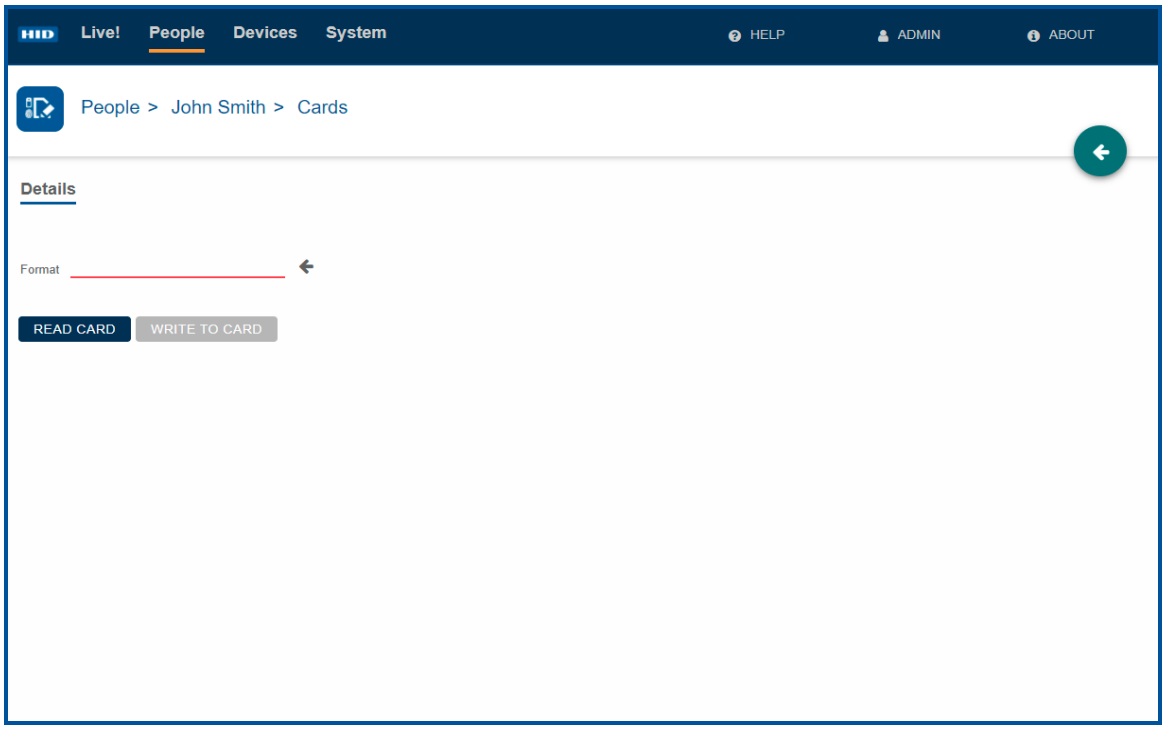


The operator can now collect and add biometric data associated with this enrolled person, see **2.10.1 Enroll Biometrics**.

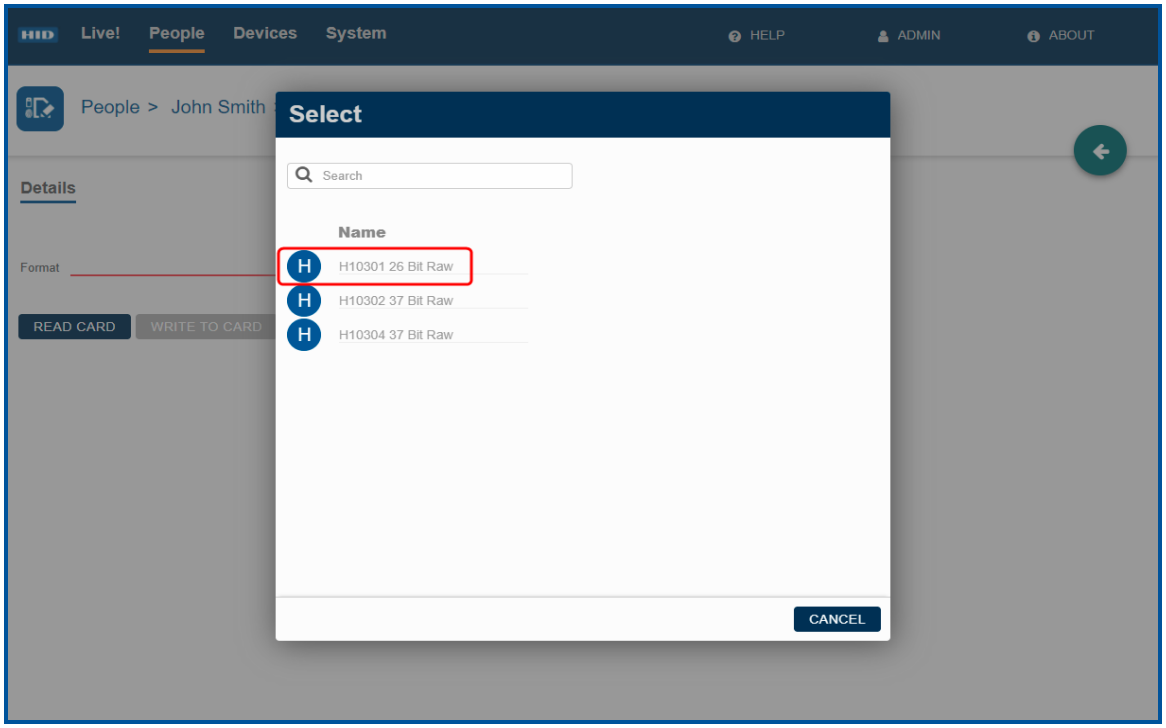
Manually enter card details

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.

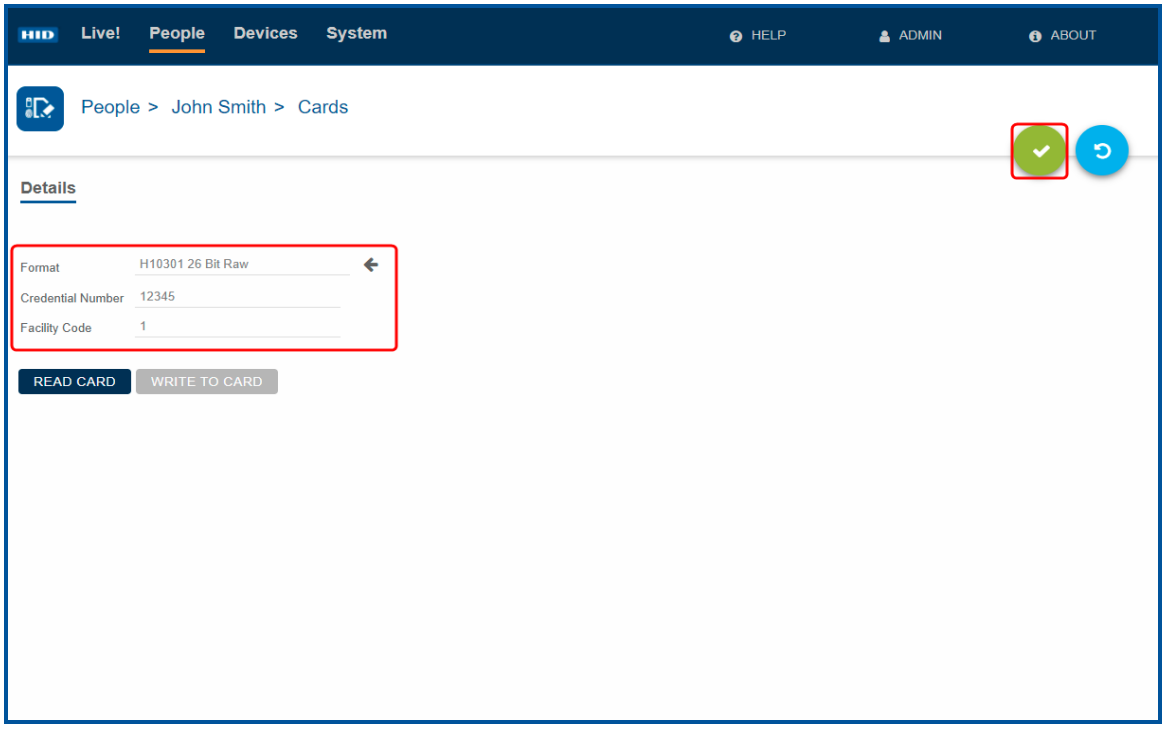


2. Select the required **Credential Format**.



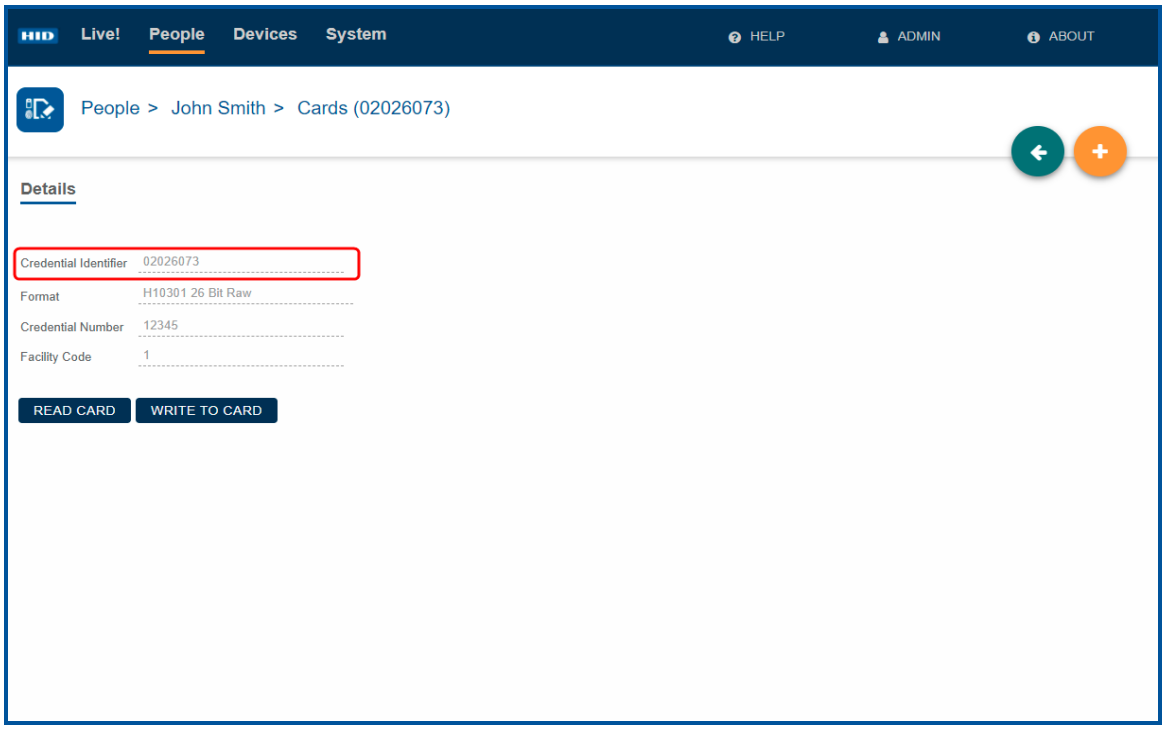
3. Enter a **Credential Number** (decimal) and if displayed, enter the **Facility Code**.

4. Click 



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 be present in the third party PACS software running on the PACS Server.



2.9.3 Install SIGNO-B-USB Module

Note: Enrolling fingerprint templates using the USB module only works with the Signo-B-USB enrollment device.

The Signo-B-USB fingerprint reader can be used to enroll biometrics to HBM.

To install the USB module:

1. Log in to HBM as an enrollment operator.
2. Click **System** > **Install USB Module**.
3. Follow the instructions given in the UI to complete the USB module install.

To enroll people, see **2.10.1 Enroll Biometrics**.

Note: HBM defaults to the SIGNO-B-USB for enrollment when it is enabled and the device is connected, even if there is a Signo Biometric Reader 25B fingerprint reader connected.

2.10 SIGNO-B-USB Enrollment

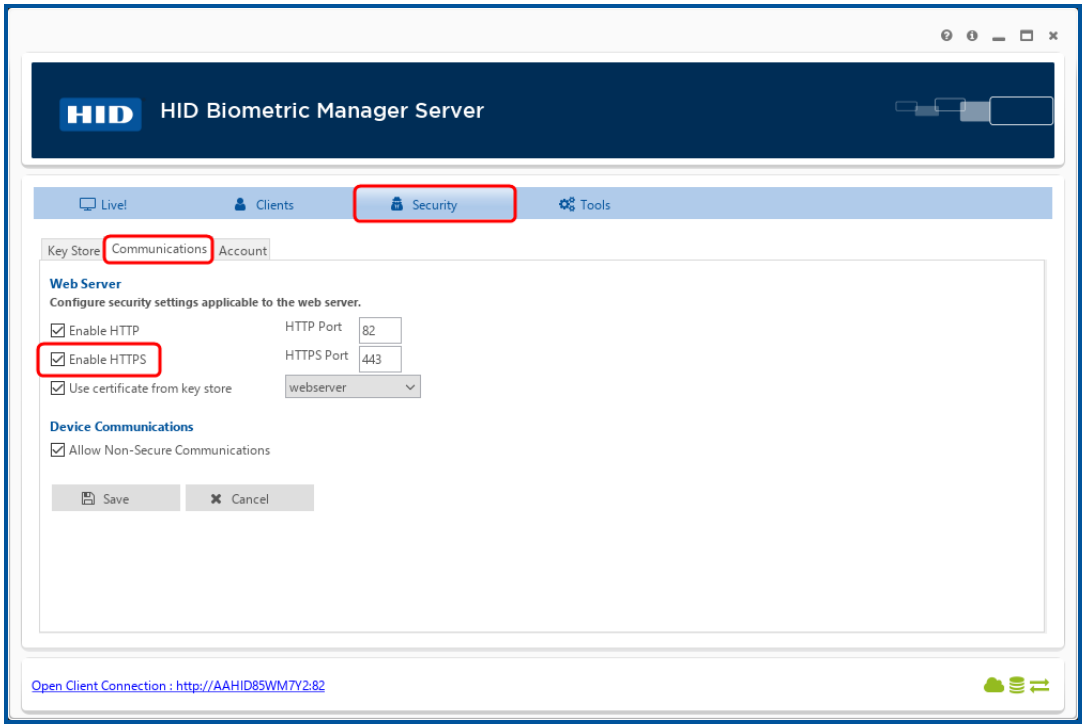
This allows your enrollment operator to enroll templates using the SIGNO-B-USB fingerprint reader. This feature uses HBM on HTTPS and uses web sockets to communicate with your devices.

Note: If the SIGNO-B-USB is being used for enrollment, it must be authorized for the enrollment workstation and operator, by a system operator.

Note: Multiple SIGNO-B-USB fingerprint readers can be used to support the need for multiple enrollment stations.

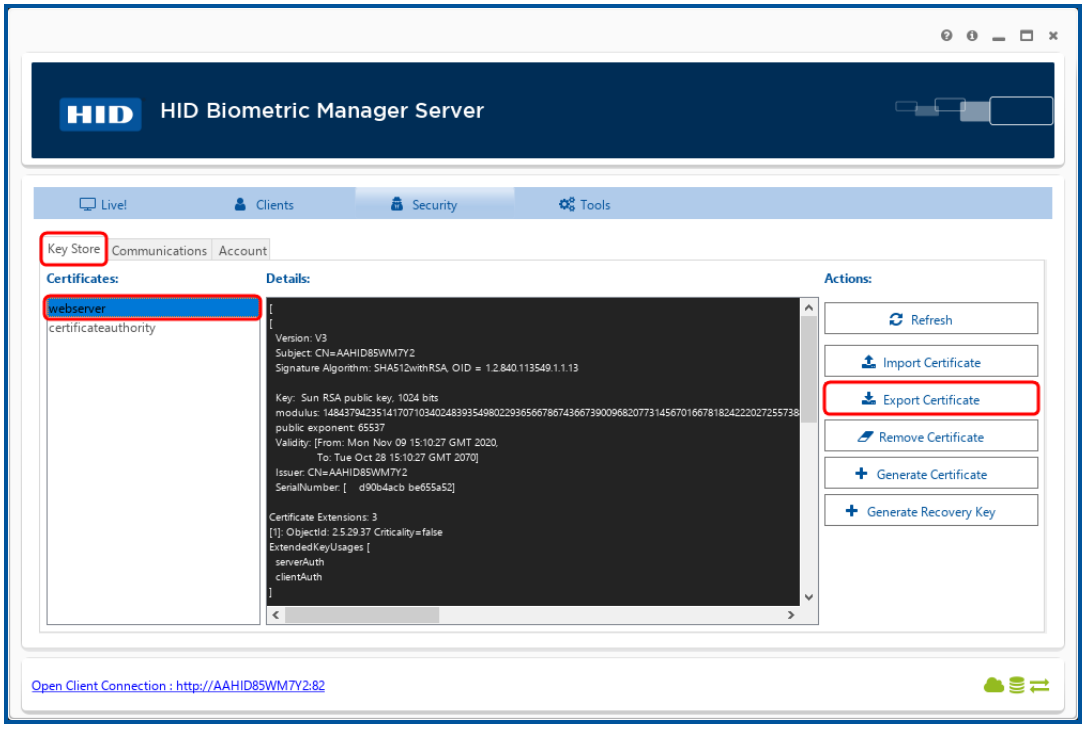
To enable this feature:

1. Login in as Administrator
2. Click **Security** > **Communications** in the HID Biometric Manager Server window.



3. Tick the **Enable HTTPS** check box.
4. Select the **Key Store** tab.

5. Click **webserver**.



6. Click **Export Certificate**.
7. Select a location for the certificate and enter a **Password**.
8. Import the certificate to your chosen web browser.

   Note: To import the new certificate, go to your browsers settings and follow the process for importing certificates.
9. Restart the browser.
10. Confirm that HBM is running in HTTPS.

2.10.1 Enroll Biometrics

One of the main features of HBM is enabling the enrollment of a fingerprint for authentication and access control when using the Signo Biometric Reader 25B.

There are two ways to enroll the biometrics of a user:

1. Signo Biometric Reader 25B reader.
2. SIGNO-B-USB desktop enrollment reader.

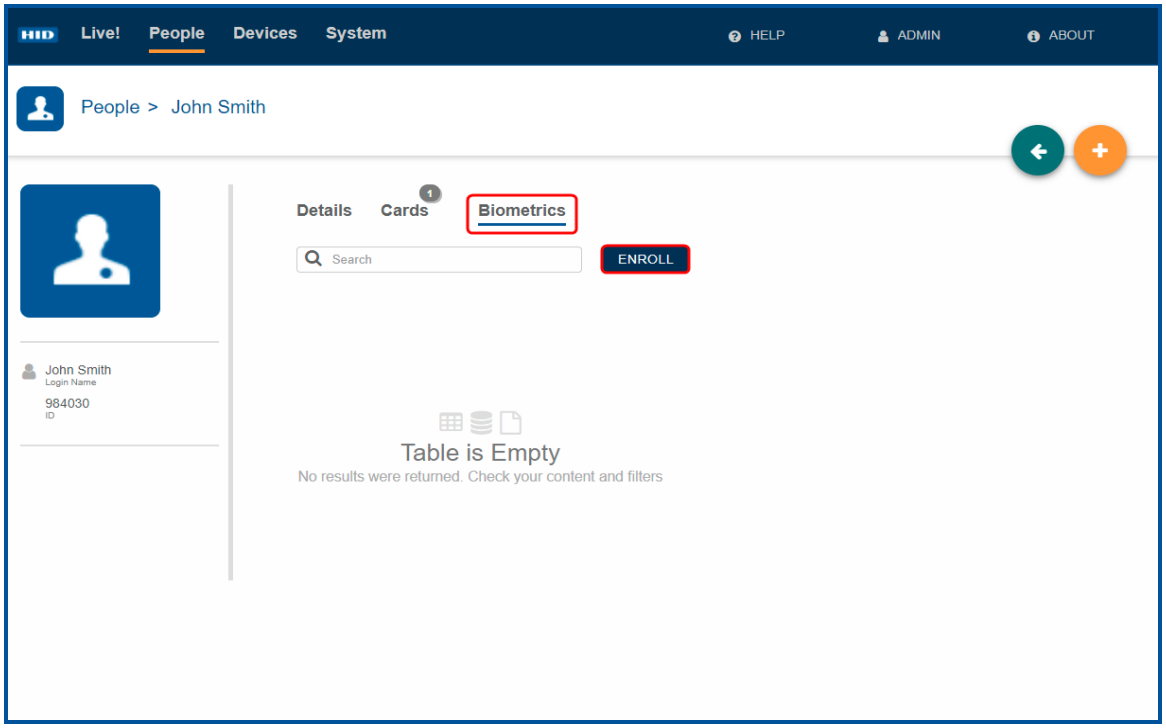
   Note: HBM will use the SIGNO-B-USB reader by default. To use the Signo Biometric Reader 25B for enrollment, you can select it at the start of enrollment.

After enrollment, the user record containing the user information and biometrics are encrypted and stored in the HBM server database by default, for distribution to the connected Signo Biometric Reader 25B devices.

Note: The templates are encrypted when stored in the server and device databases by default.

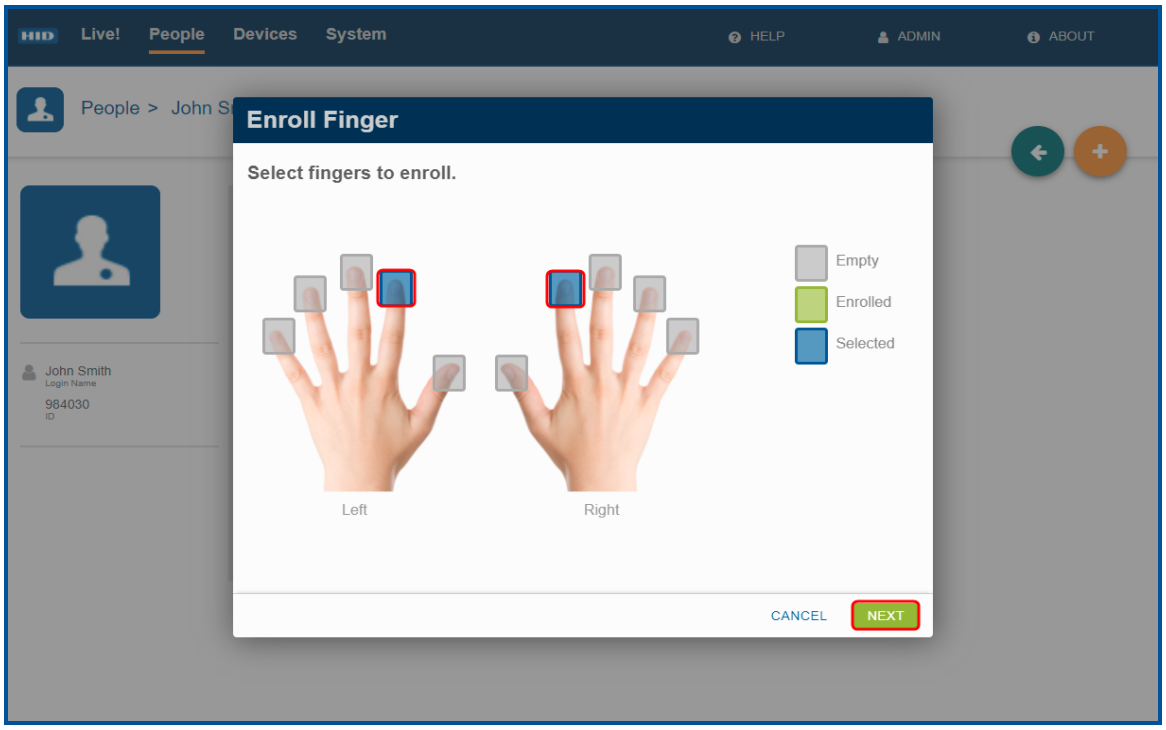
Note: Three templates with 10 fingerprints each can be enrolled per reader.

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



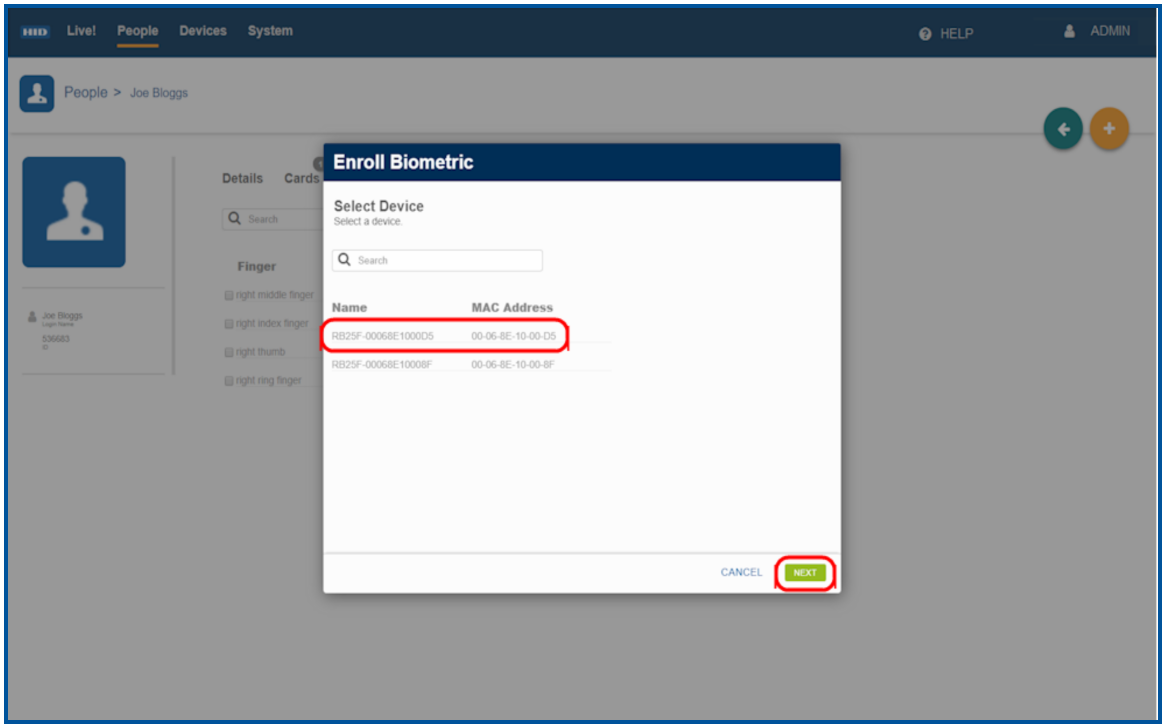
4. In the **Enroll Biometric** pop-up window select the fingers you wish to enroll and click **NEXT**.

   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.



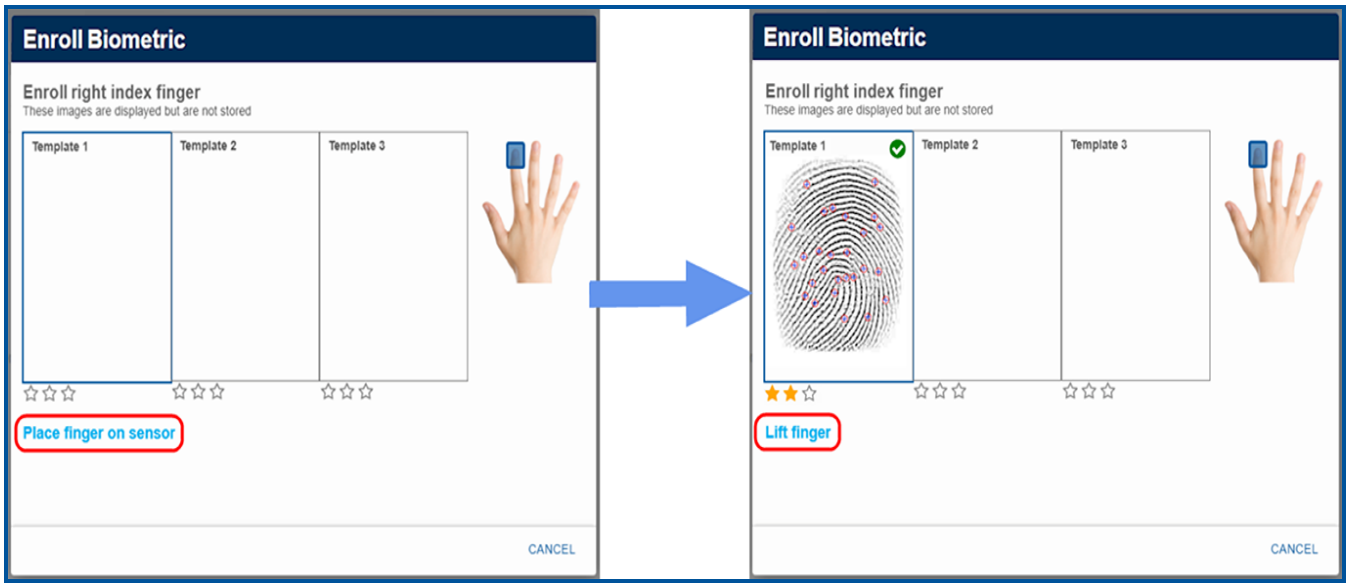
5. Select a device from the displayed list and click **NEXT**.

   Note: Device names can be changed to a logical name for easier identification, see **2.6.3 Configure device settings**.



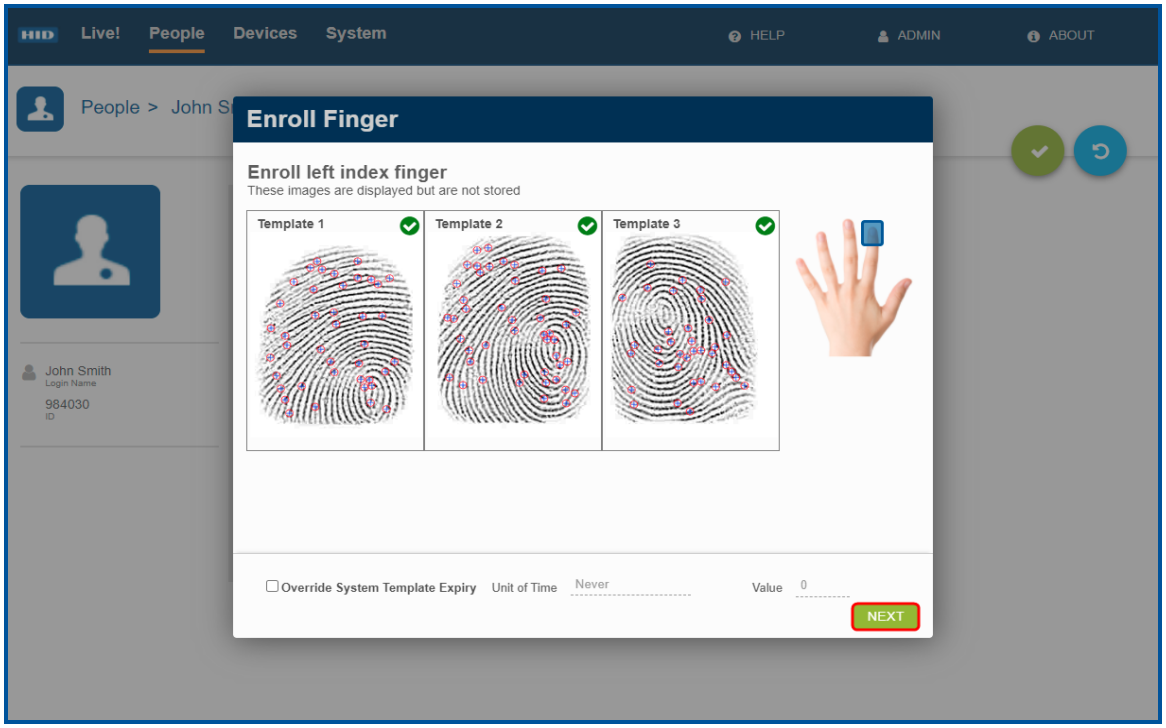
6. For the highlighted finger you will be prompted to **Place finger on sensor** followed by **Lift finger**. It is recommended that you follow the on-screen prompts, in the correct sequence, to ensure a successful finger scan.

   Note: For information regarding the correct method of presenting fingers to the scanner during the biometric enrollment process, see *HID Signo Biometric Reader 25B User Guide* (PLT-04900).



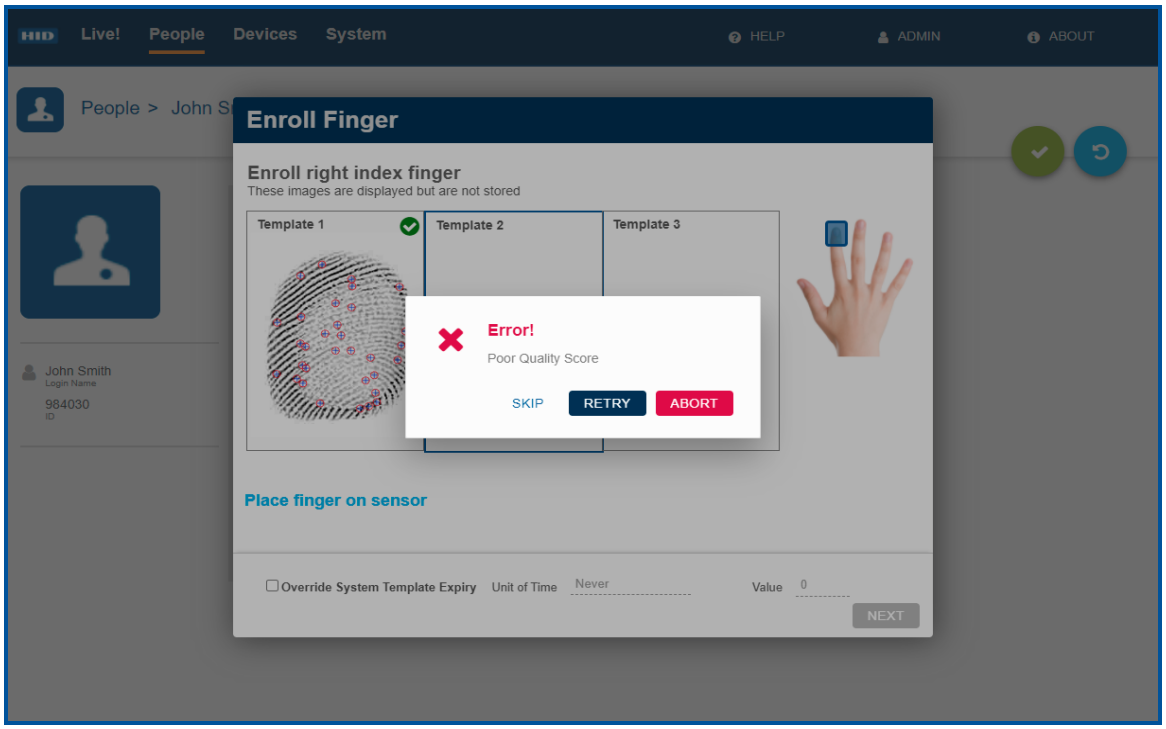
7. Continue to follow the on-screen prompts until you have successfully scanned the first finger three times. Click **NEXT**.

   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.



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. If there is a problem when scanning a finger, a pop-up window will give the options to **SKIP** that finger, **RETRY** to scan again, or **ABORT** to cancel enrollment.



10. 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.

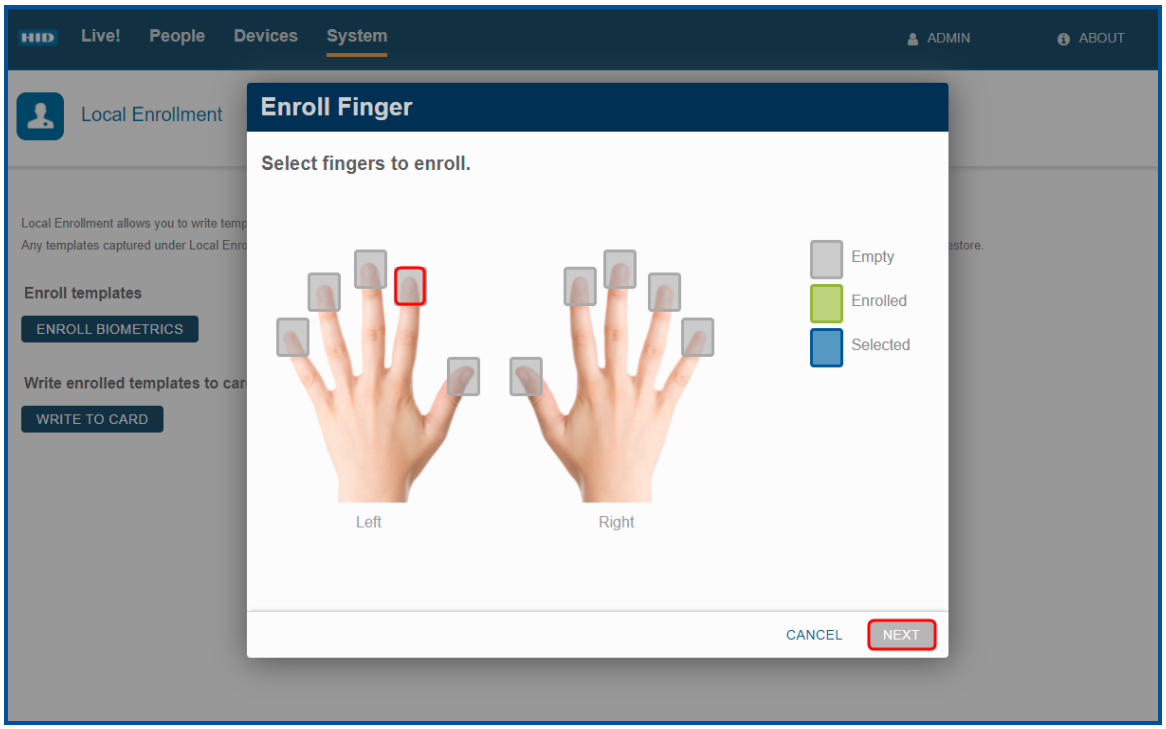
2.10.2 Local enrollment

During regular user enrollment, the user fingerprint template is stored in the server database and downloaded to connected devices to allow template on device authentication using Finger Only or Card and Finger authentication modes. This allows HBM to write templates to a card, for users that are not enrolled in the system such as guests or visitors.

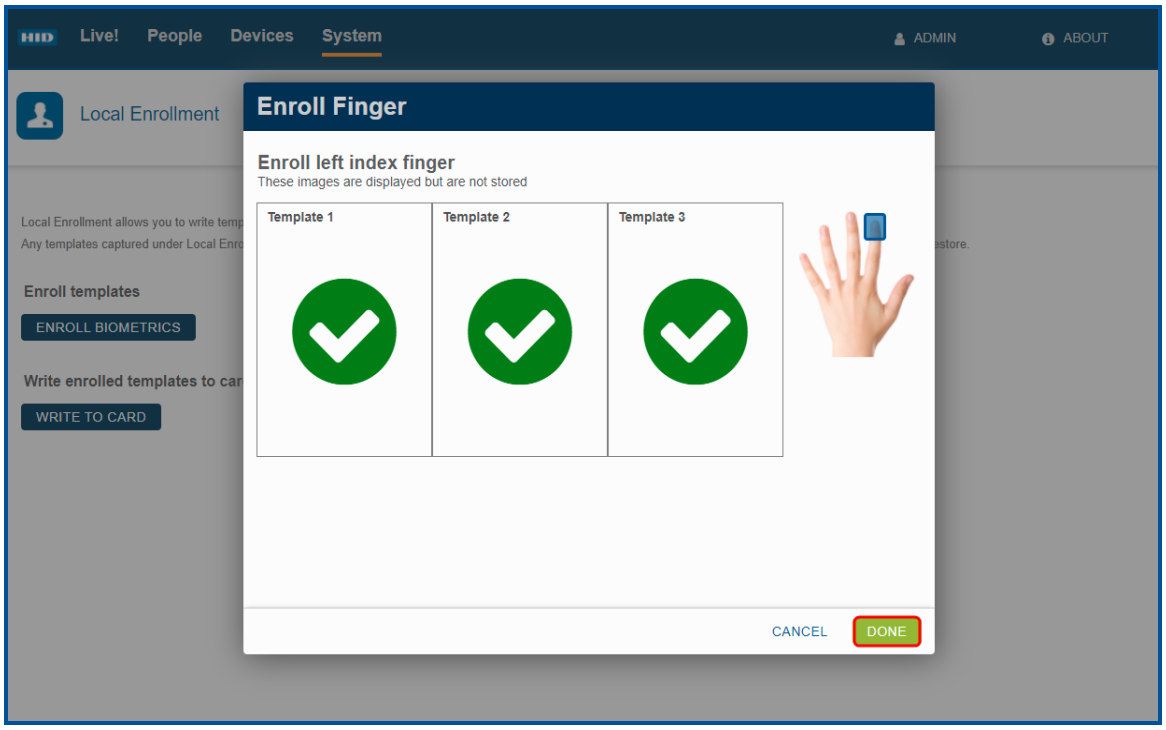
Note: Only use local enrollment with the Template on Card authentication mode. If the authentication mode is changed after a local enrollment, the user will have to be enrolled again.

Note: The **Live!** event transaction will only list the PACS card information for an access event.

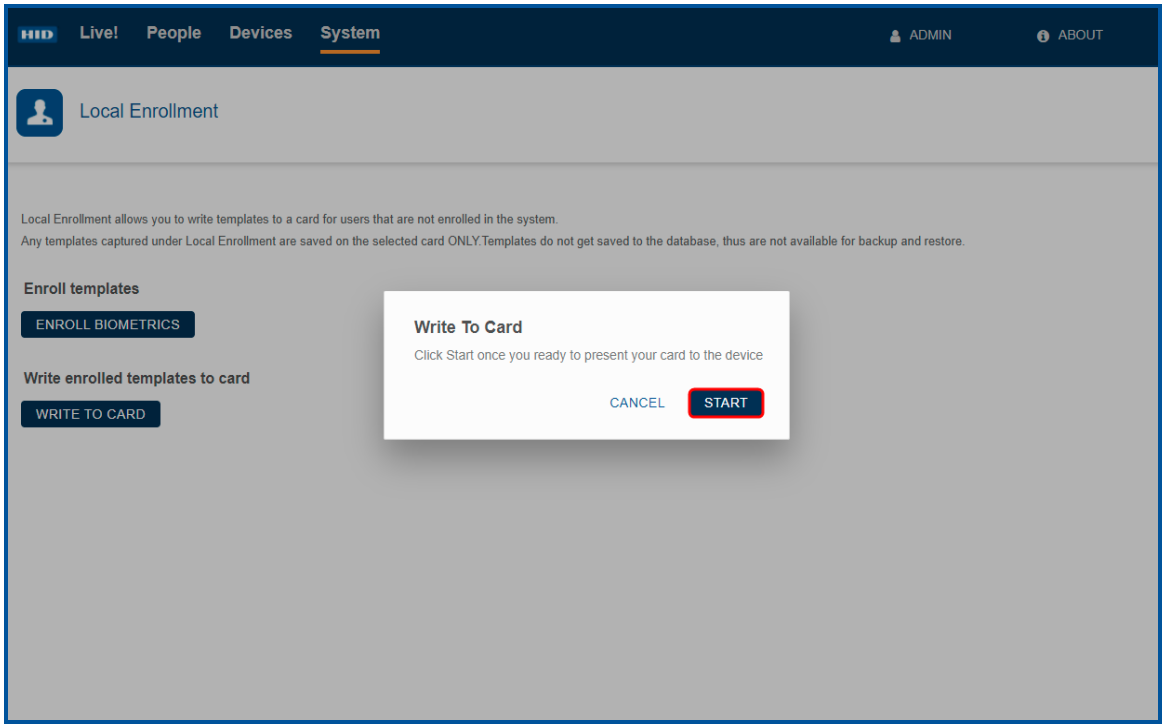
1. Click **System** > **Local Enrollment**.
2. Click **ENROLL BIOMETRICS**.
   Note: If you have more than one connected device, you will be prompted to select one to use for the enrollment.
3. Select which fingers you want to enroll and click **NEXT**.



4. Follow the on screen prompts to scan the finger.



5. Click **DONE** to close the template window.
6. Click **CONFIRM** to write the enrolled fingerprint template to the card.
7. Click **START** and present the card to the reader.

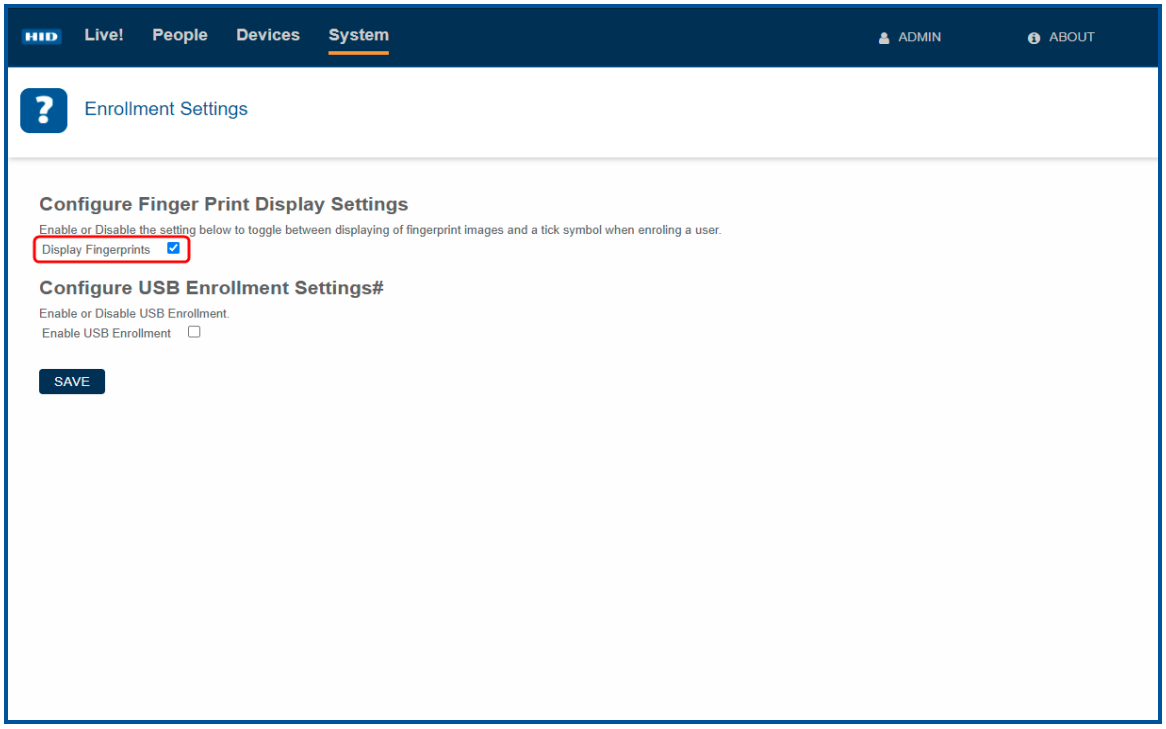


8. A pop-up window will appear when the enrollment is successful.
   When presented, the credential will appear in the **LIVE!** feed as **No User Name(Unknown)**. The fingerprint template is stored locally in the memory of the Signo Biometric Reader 25B reader and will not be added to the database.

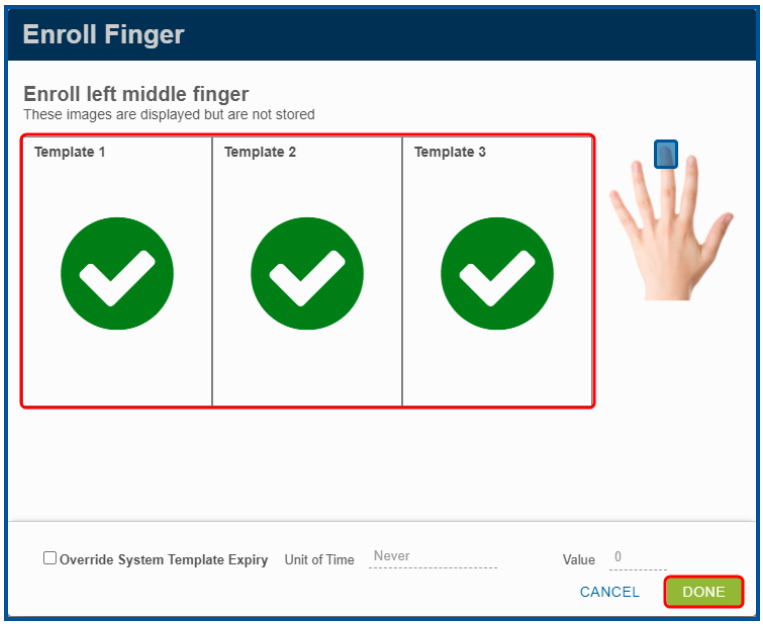
2.11 Preventing user fingerprint display during enrollment

During fingerprint enrollment the User Interface (UI), displays in real time the fingerprint that is being enrolled. There is the option to prevent the fingerprint image being displayed for privacy.

1. Go to **System** > **Enrollment Settings** and select the **Display fingerprints** tick box for the fingerprints to be displayed. Deselect the tick box to remove the fingerprint display.



2. Click **SAVE** to finish.
3. With the **Display fingerprints** deselected, the fingerprints will be replaced with a green tick once each scan of the finger has been completed.



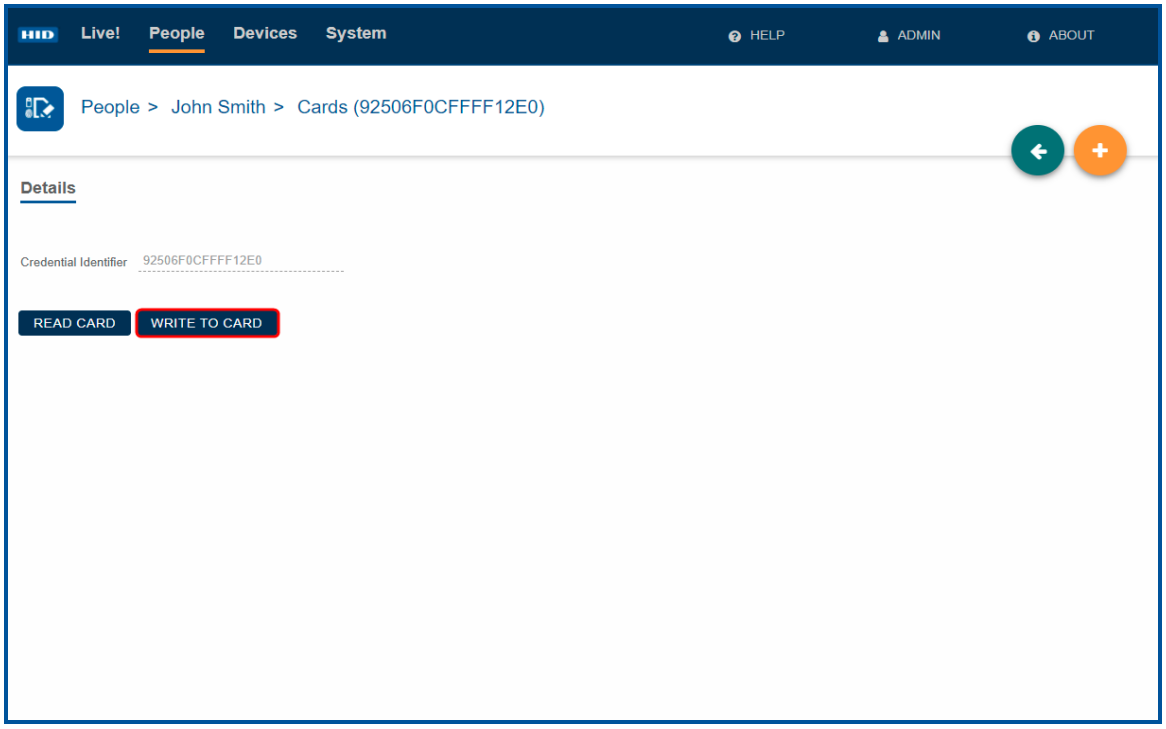
4. Select **DONE** to Finish

2.11.1 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.

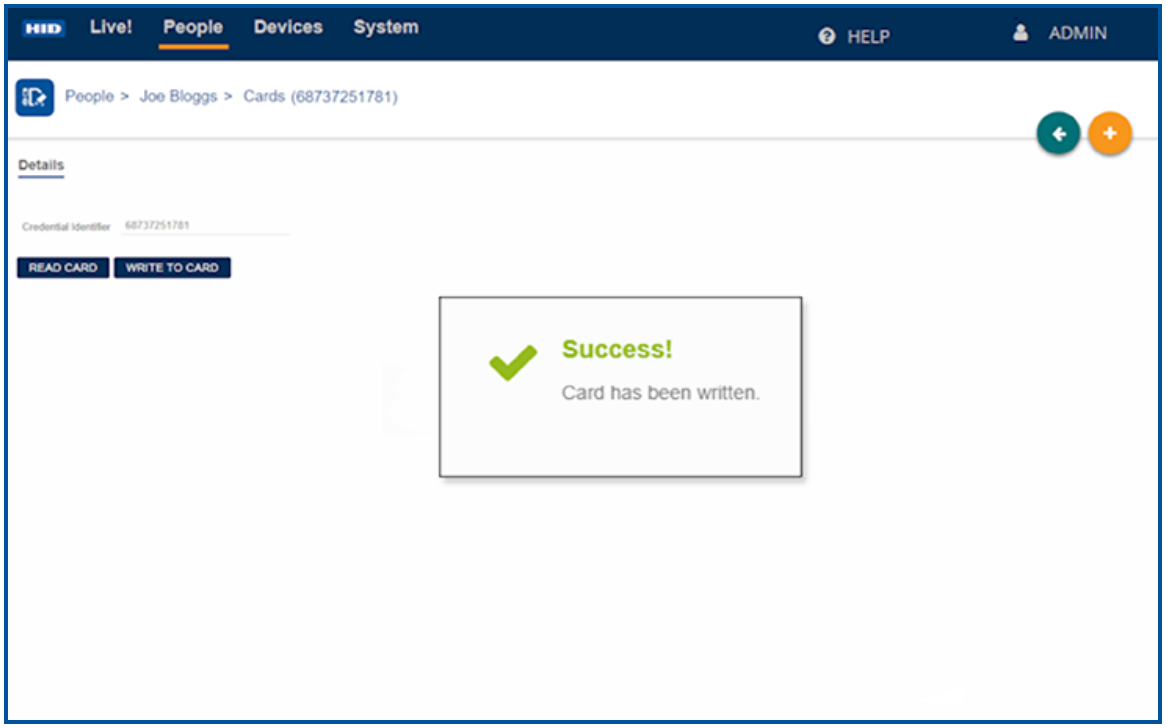
Note: Template on Card only supports Seos 8K (available since September 2017).

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



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

5. You will have approximately five seconds to present the supported card to the Signo Biometric Reader 25B device in order to write the profiles to the card. The LED bar will flash while writing to the card. Keep the card close to the reader until the LED bar returns to it's default color. You will be notified when the card has been successfully written to.



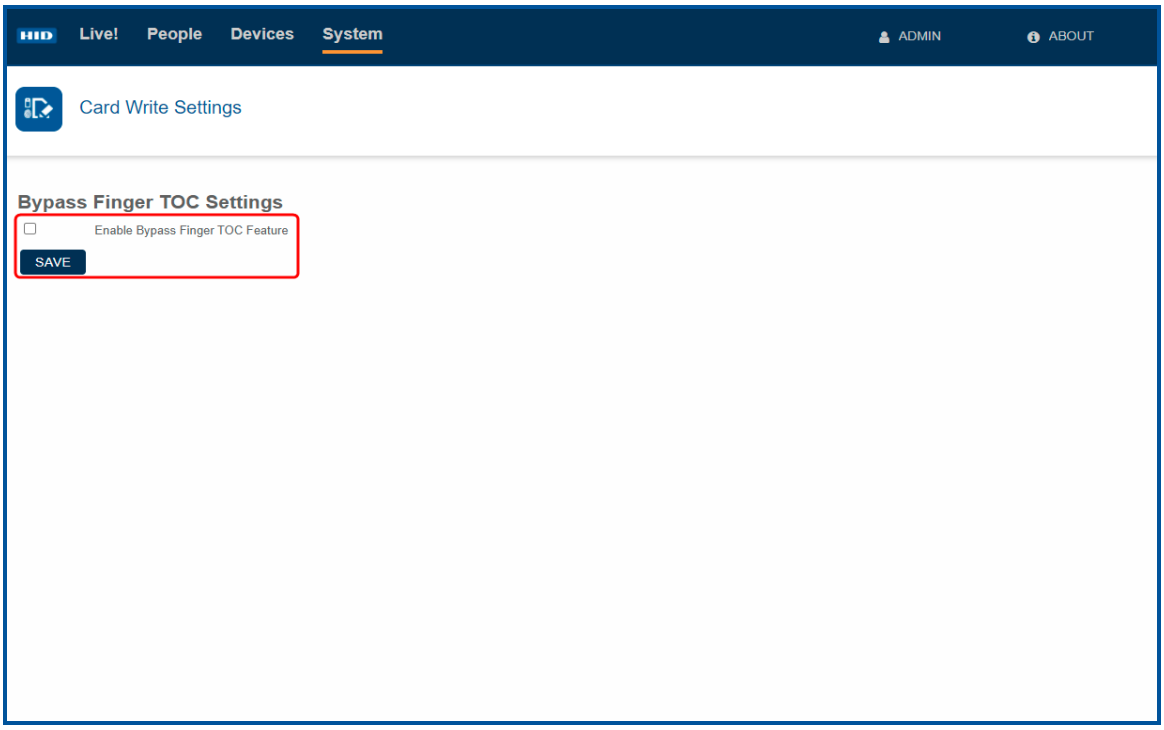
6. For a **Template on Card** authentication mode, the enrolled person can now enter the door by presenting this card, immediately followed by the correct finger scan on the Signo Biometric Reader 25B.

Note: When presenting the card and fingerprint, there is a time window of one second between card and fingerprint scan.

2.12 Bypass finger TOC

The option to bypass the fingerprint Template on Card (TOC) feature can be toggled on or off by going to **System** > **Security Settings** > **Card Write Settings**. The check box can be selected to enable the bypass or deselected to disable.

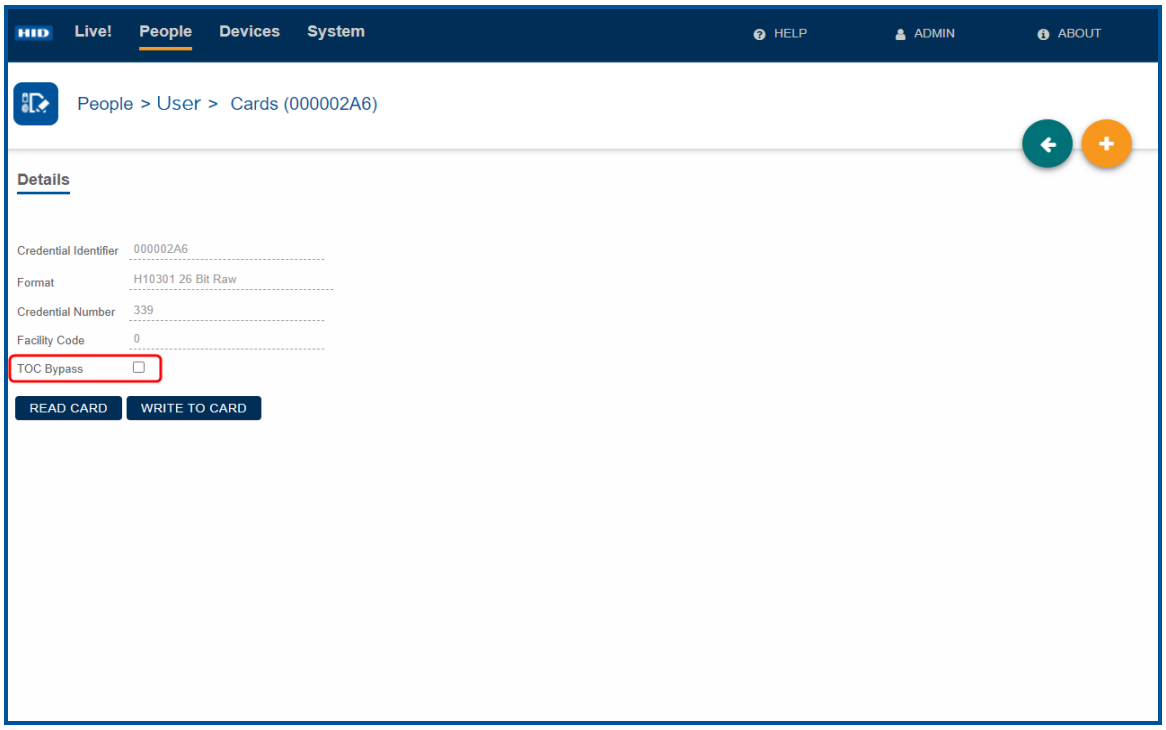
This allows an individual to be in **Card Only** mode if the **Device Profile** is set to **Template on Card** mode.



2.12.1 Enrollment without fingerprints

To configure enrollment without fingerprints for the **Bypass Finger TOC** feature:

1. Select the **2.12 Bypass finger TOC**.
2. Click **People** and select the required user.
3. Click **Cards** and select the required card.
4. Deselect **TOC Bypass**.



5. Click **WRITE TO CARD**.
6. Select the required device.
7. The finger scanner will illuminate when the card is read.
8. The **Live!** feed will register a Credential Read.

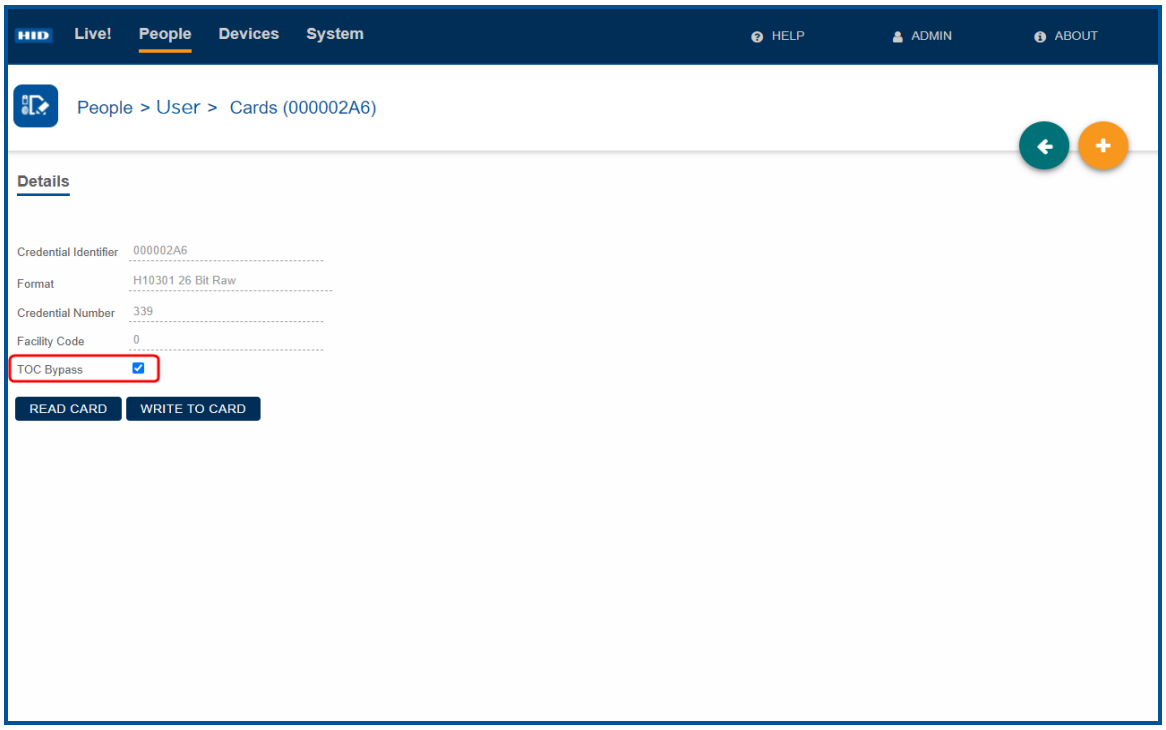
Note: If the **TOC Bypass** is selected, an alert message will appear stating that no templates have been enrolled when **WRITE TO CARD** is selected.

Note: If the **1.1 Bypass finger TOC** is deselected the **TOC Bypass** will not be available. An alert message will appear stating that no templates have been enrolled when **WRITE TO CARD** is selected.

2.12.2 Enrollment with fingerprints

To configure enrollment with fingerprints for the **Bypass Finger TOC** feature:

1. Select the **2.12 Bypass finger TOC**.
2. Click **People** and select the required user.
3. Click **Cards** and select the required card.
4. Select **TOC Bypass**.



5. Click **WRITE TO CARD**.
6. Select the required device.

   Note: If the **Bypass finger TOC** or the **TOC Bypass** is left deselected, when clicking **WRITE TO CARD** the **Select fingers to write** window will appear. Select a maximum of two fingers and select **WRITE TO CARD**.
7. Click **Live!** and scan the card.
8. Scan a finger.

   Note: An event will appear in the **Live!** feed for a Credential Read transaction followed by a Biomatch transaction.

2.13 BioTemplate settings

The BioTemplate settings can be found under **System** > **BioTemplate Settings**, and allows:

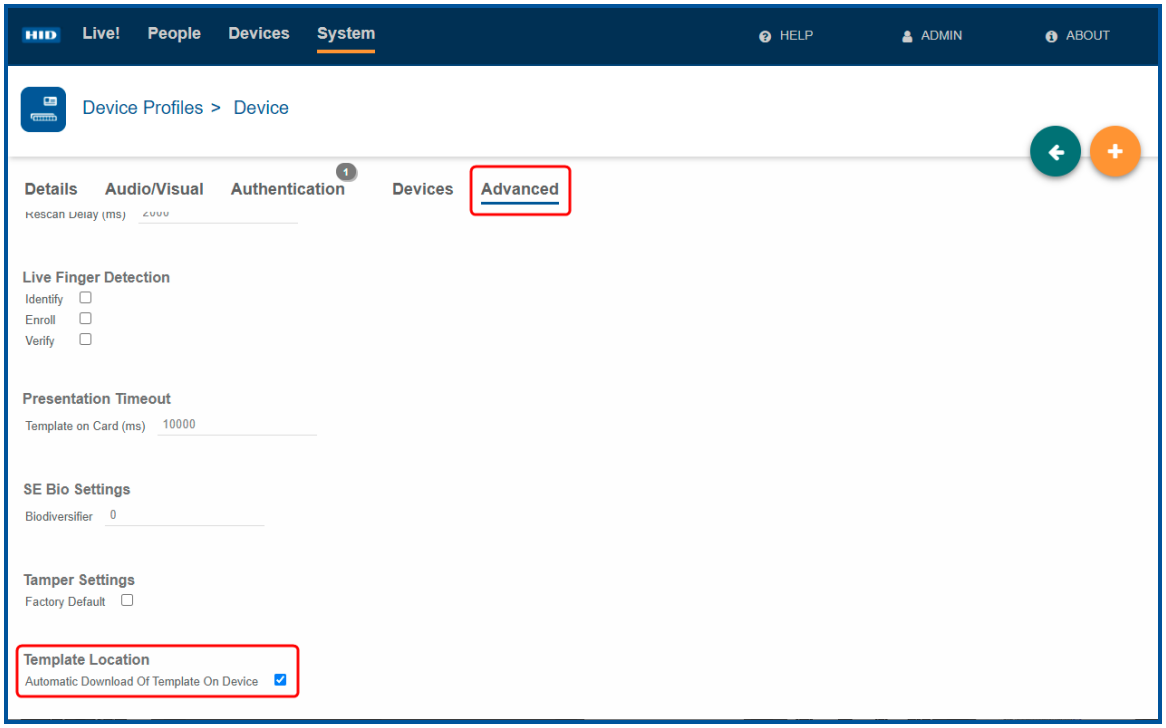
- Set a template expiry date.
- Schedule the deletion of expired templates.
- Delete all HBM database templates.

2.13.1 Auto download template

Enabled by default, this feature synchronizes HBM and connected devices. If auto download template is disabled the template synchronization with HBM is disabled and removes all templates from devices, and the authentication mode can not be set to any mode that requires a template on the device.

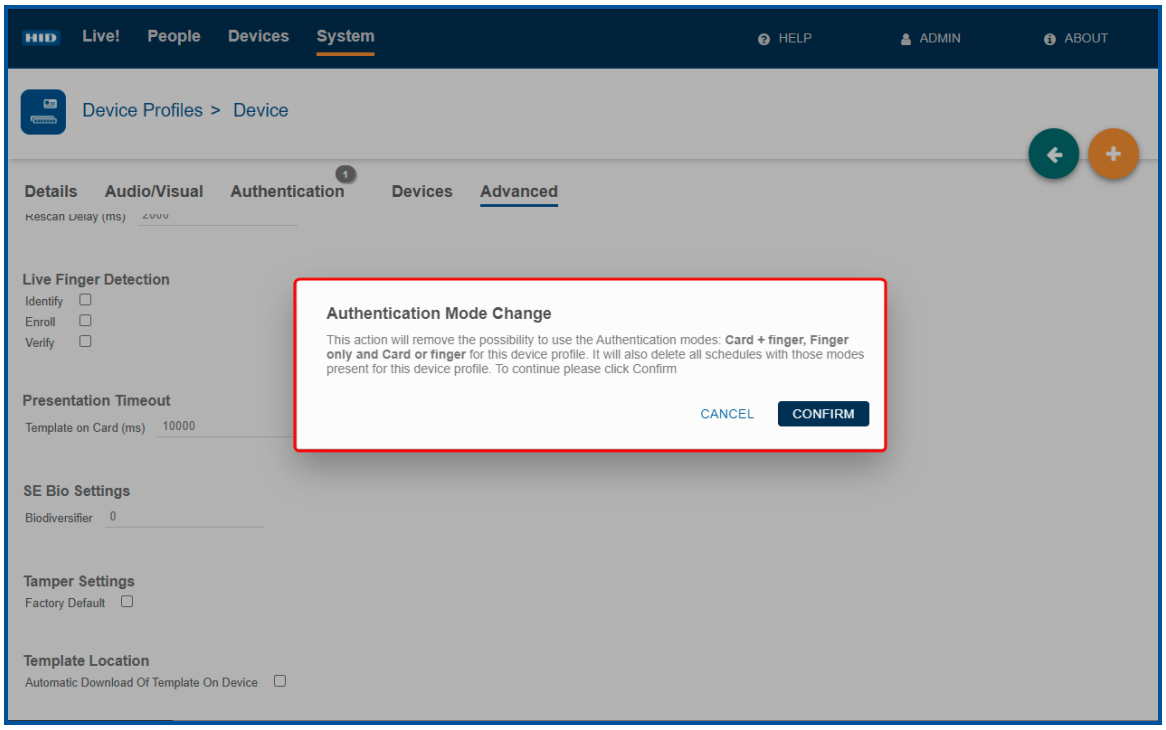
Before disabling the **Automatic Download of Template On Device** you must change your device profile **Authentication Mode** to **Template On Card**, or **Card Only**. You will be prompted by HBM to change it if you have not.

1. Navigate to **Devices** > **Device** Profiles and choose the profile you want to edit.
2. Click the **Advanced** tab.
3. Scroll down to **Template Location**.



4. Clear the **Automatic Download Of Template On Device** check box.

5. Read the Authentication Mode Change pop-up notice, then click **CONFIRM**.



6. Click .

You can verify this by going to the **Details** tab of the **Device Profile**, and selecting the **Authentication Mode**. There should only be two modes of authentication, **Template on Card** and **Card Only**.

Note: If the option is disabled, the authentication modes that require a user template in the device database are not available.

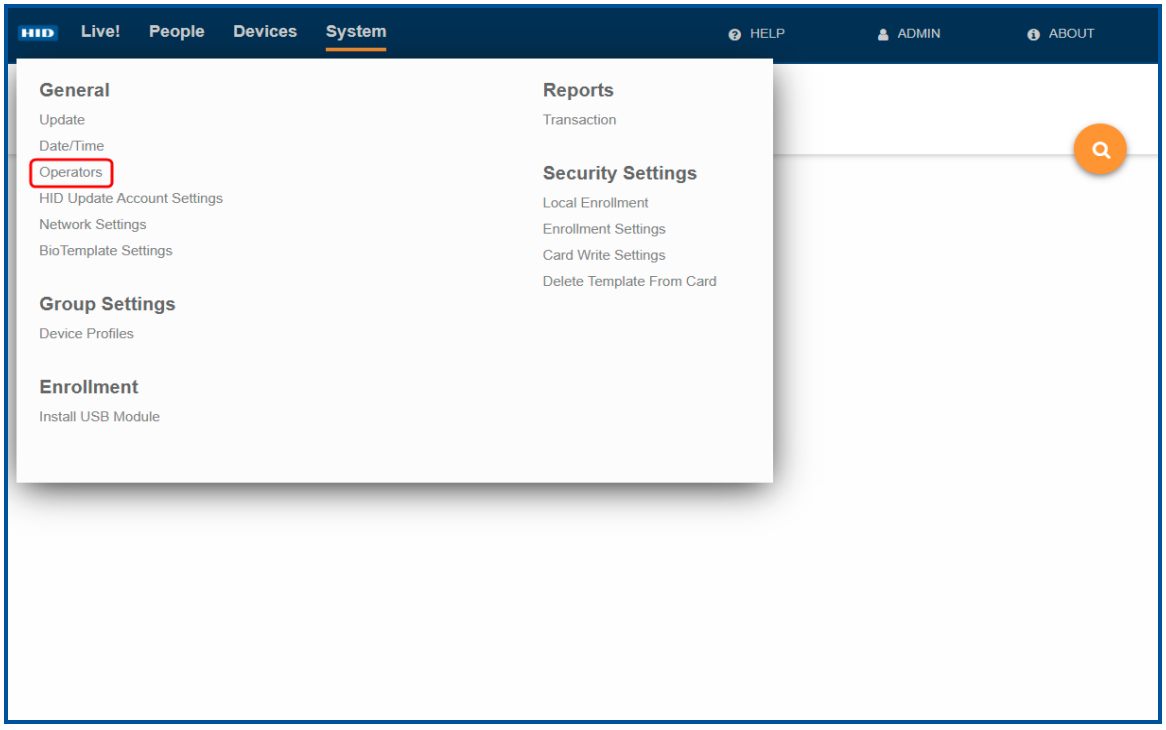
2.14 Create HID Biometric Manager operators

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

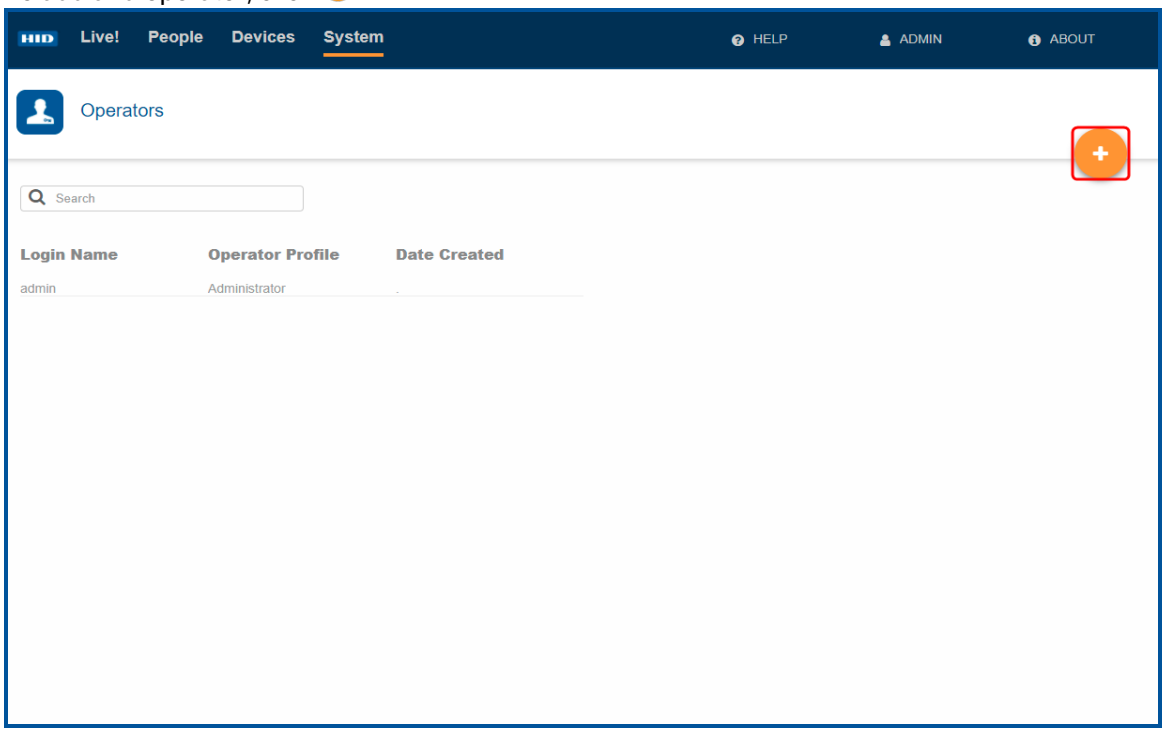
- **Administrator:** This operator role has full access to HID Biometric Manager web application with functions to install and manage Signo Biometric Reader 25B devices, enroll people in the system, add credentials, and collect and store associated biometric data.
- **Device Administrator:** This operator 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 Signo Biometric Reader 25B. This operator role has limited access to user information.
- **Enrollment:** This operator role has full access to HID 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 HID Biometric Manager operator roles:

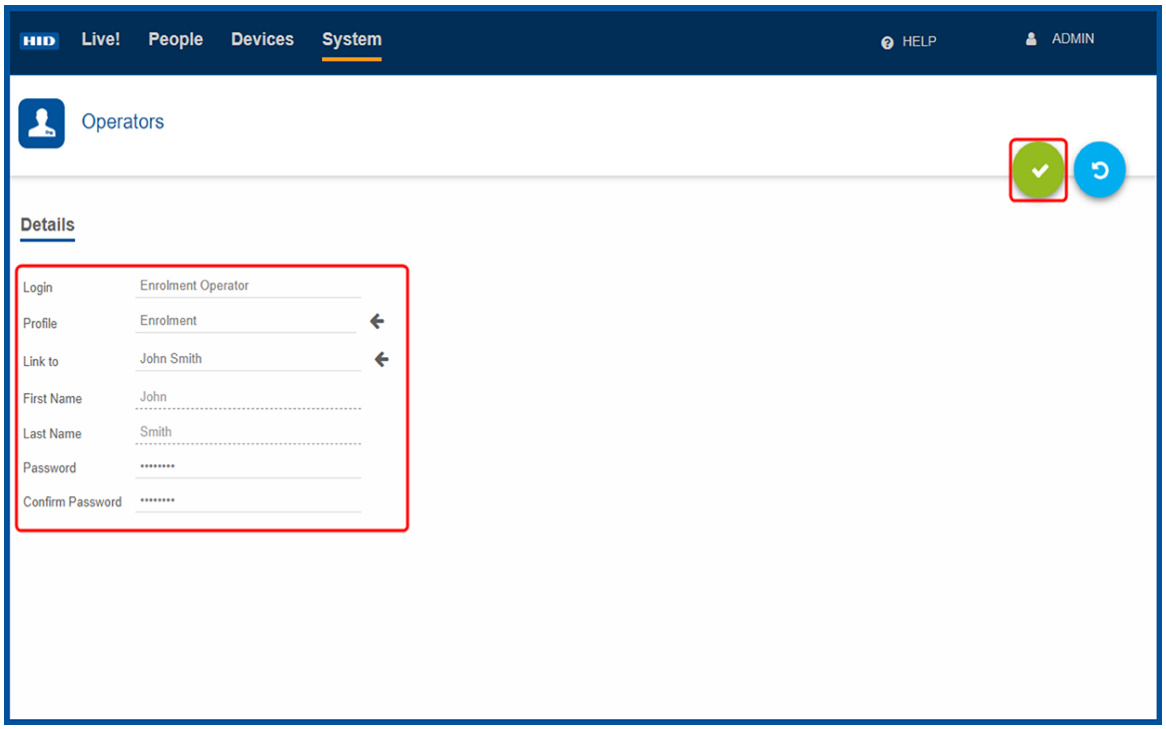
1. Click the **System** option.
2. Select the **Operators** option to access software and firmware update settings.



3. To add and operator, click .



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 .

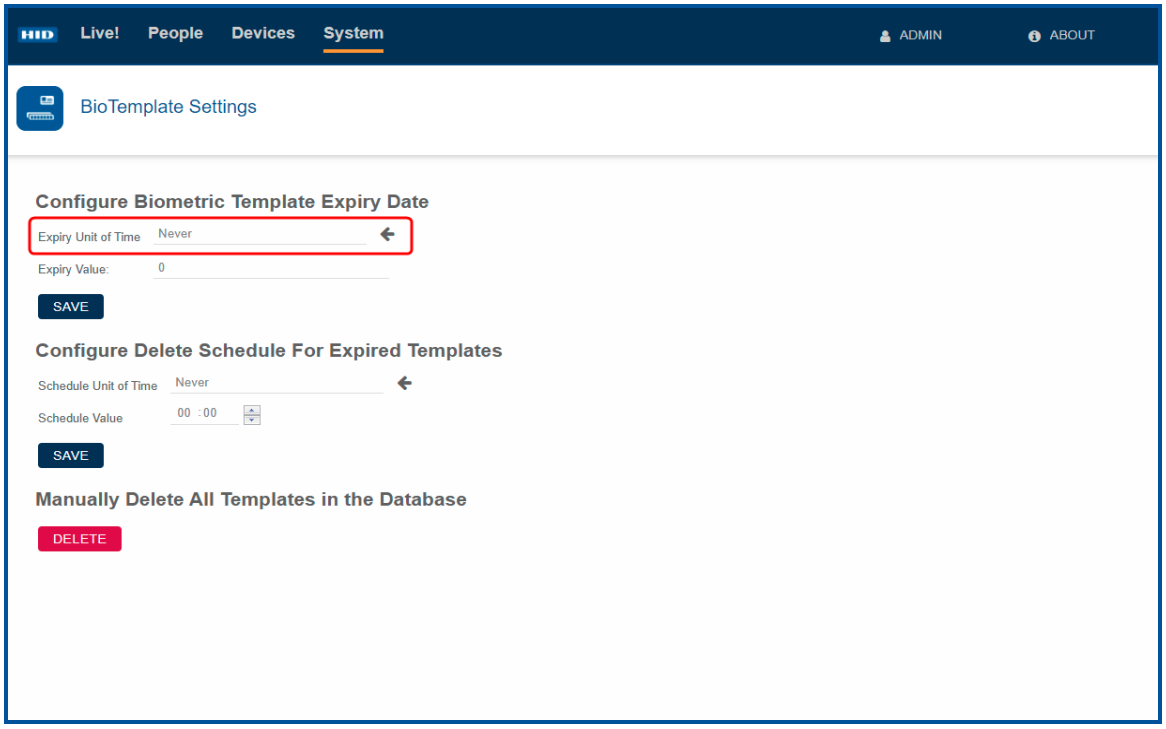


2.14.1 Configuring Template expiry date

Expiry dates can be allocated to individual templates. The system settings are set by default during enrollment but they can be changed during enrollment and later if needed.

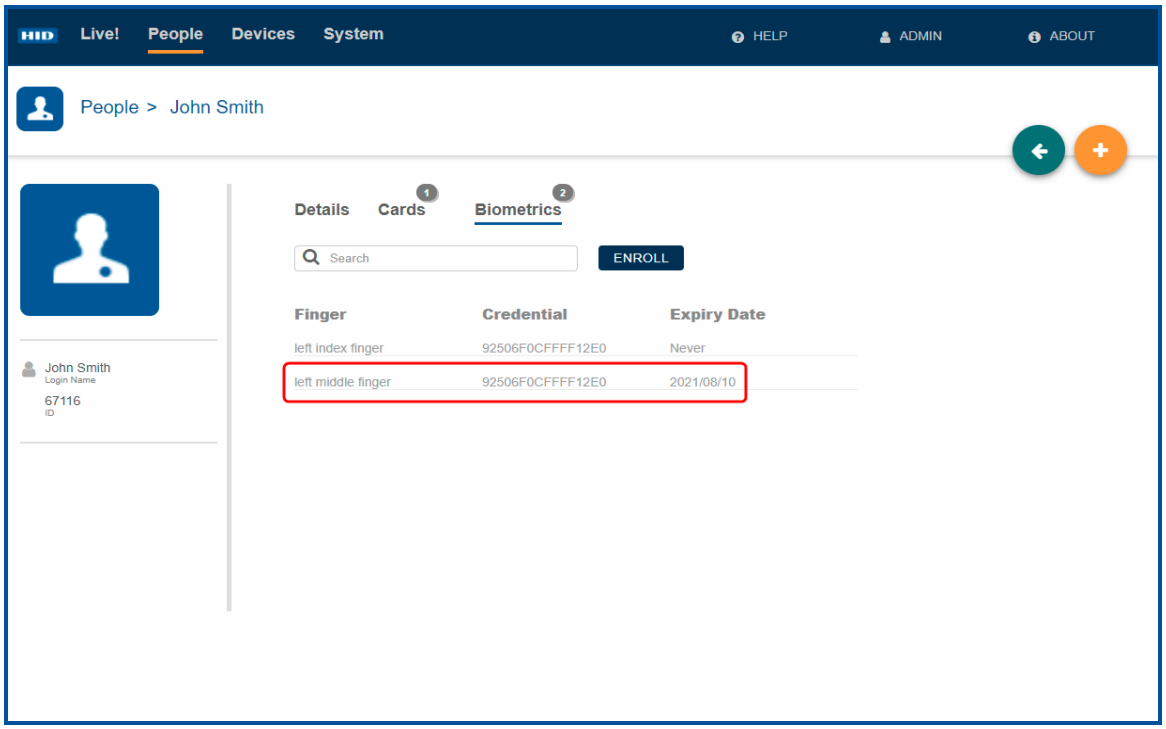
To set the Template expiry date:

1. Navigate to **System** > **BioTemplate Settings**.
2. Under **Configure Biometric Template Expiry Date**, click the arrow to select a **Unit of Expiry**.



3. Select the desired **Unit of Expiry** from the drop down list.
4. Enter an **Expiry Value**.

Note: All new templates will now inherit the **Expiry Date** set in the biometric template schedule. This is visible alongside the template.

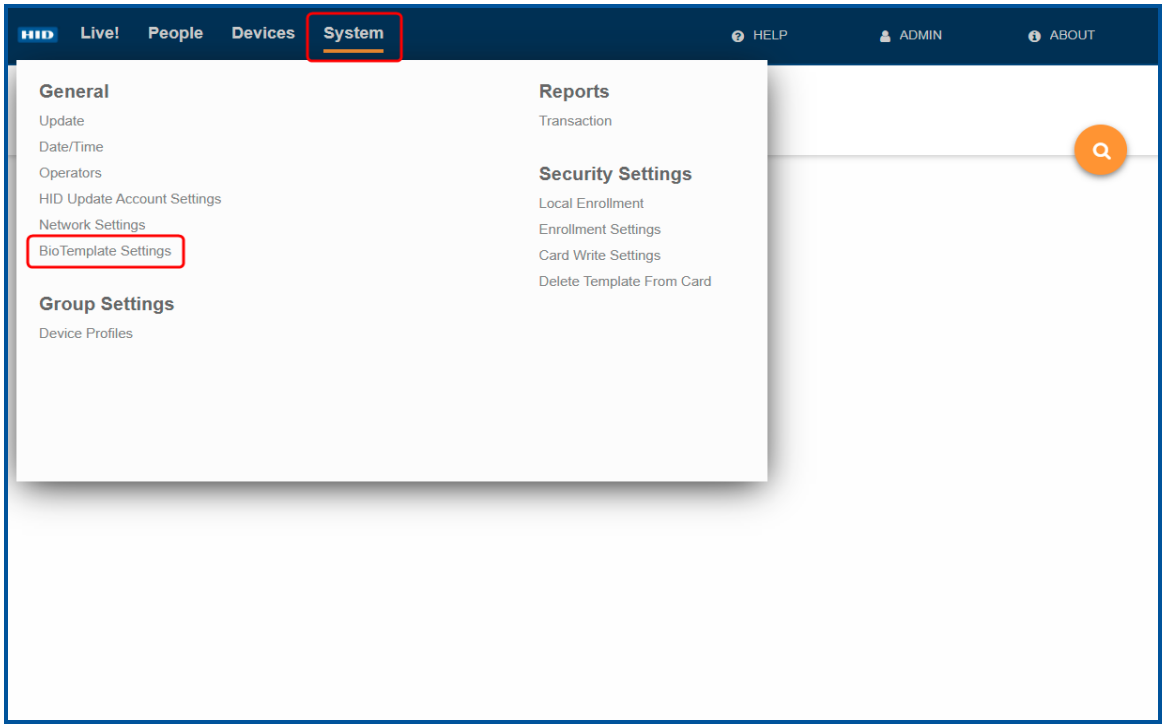


2.14.2 Configuring schedule for deleting expired templates

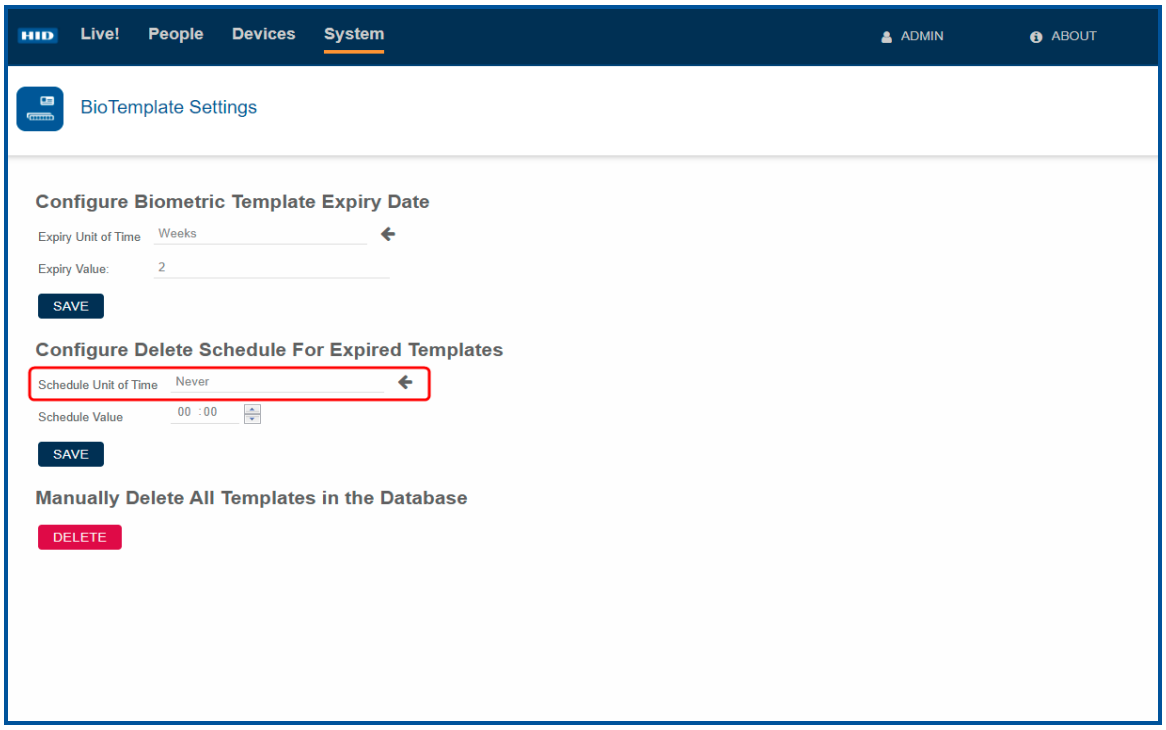
To avoid a backlog of expired templates, a schedule can be configured to automatically delete the expired templates. This is done through the **BioTemplate Settings** window.

Note: The schedule applies to all Biometric Templates enrolled after the schedule is set.

1. Click the **System** option.
2. Click **BioTemplate Settings**.



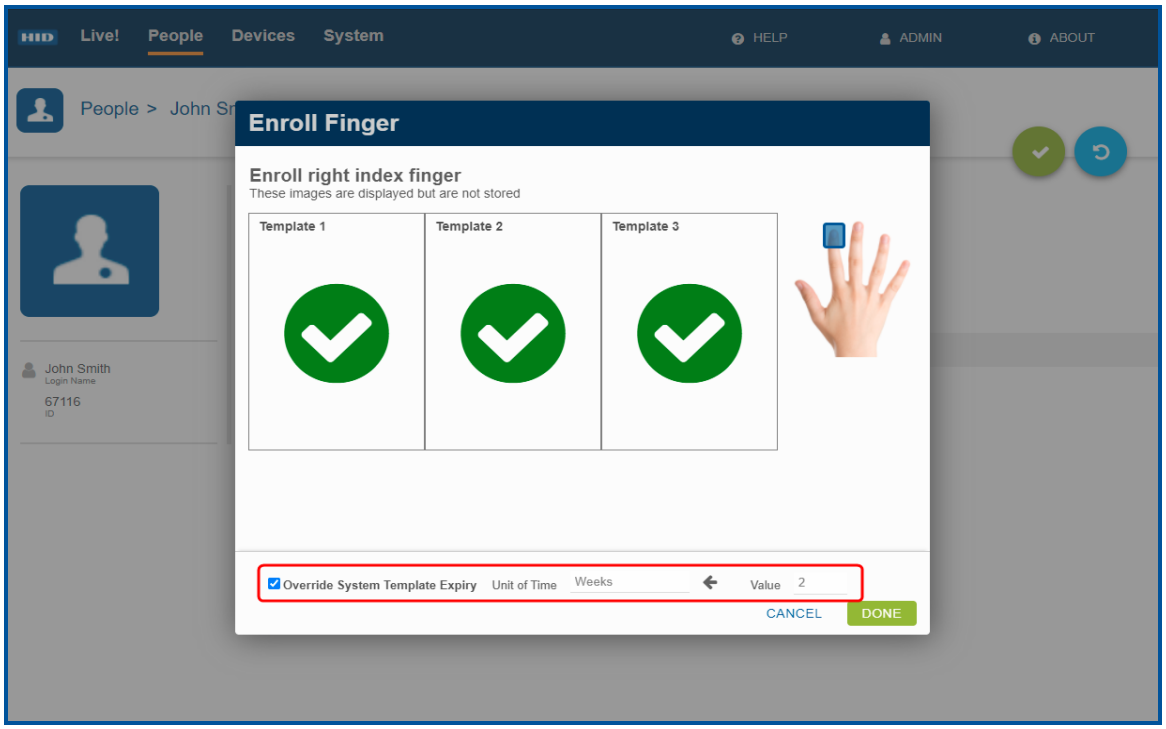
3. Use the drop down arrow to enter the desired **Schedule Unit of Time** and enter a **Schedule Value**.



2.14.3 Override System Template Expiry

When enrolling a biometric template, it will automatically inherit the system template expiration time that is set.

1. During enrollment the system template expiration can be overridden by selecting the tick box to **Override System Template Expiry**.



2. Select the required **Unit of Time** and enter the required value.
3. Click **DONE**.

2.15 Configure device template encryption

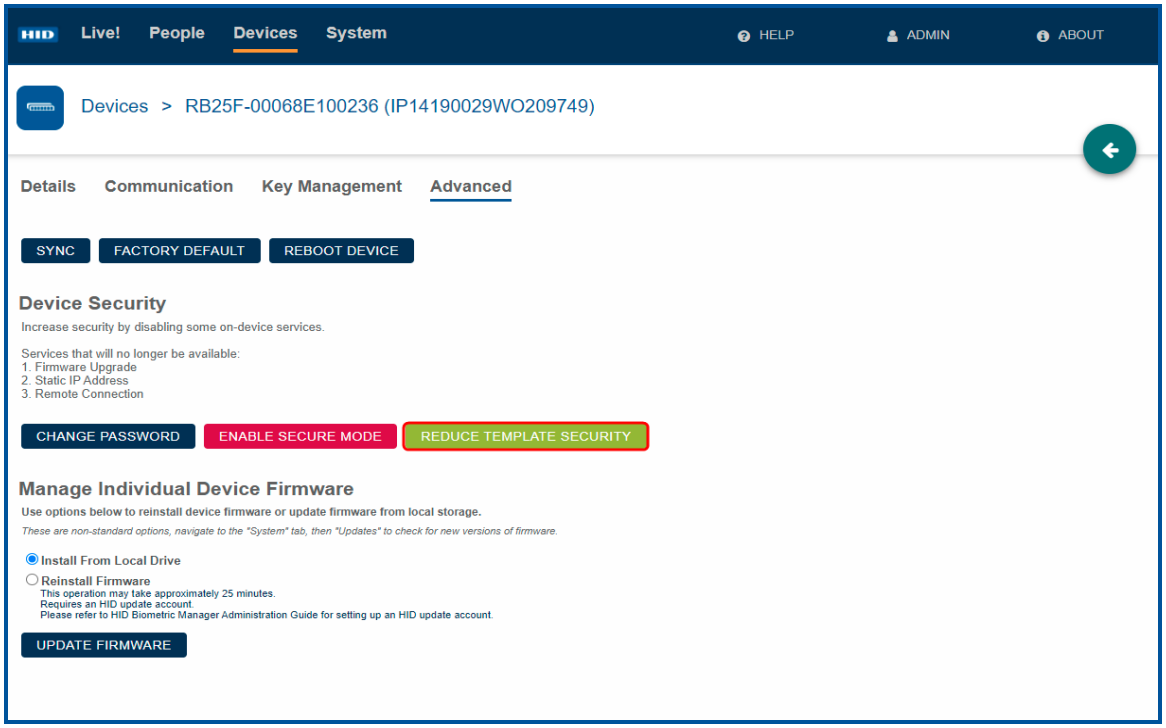
By default, HBM provides security for user enrollment data by encrypting the template stored in the server and the device database. The device and server must be synchronized after any network disruption and power loss or device reset. When there is no power loss or device reset, the Signo Biometric Reader 25B will operate offline with HBM running on the server.

To provide uninterrupted operation when in use with an unreliable network and power supply, HBM gives the option to adjust the template security on the devices.

Note: Only use this option if the Signo Biometric Reader 25B is installed in an area with an unreliable network connection and frequent power outages.

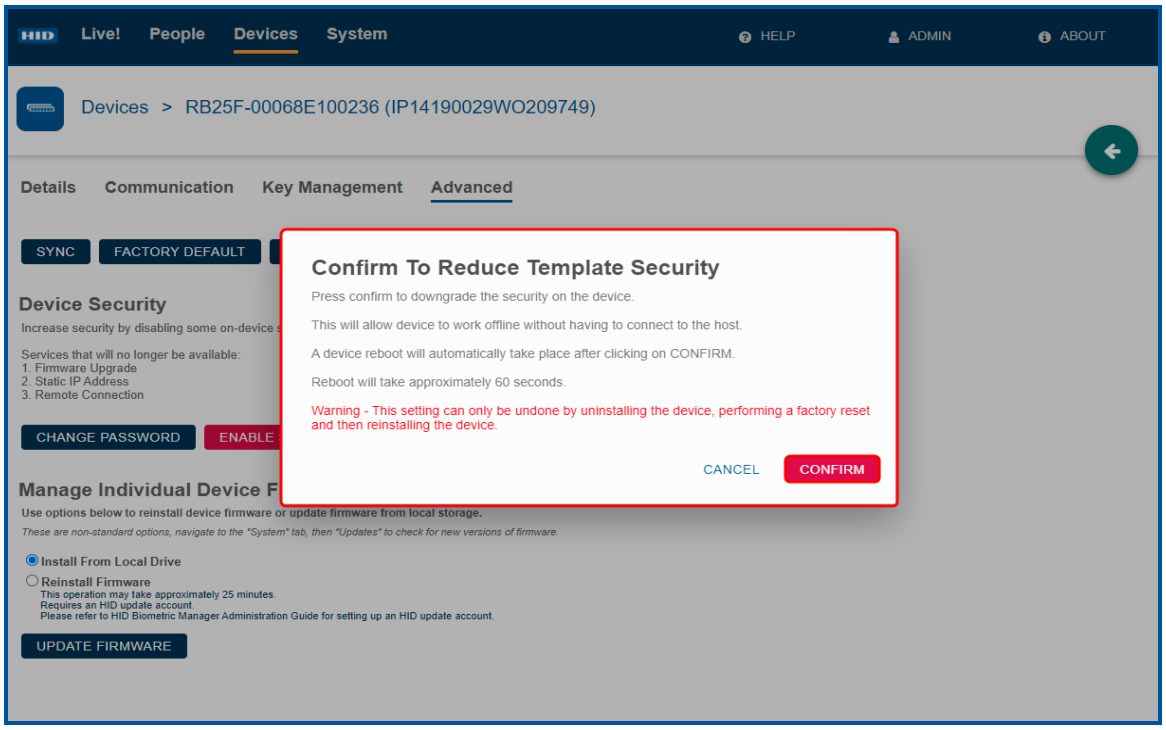
Configuring the device template encryption allows different levels of encryption for individual devices. Disabling the device template encryption allows operation without connecting the device to the server.

1. To configure the template encryption go to the **Devices** page and select the required device. Under the **Advanced** tab there is the option to **REDUCE TEMPLATE SECURITY**.



Important: Read the information given in the pop-up window before confirming the action.

2. Click **CONFIRM** in the pop-up window.



Note: This mode is advised for users with network instability.

Audit trail of template encryption

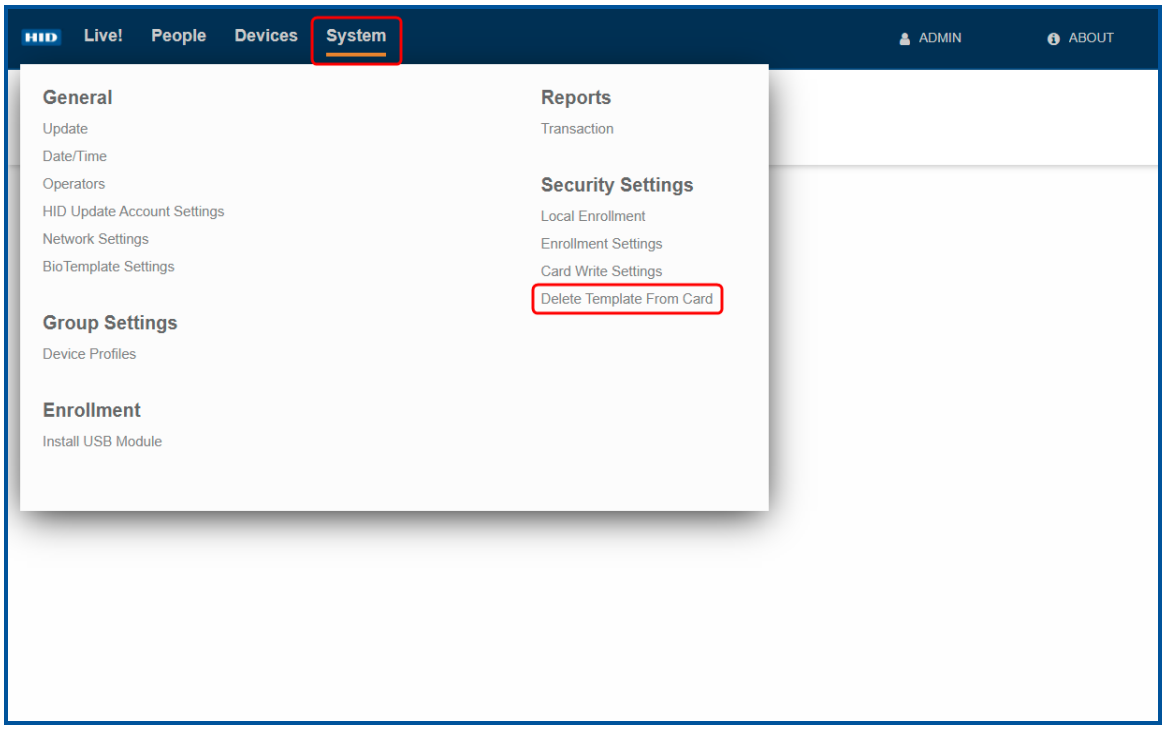
This allows you to keep track of important configuration changes to features like security settings and template encryption. Once the device has rebooted it will appear as an event in the **LIVE!** feed.

Click **System** > **Transaction Report** to make sure disabling the template encryption appears on the transaction report.

2.16 Delete template on card

This allows you to delete all of the templates on a single card by presenting it to a reader.

1. Click **System** > **Delete Template From Card**.

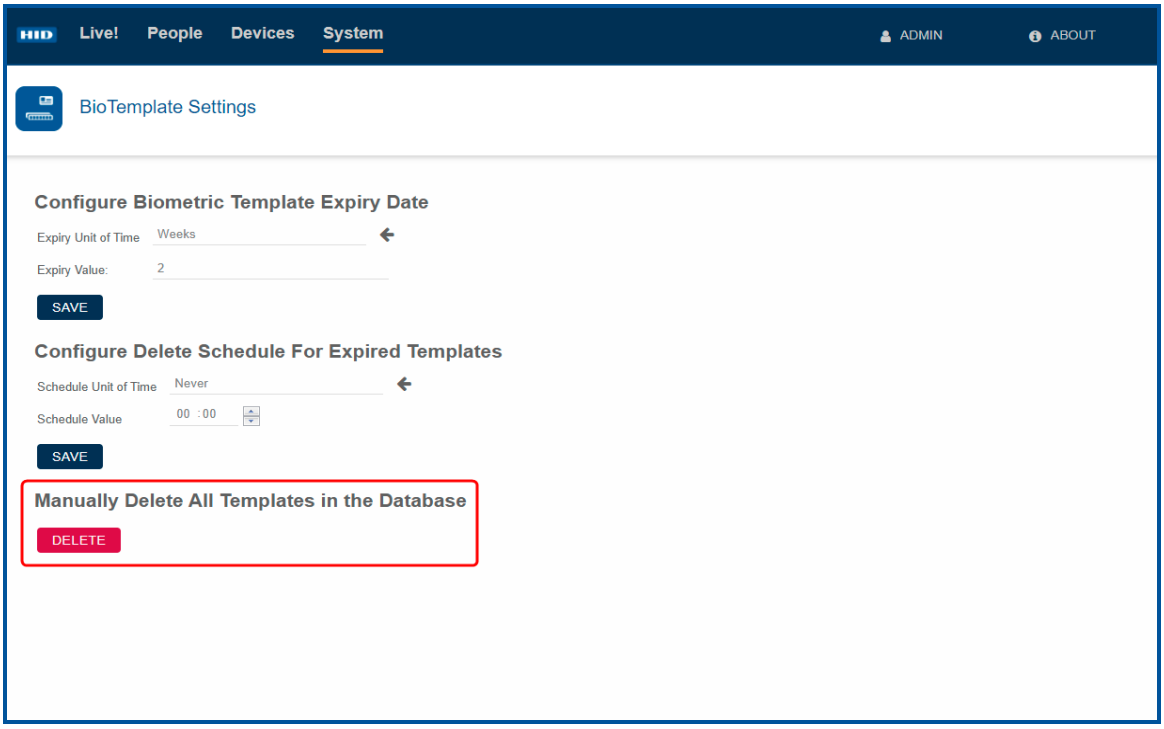


2. Click **DELETE TEMPLATE ON CARD**.
3. Click **CONFIRM**.

   Note: If you have more than one connected reader, select the desired reader from the list and click **NEXT**.
4. When the device beeps, present the card you want to delete all of the templates from.

2.17 Delete all templates

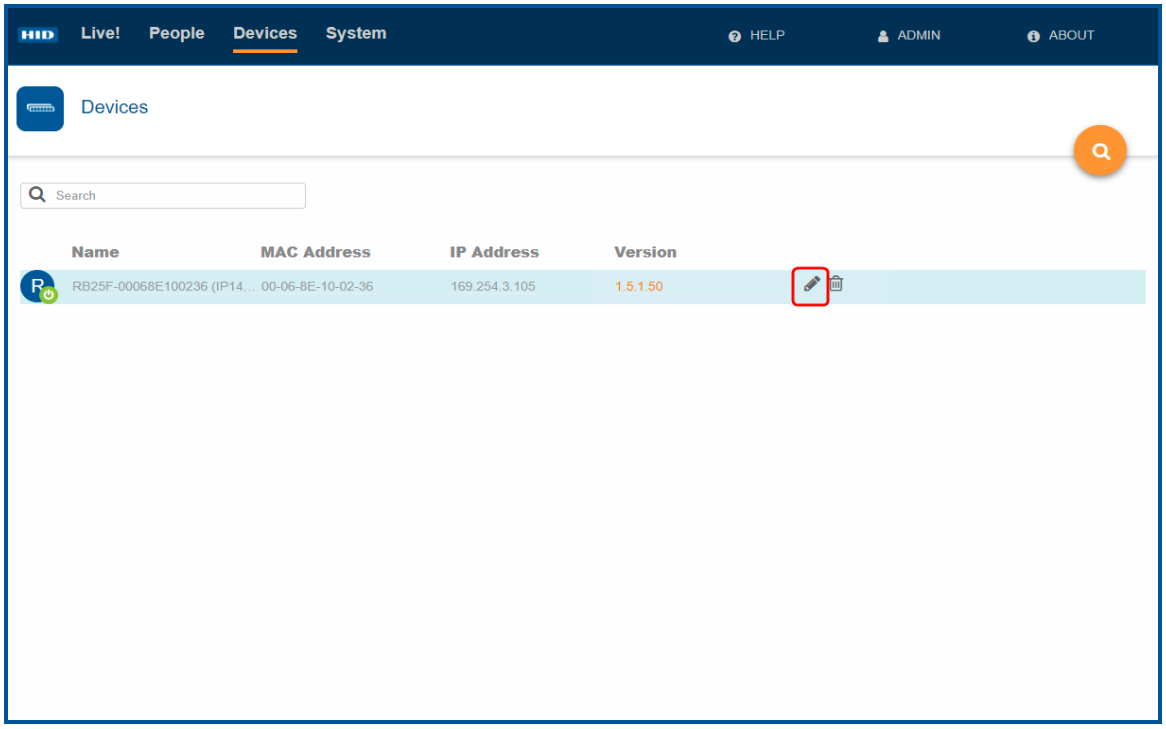
All templates in the HBM database can be manually deleted by going to the **BioTemplate Settings** screen and selecting the **Delete** button under **Manually Delete all Templates in the Database**.



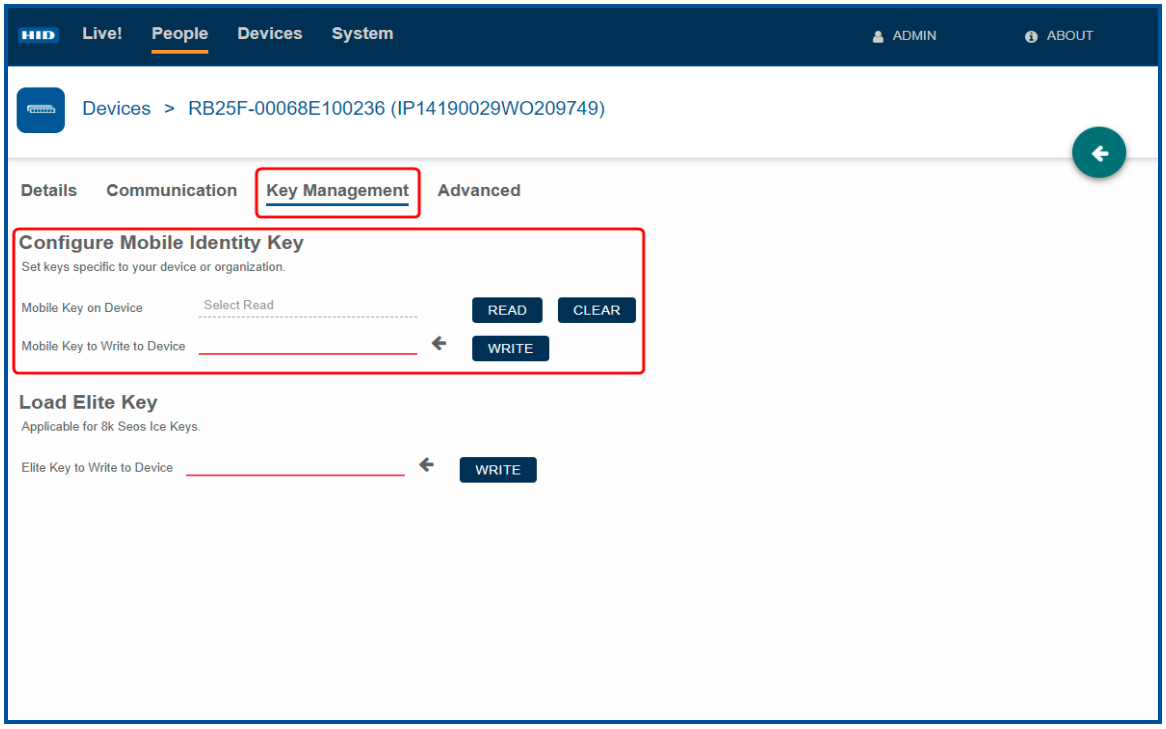
2.18 Load a MOB key onto a device

To load a Mobile Access (MOB) key onto a Signo Biometric Reader 25B device with HID Biometric Manager:

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

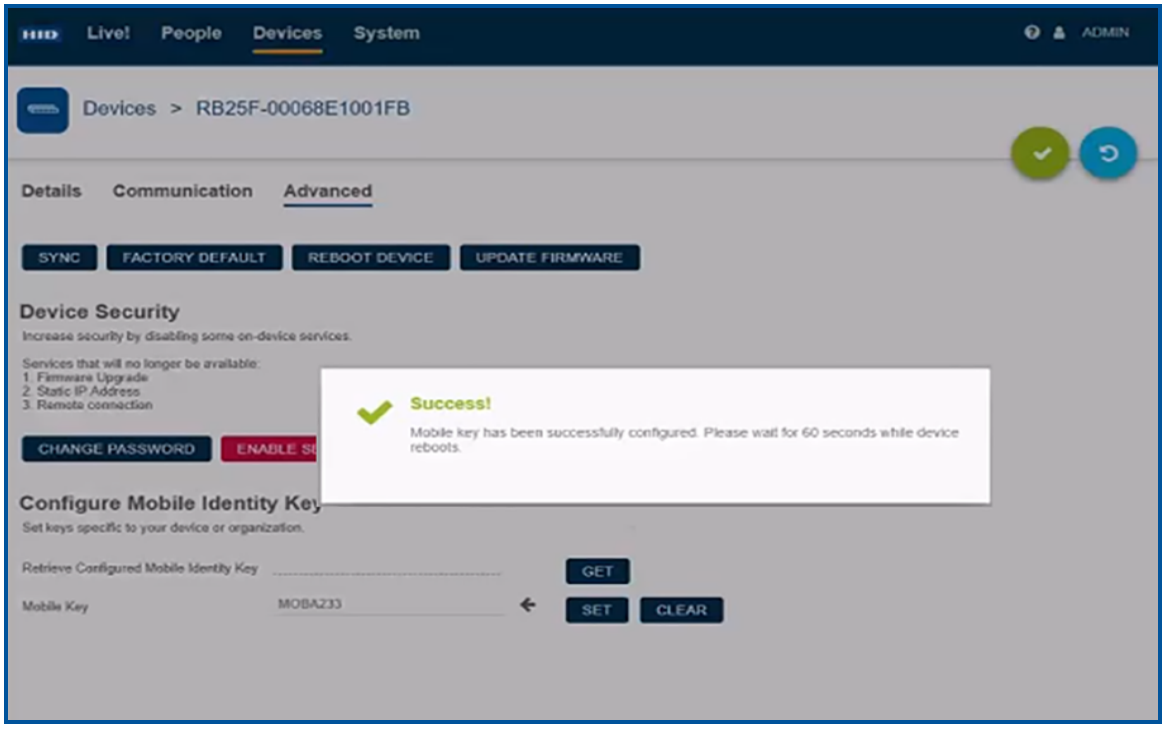


2. On the Devices page, select the **Key Management** tab. Click **READ** to check for any previously loaded MOB keys on the device. Click **CLEAR** to remove any displayed MOB keys that have been read from the device.



3. Click the drop down arrow for **Mobile Key to Write to Device** and select a MOB key from the list.

4. Click **WRITE** to load the selected MOB key onto the device.
   Note: The device can only contain one MOB key at any given time.
5. Click ✓ to finish after the successful pop-up window has disappeared.



2.19 Load HID Elite keys

This feature allows HID Reader Technician to push HID Elite™ keys to the customer via the web. Currently, only Seos® and iClass® cards are supported by the HID Elite keys on this device.

Note: Standard keys will not work on the Signo Biometric Reader 25B 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.

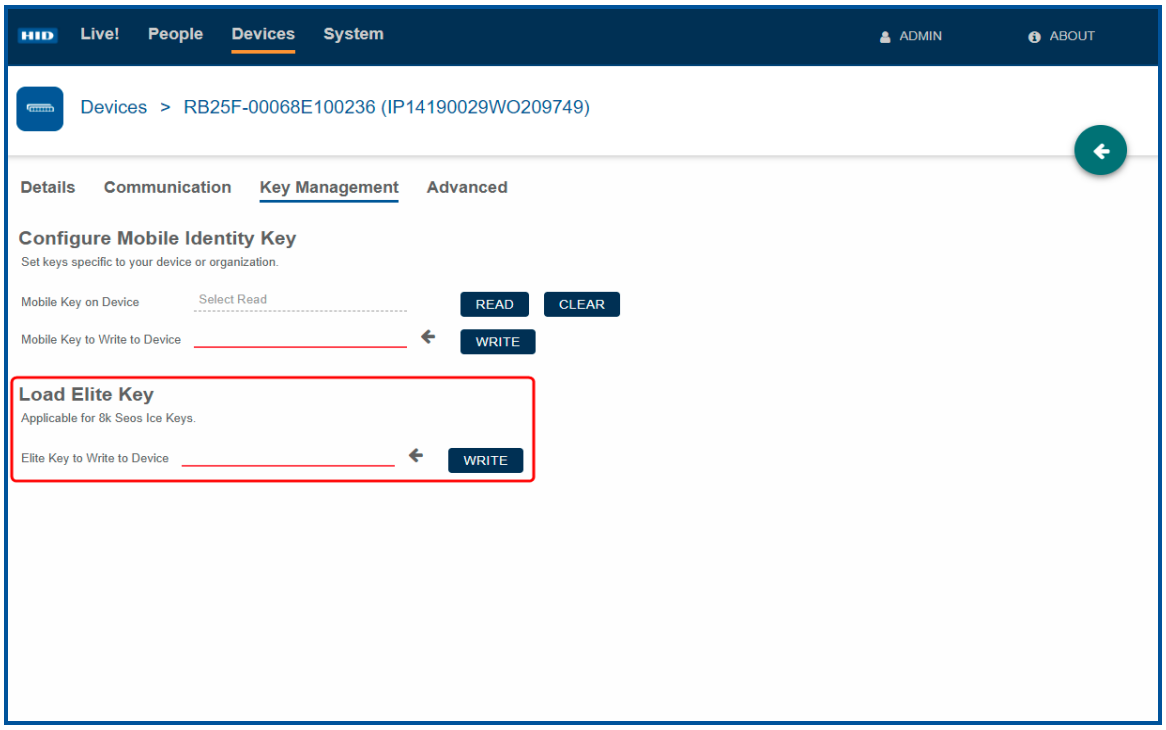
The reader technician account needs to be set up in order to perform this operation. See **A.2 Validate a Reader Manager account in HID Biometric Manager**

Note: You need to be fully enrolled in HID Elite with an ICE Key reference for Signo Biometric Reader 25B to load your ICE Key in the field. This may require contacting HID Credential Programs for confirmation of enrolment.

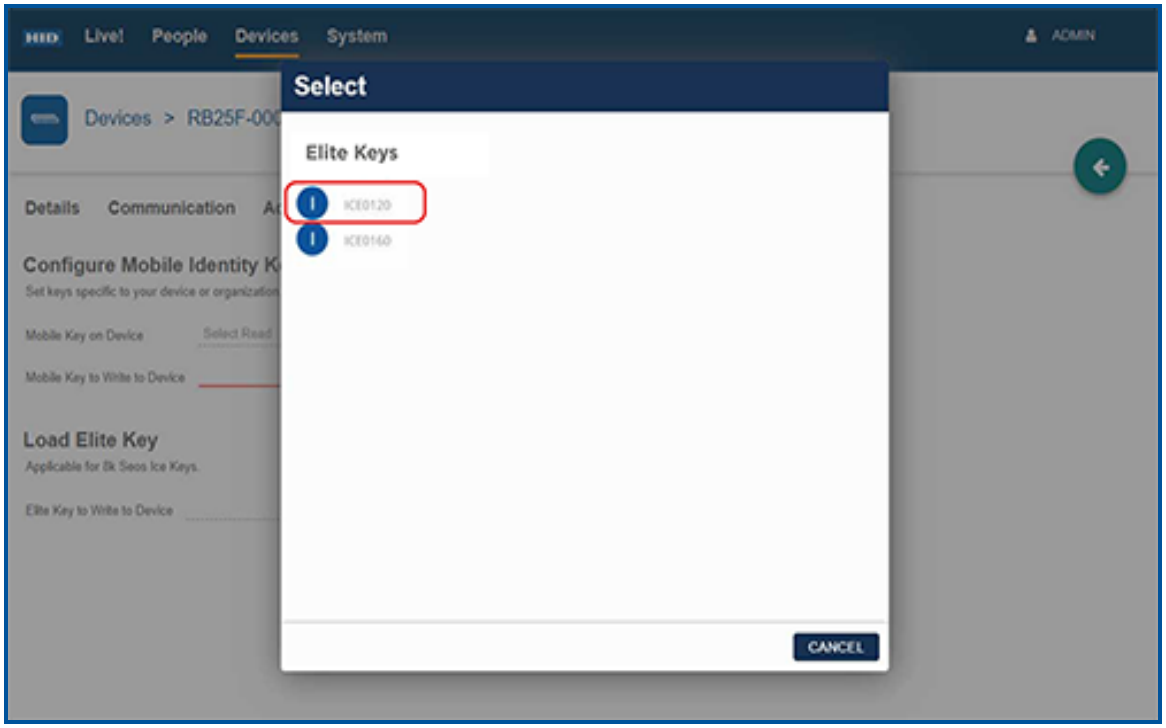
To load Elite keys:

1. Select a device.
2. Open the **Key Management** tab.

3. Click the arrow to select Elite keys.



4. Select a key set to load.



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

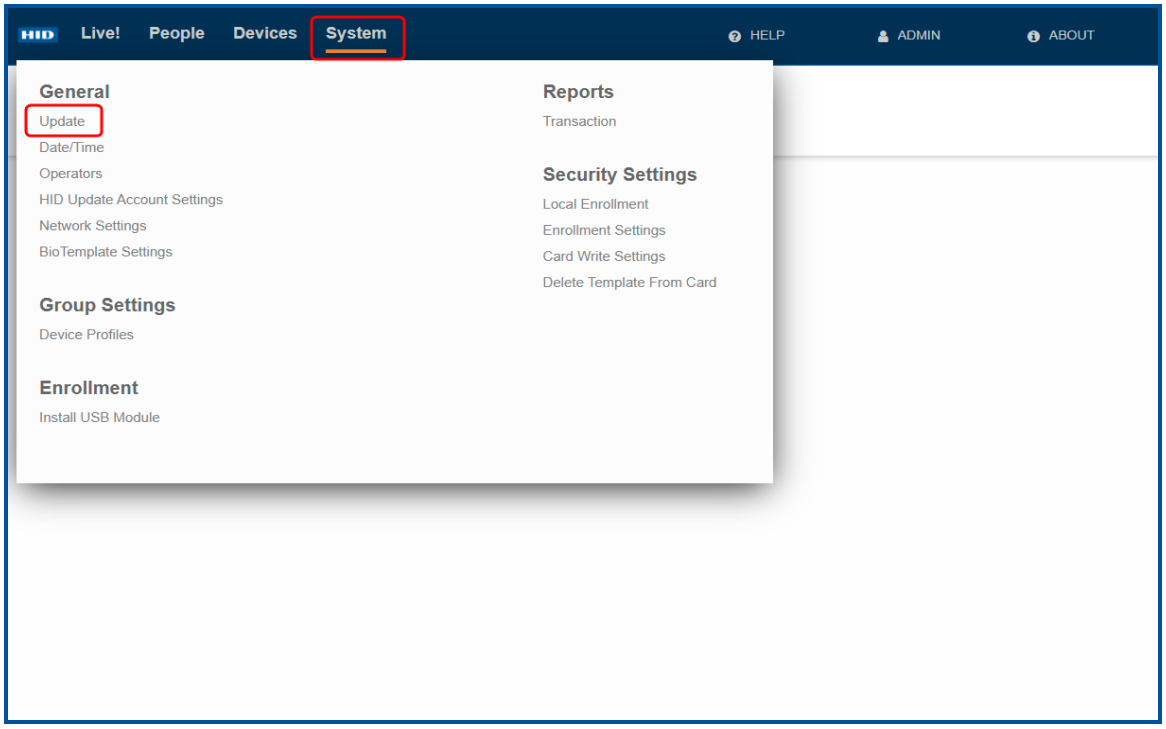
2.20 Configure software/firmware update settings

This allows you to check for software and firmware updates for connected devices.

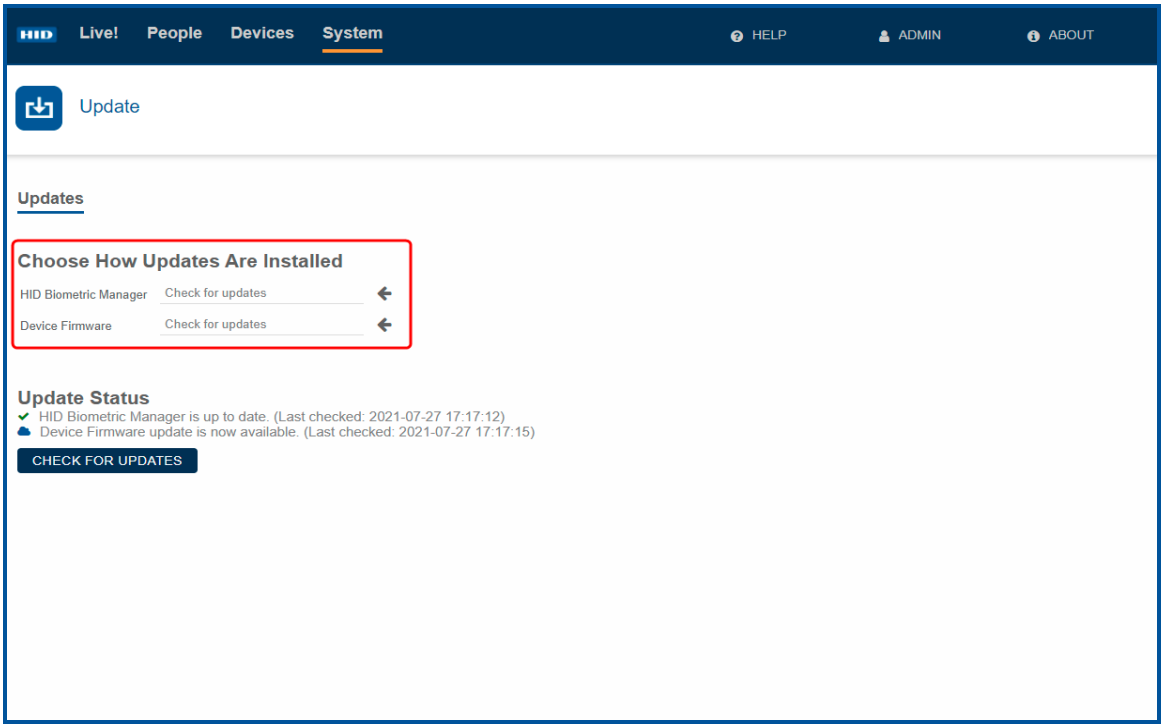
Important: Check for software and firmware updates regularly.

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

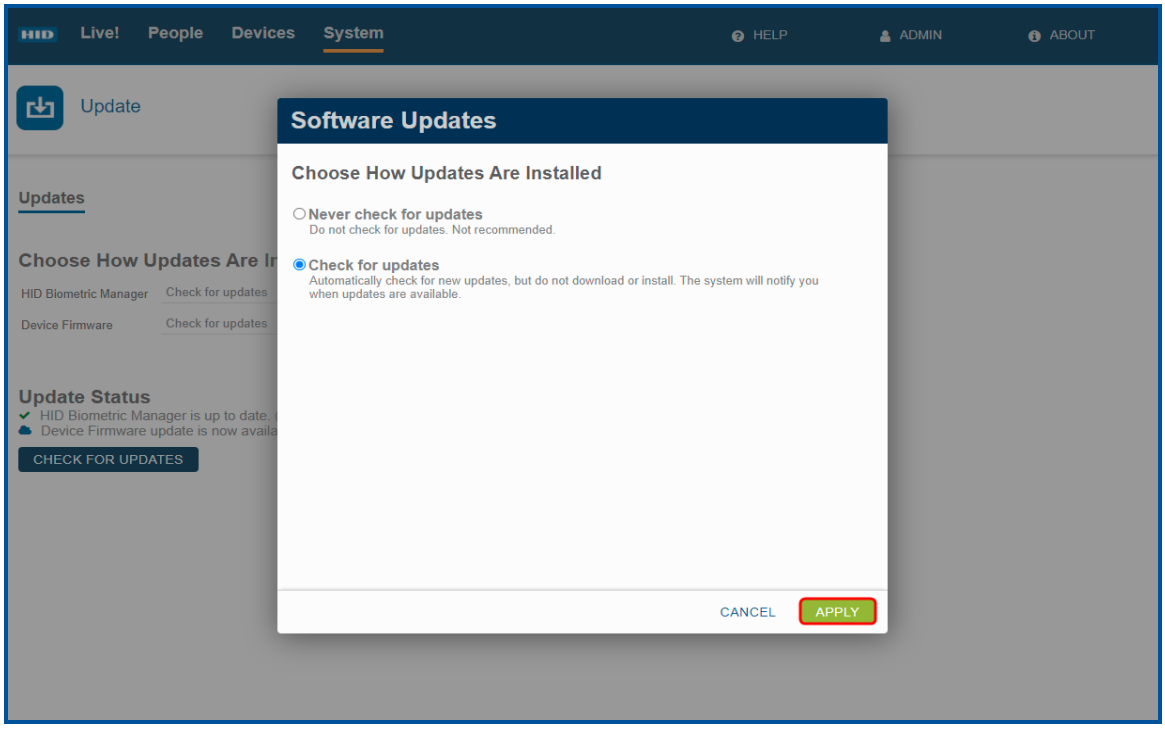
1. Click the **System** option.
2. Click **Update** to access software and firmware update settings.



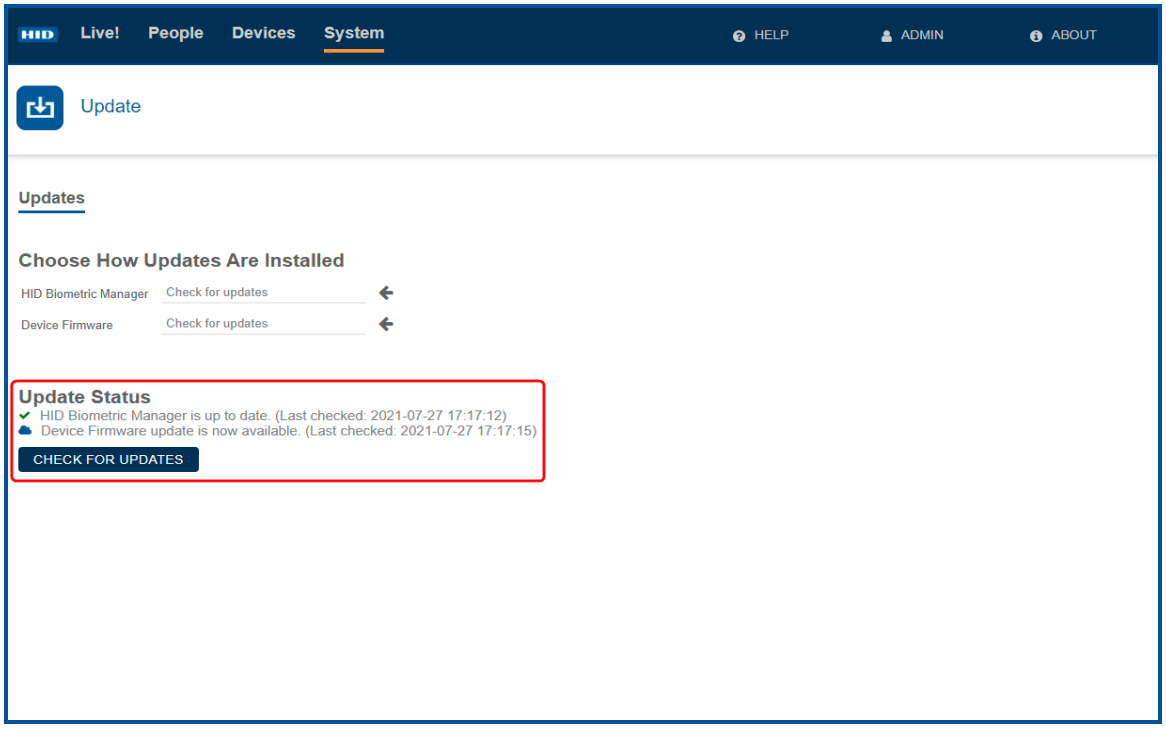
3. Select the arrow icon associated with:
   - **HID Biometric Manager:** To access options to configure how HID Biometric Manager software updates are installed.
   - **Device Firmware:** To access options to configure how device firmware updates are installed.



4. Click **System**.
5. Select the required update option and click **APPLY**.



6. 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 **2.6.4 Device firmware update**.



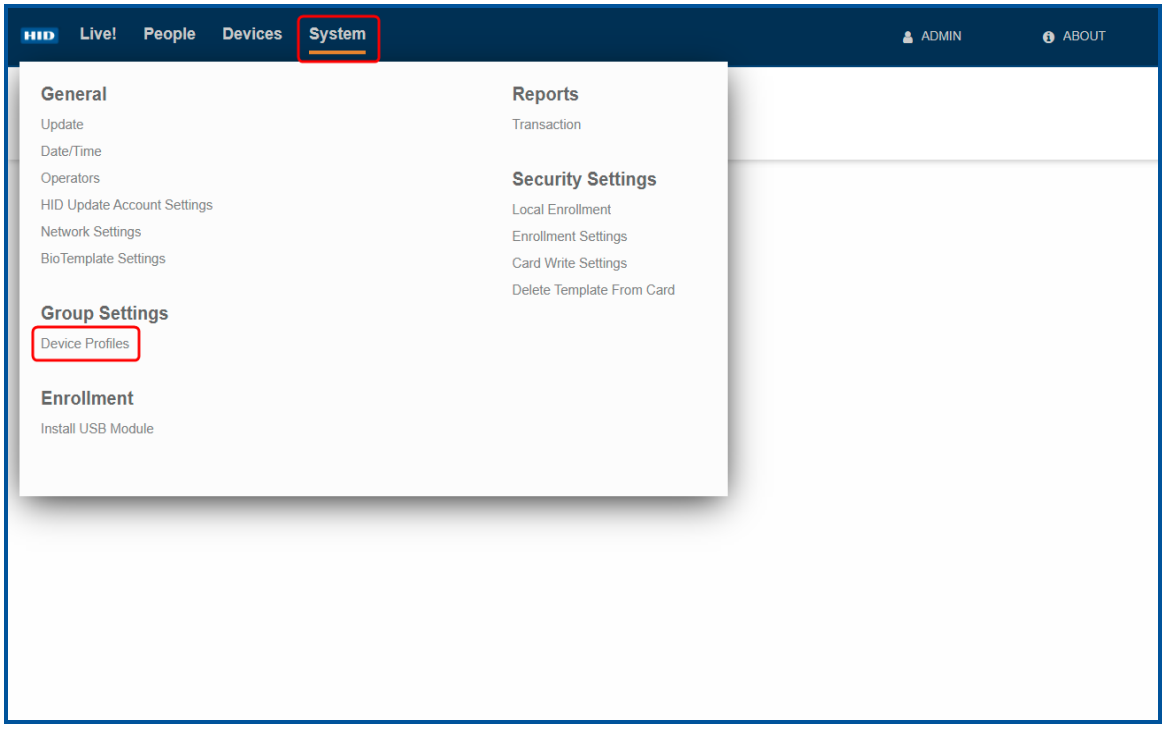
2.21 Device profiles

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.

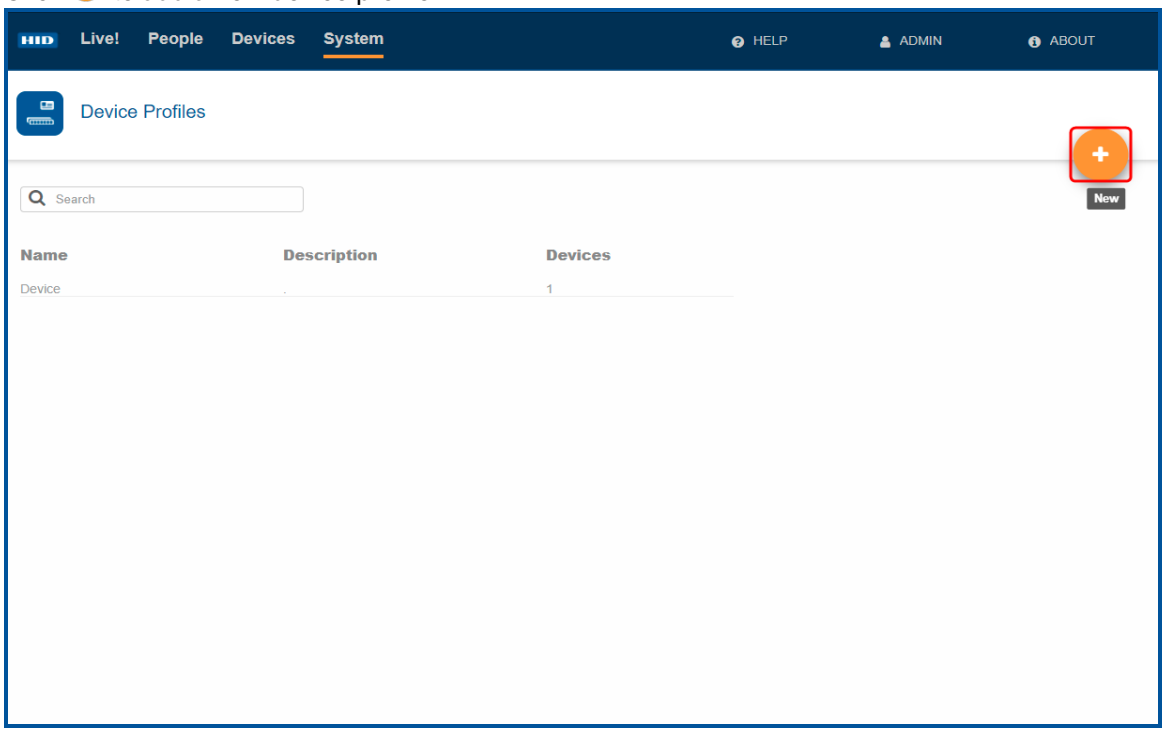
2.21.1 Create a device profile

To create a new device profile:

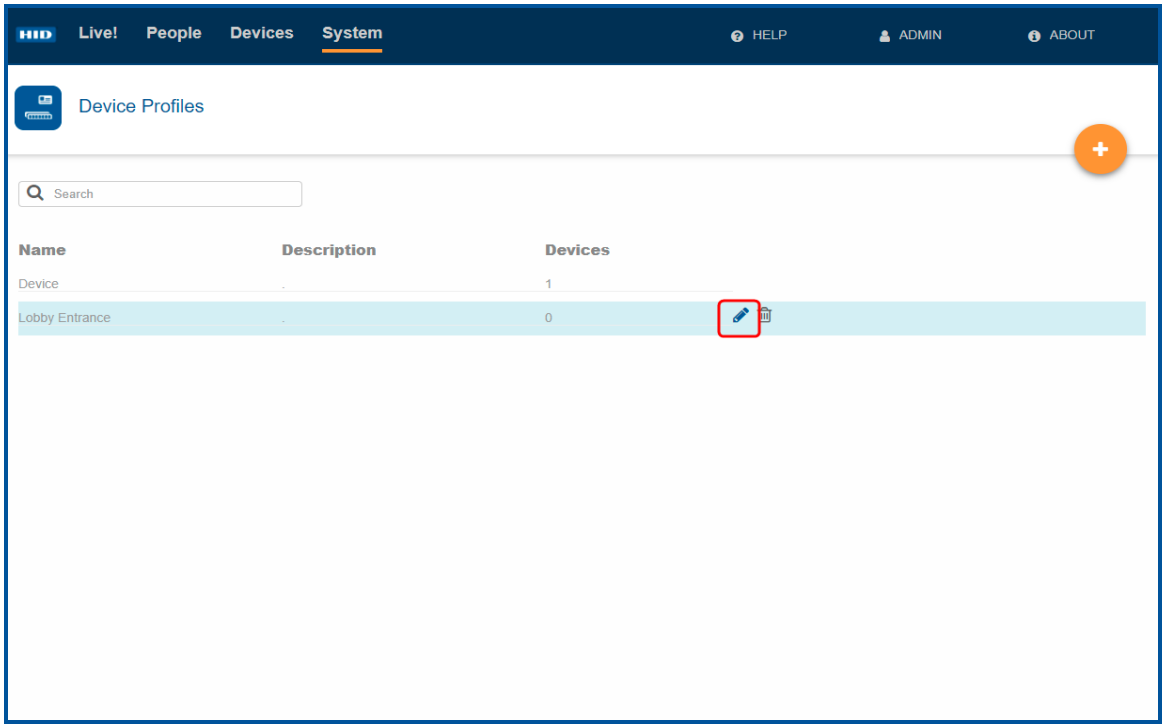
1. Click **System** and select the **Device Profiles** option.



2. Click  to add a new device profile.



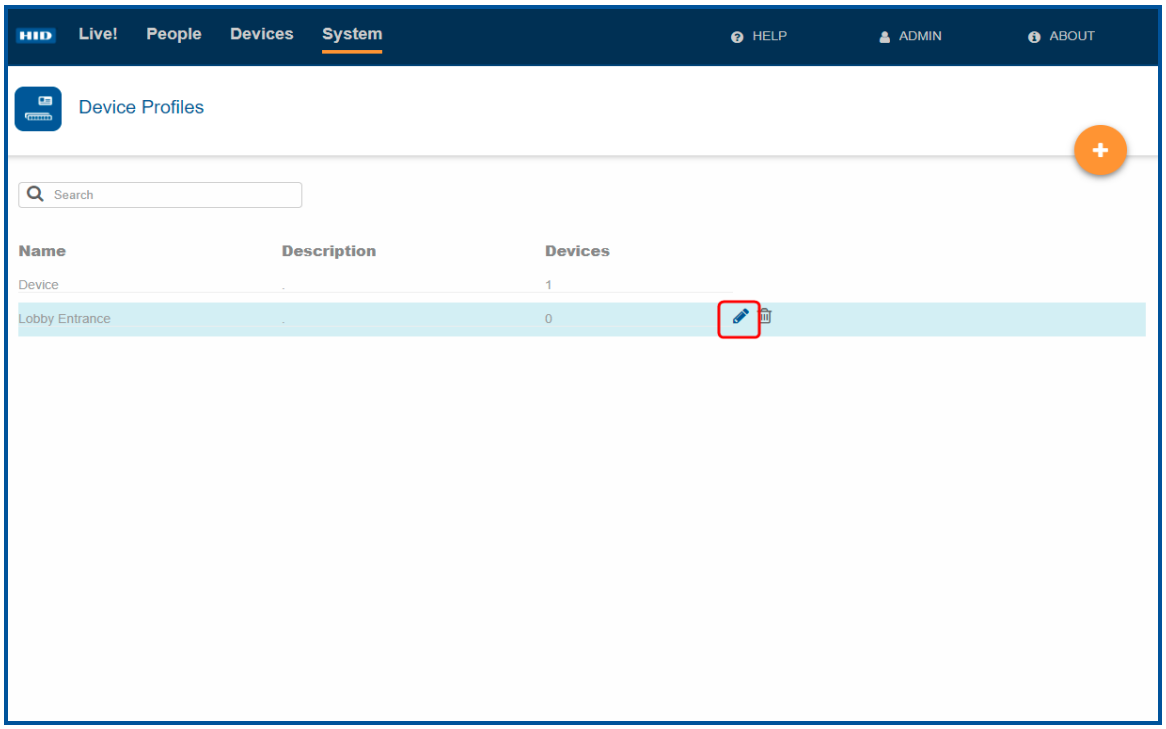
3. Enter a **Name** and optional **Description** for the new device profile.
4. Click  .
5. The created device profile is listed on the **Device Profiles** screen. To edit a profile, highlight a device profile from the displayed list. The **Edit/Delete** icons appear on the screen for the highlighted device profile.
6. Click the **Edit** icon  associated with the device profile to access the profile attributes. See **2.21.2 Edit a device profile**.



2.21.2 Edit a device profile

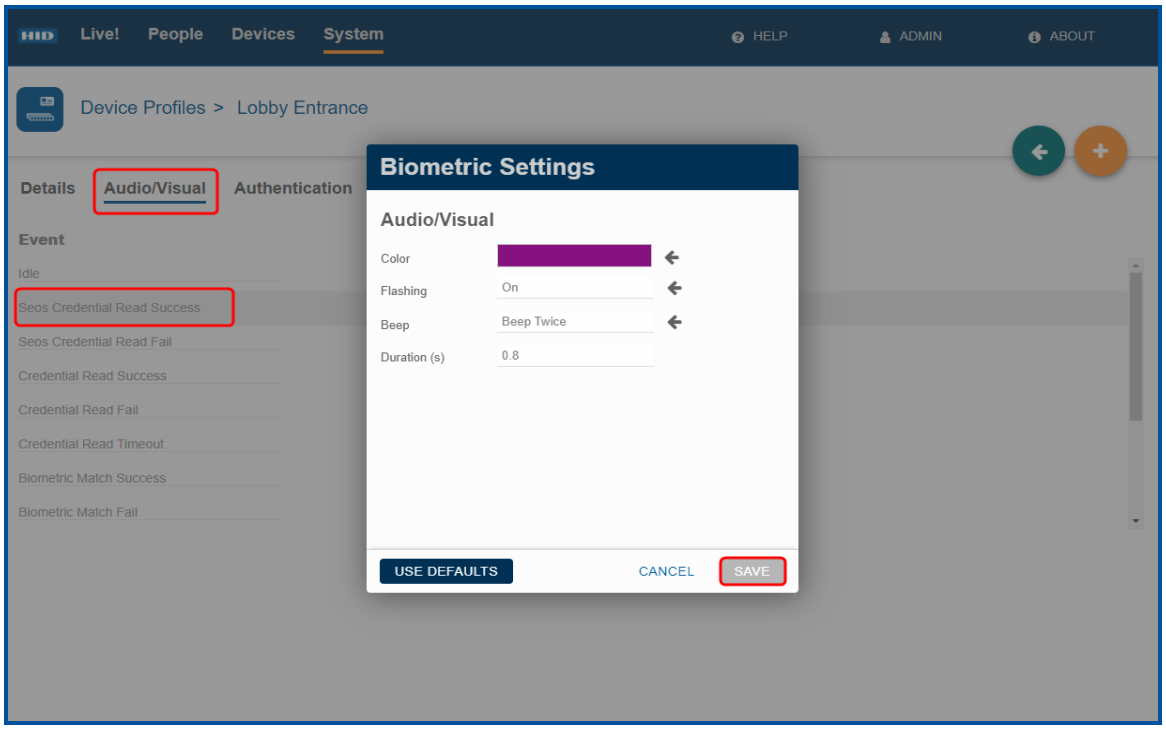
To edit the attributes of device profile:

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



3. Click **Audio/Visual**.
4. Select an **Event**.
5. Click the ← on an **Event** type from the displayed list to choose the attributes for the selected event.
6. Click **SAVE**.

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

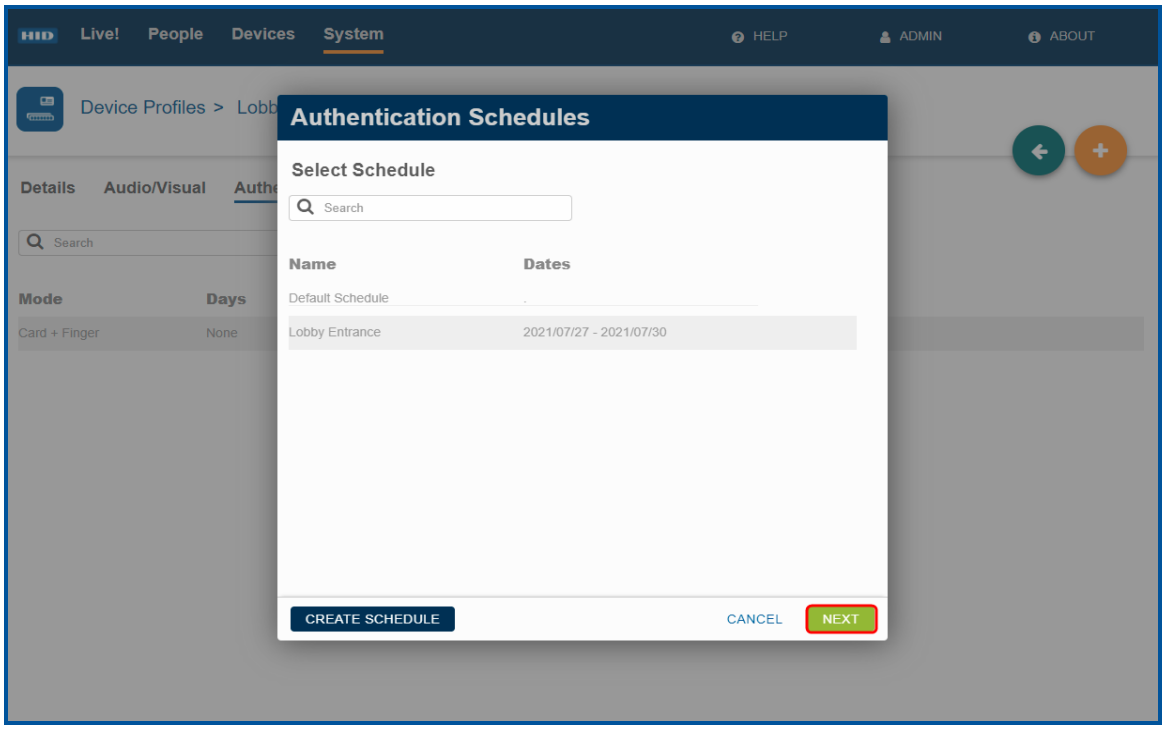


Note: Steps 7-8 are optional.

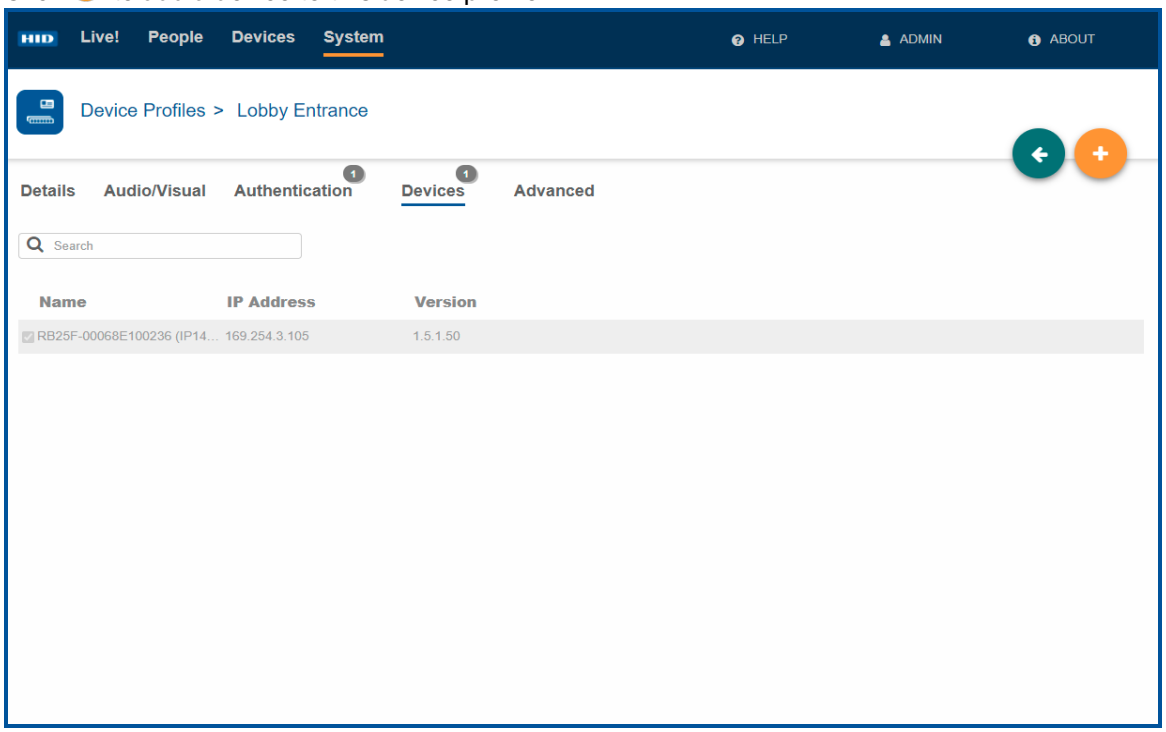
7. On the **Device** screen, select **Authentication**.
8. Click **ADD SCHEDULE** to schedule when a device will operate in a special Authentication Mode. Select a schedule from the list and click **Next**.

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

   Note: Creating a schedule allows the device to operate in different authentication modes for different parameters for example, day of the week or time of the day. If no schedule is created the default schedule of 24/7 will be applied.

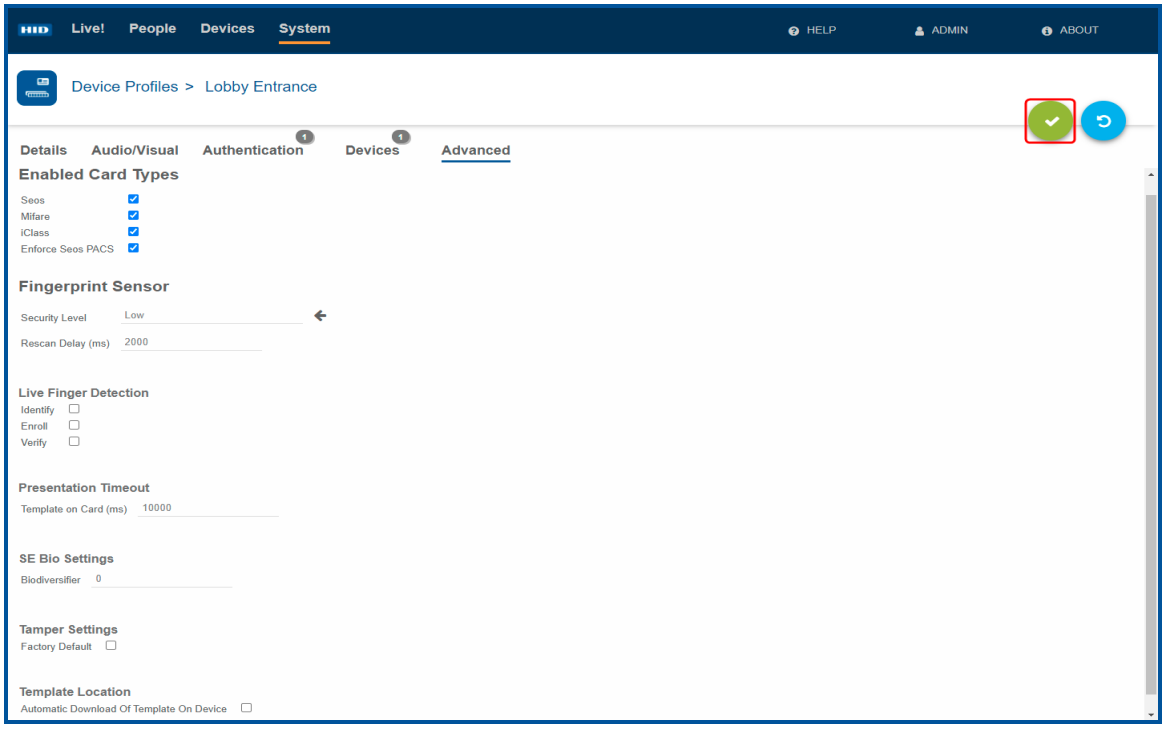


9. On the **Device** screen, select **Devices** to view the list of devices that belong to this device profile. Any changes made to this device profile will be applied to these listed devices.
10. Click + to add a device to this device profile.



11. On the **Device** screen, select **Advanced**.
12. Select the card types which the device should support and the fingerprint sensor settings.

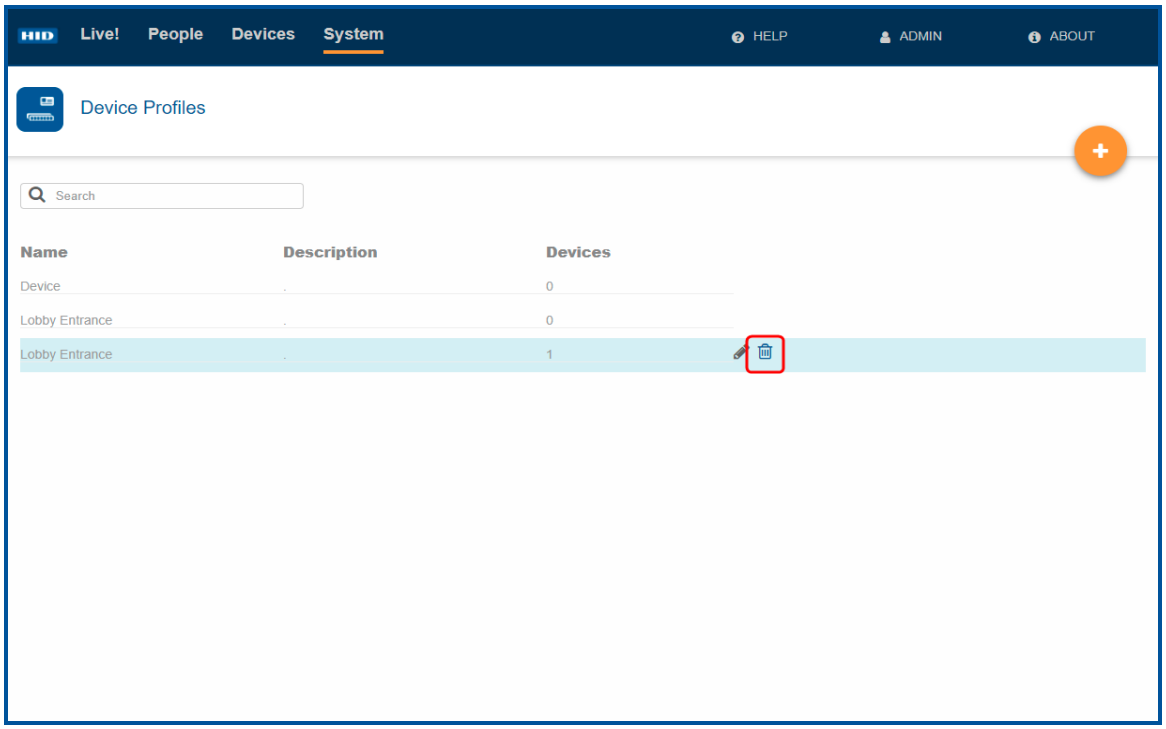
13. Click .


Live!
People
Devices
System
HELP
ADMIN
ABOUT
Device Profiles > Lobby Entrance
Details
Audio/Visual
Authentication
Devices
Advanced
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
Template Location
Automatic Download Of Template On Device

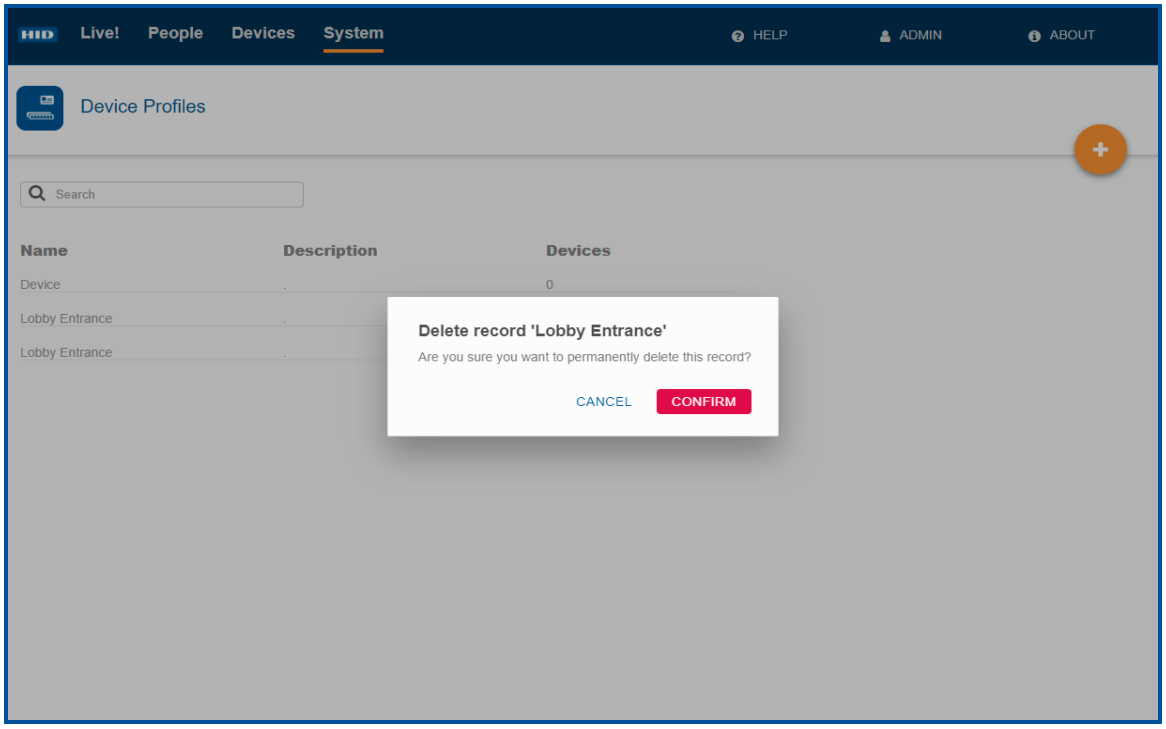
2.21.3 Delete a device profile

To delete a device profile:

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



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

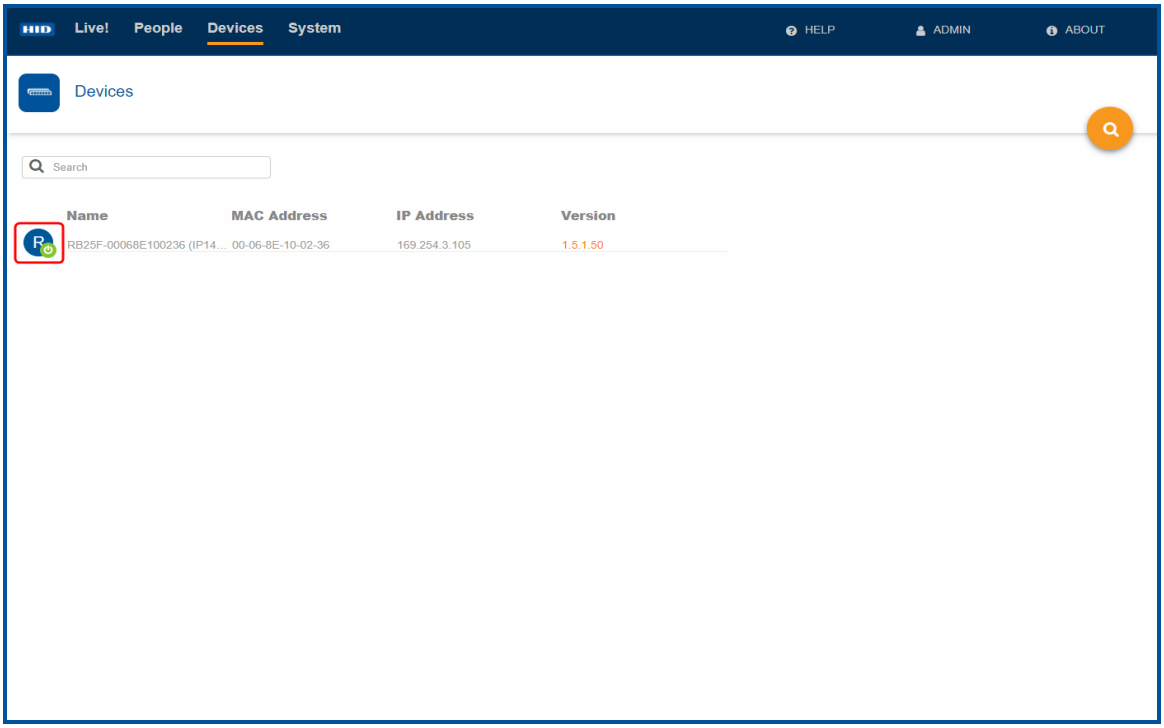


2.22 Device health indication

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
	High level communications in place and device ready.	The device is ready to be used and there are no issues.
	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.
	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.
	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.



2.23 Device debug page

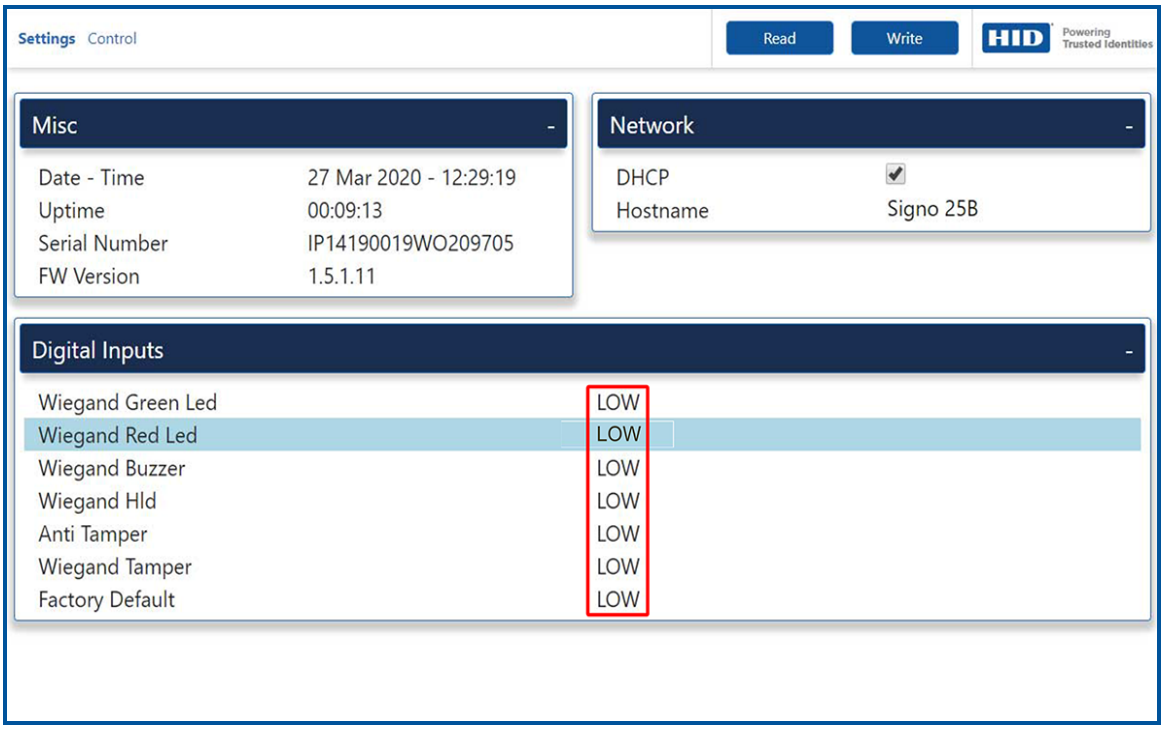
The device debug page provides a live view of the status of each input for the device and serves as a diagnostic tool during installation and operation.

Note: The device debug is only accessible for 30 minutes after a device factory reset

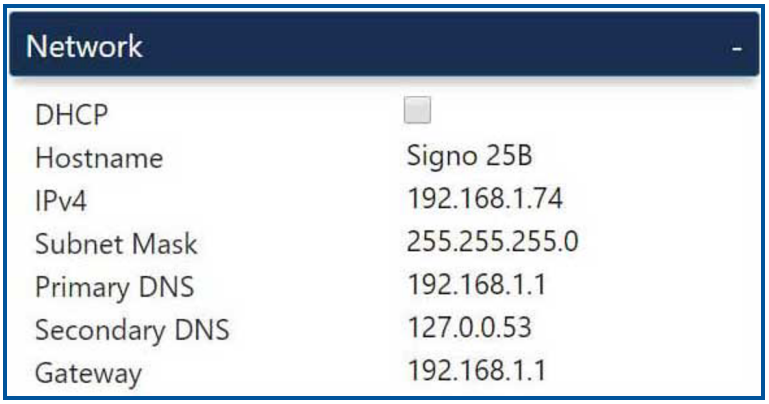
To access the device debug page, search **http://<Device IP>:8888** in a Web browser.

The **Misc** 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**.

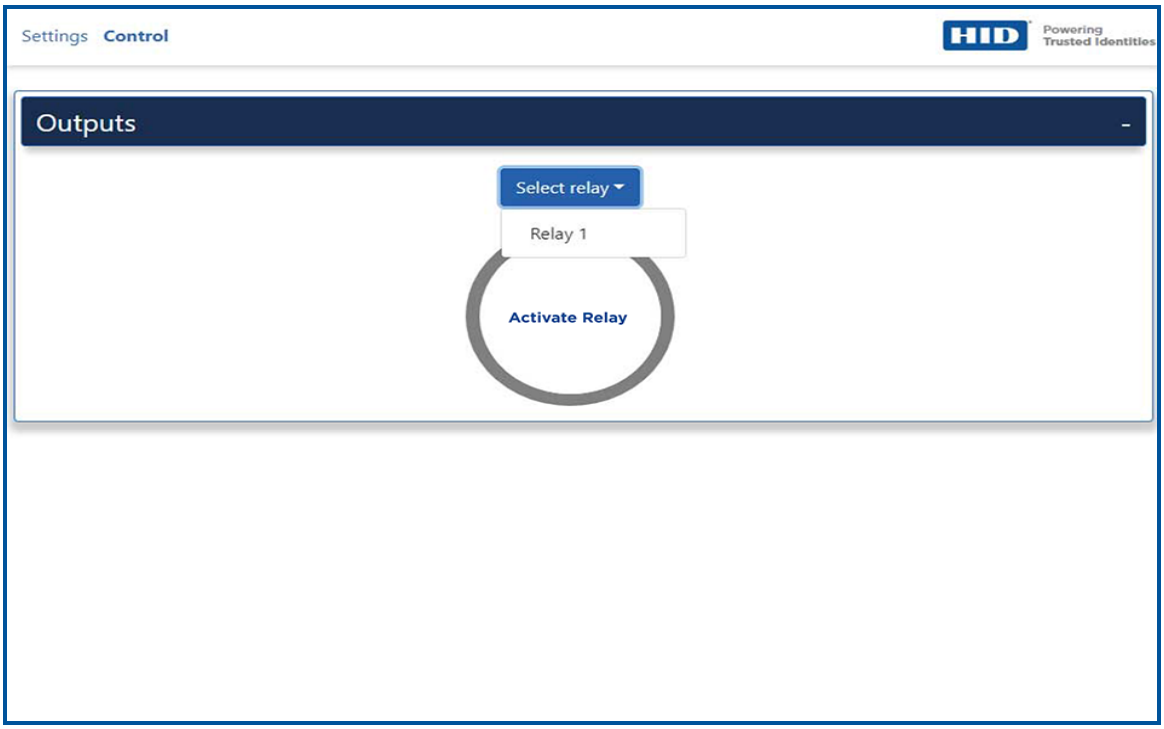


When the **DHCP** option under the **Network** window is deselected, the **Network** window will expand. The details can be manually entered as required.



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: This feature is not available for the iCLASS SE RB25F. It is exclusive to the Signo Biometric Reader 25B only.



Note: The internal relay will toggle for five seconds.

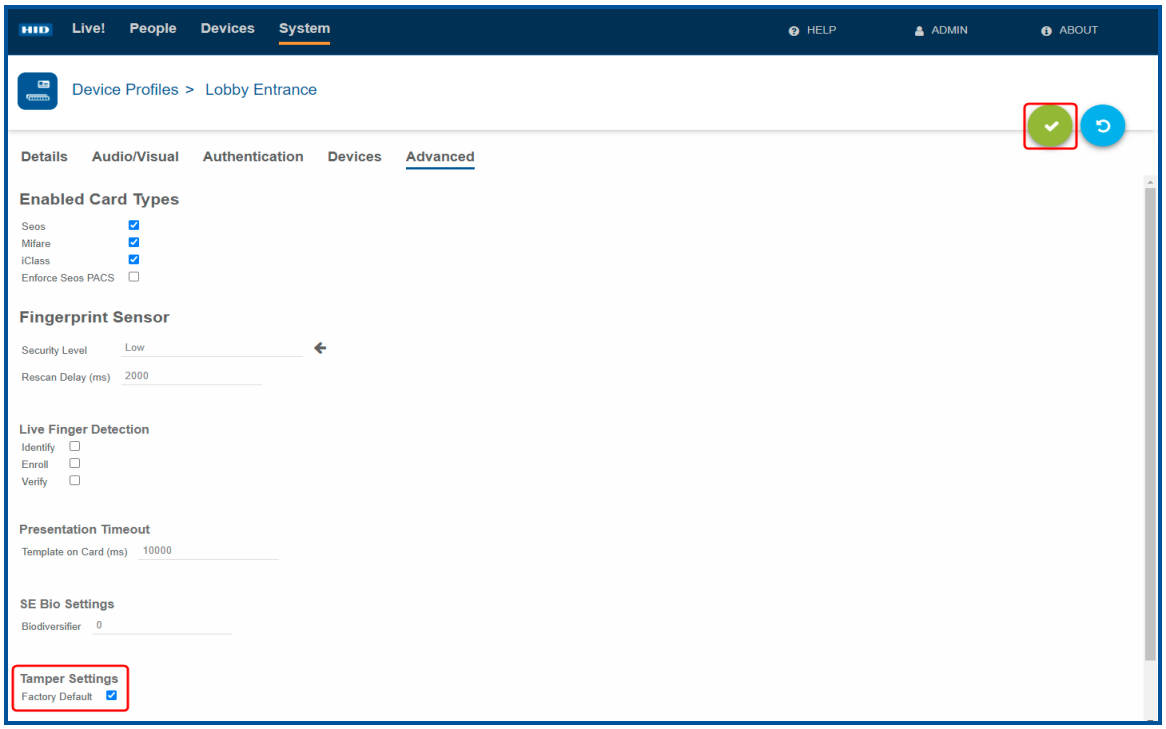
2.24 Tamper settings

The Signo Biometric Reader 25B has an anti tamper feature that can be enabled or disabled in HBM. When any of the connected devices are removed from the casing, the **Factory Default** feature will trigger, resetting and rebooting the connected device to factory settings. This removes any stored biometric templates from the connected device, and any device configuration settings. The devices will not communicate with the HID Biometric Manager until it has been reinstalled.

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

Important: **If maintenance to the power system has been scheduled, disable the Factory Default Tamper Settings before maintenance begins, to avoid having to re-install the devices in the event of an accidental tamper during maintenance.**

1. To toggle the **Factory Default** setting on or off, navigate to the **Device Profile** page and select the **Advanced** tab.
2. Click .

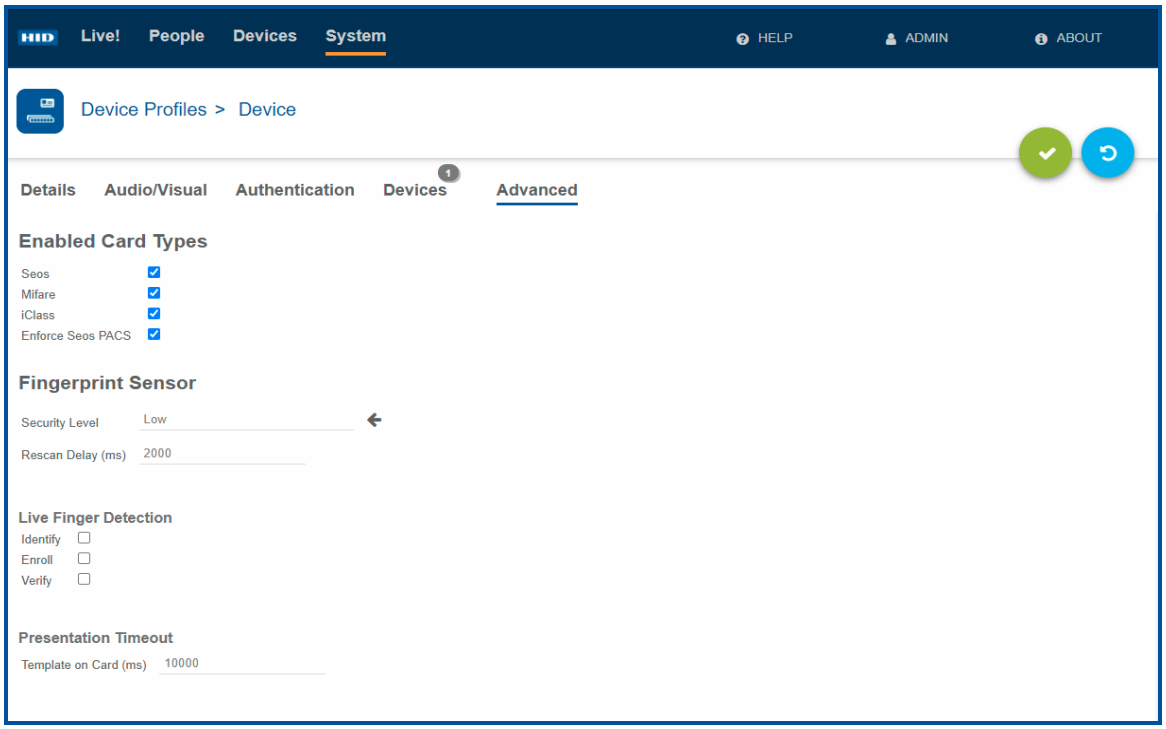


In the case of an accidental tamper where the device keeps power, a Tamper event will appear in the **Live!** view. The Device health will now be red. To restore communications between the Device and HID Biometric Manager, the Device must be uninstalled from HID Biometric Manager and then re-installed.

2.25 Enforce Seos read

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

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



2. Click .

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

2.26 Backup and recovery

HBM supports a Microsoft SQL database for storing device configurations and encrypted user enrollment information. The backup and recovery feature allows you to move HBM to a different server without having to re-install devices, and re-enroll the users.

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

Note: The backup and recovery feature is only available with Firmware version 1.5.1.22 or higher.

2.26.1 Generate recovery key

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

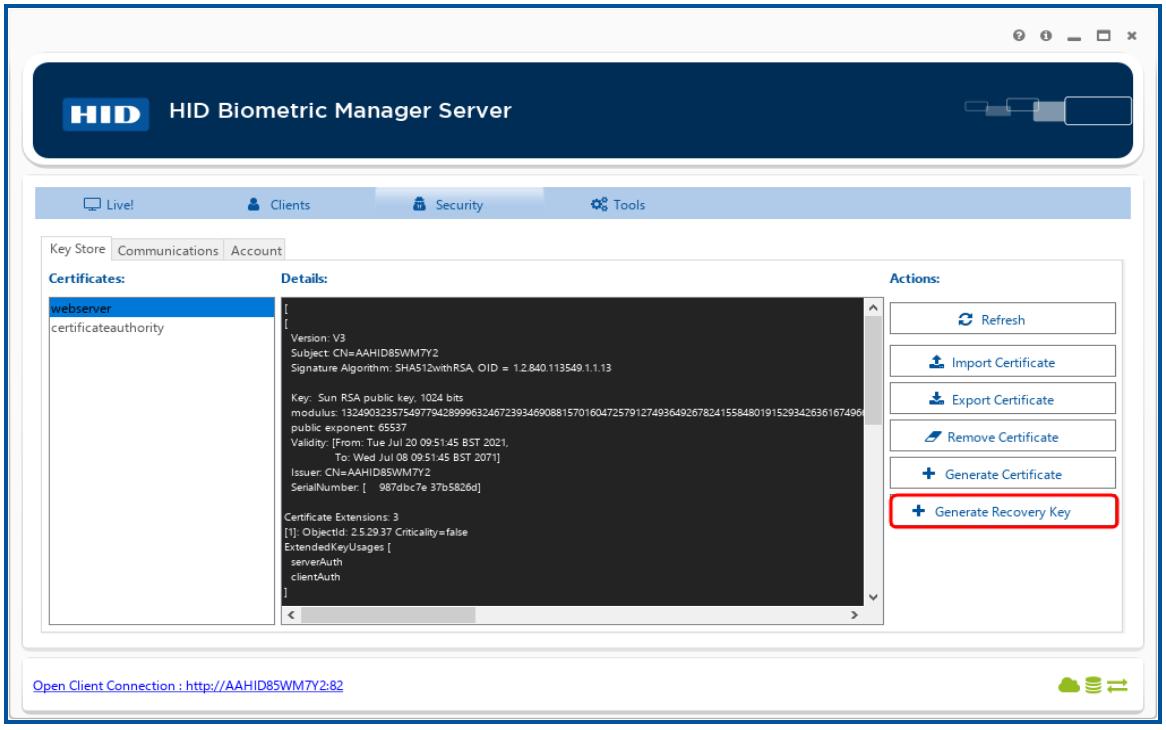
A new key is only required if:

- Clean install is performed
- After updating to 1.5.1.22 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**.



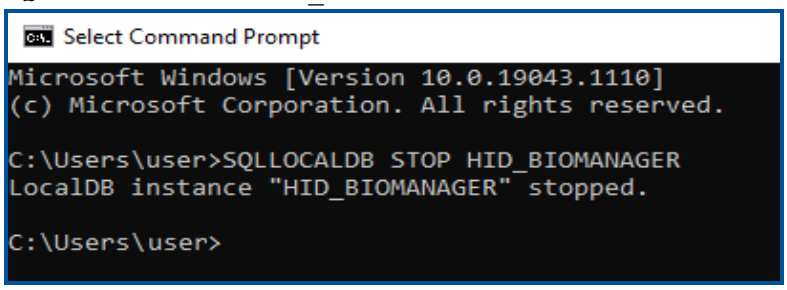
2. The **Recovery Key Generator** window is displayed. Click **Generate Key**.
3. Click **OK** once the Recovery Key message appears then close the **Recovery Key Generator** window.
4. Copy and save the generated recovery key and save to a secure machine or multiple locations other than the HBM server.

   Important: If the Recovery is lost, the backups can not be recovered.

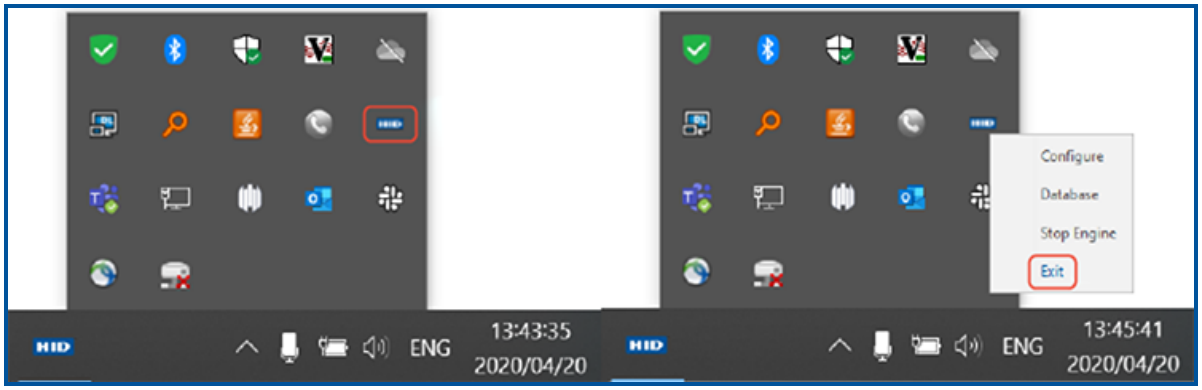
2.26.2 Backup procedure

The following shows the backup procedure on the original server.

1. Stop the SQL local database by opening a command prompt and type:
   `SQLLOCALDB STOP HID_BIOMANAGER`.



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.

   The backup is now complete. It is now safe to start up HBM if no recovery procedure is needed.

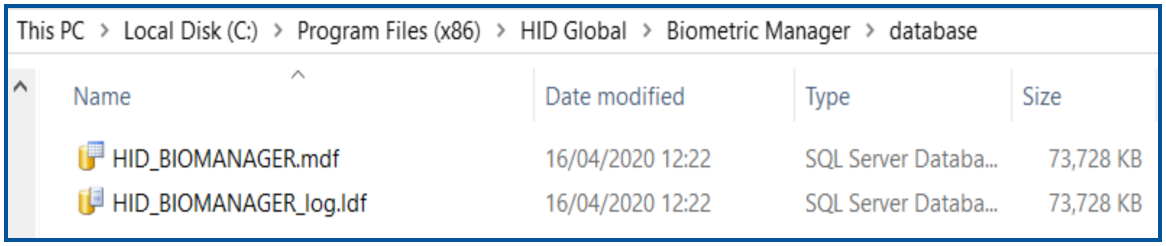
   Note: During the backup procedure, the readers will continue to operate but HBM will be unavailable.

2.26.3 Restore procedure

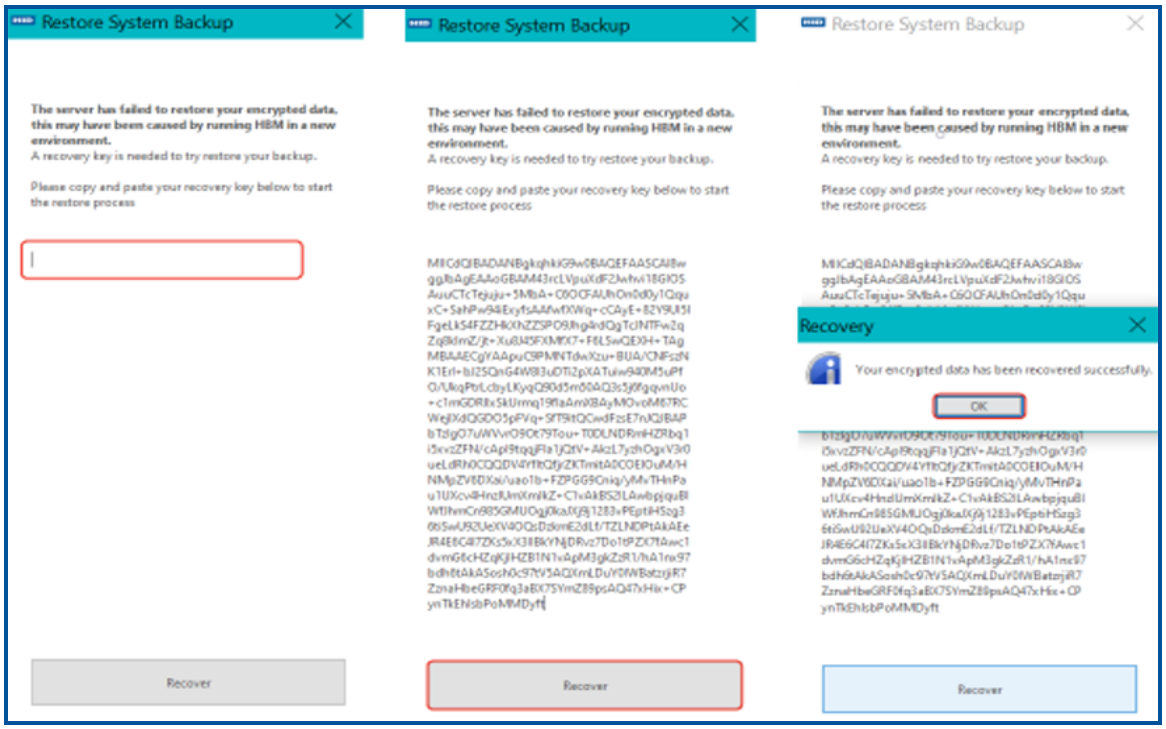
The restore procedure takes place on the recovery server.

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.

   Note: To check the SQL version on the recovery machine, connect to the server side Database and perform the **Select @@version** command.
3. Install HID Biometric Manager but do not start up HBM.
4. Copy and paste the previously backed up **.mdf** and **.ldf** files to **C:\Program Files (x86)\HID Global\Biometric Manager\database**.

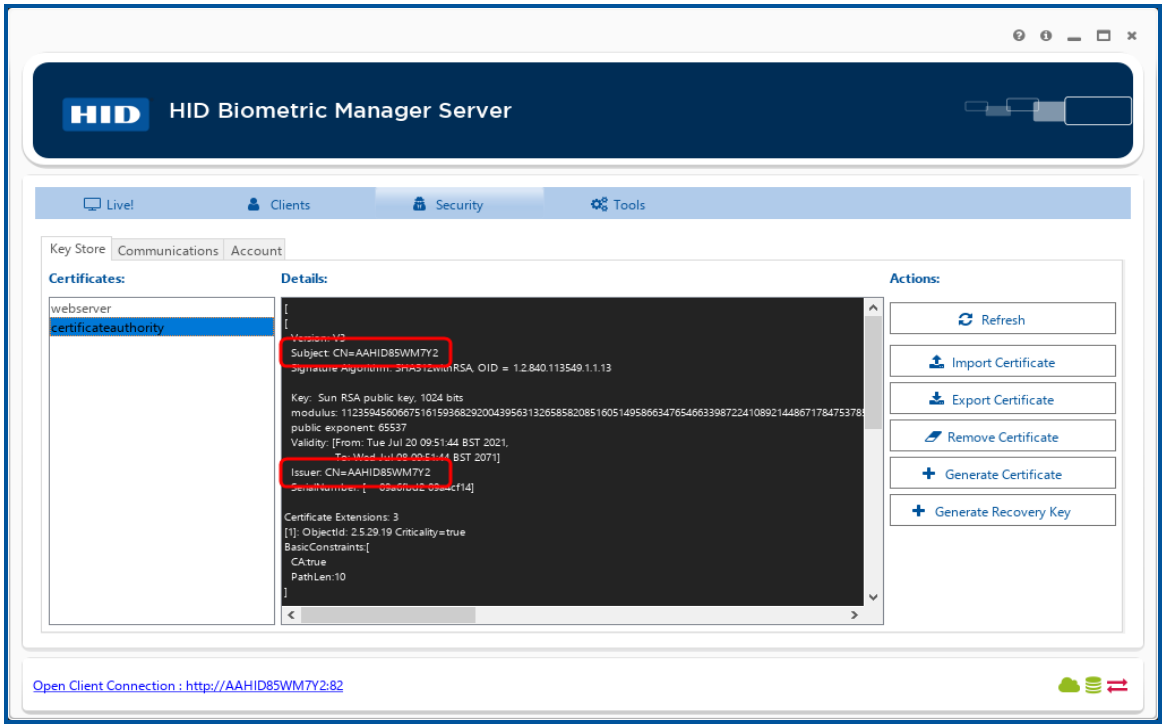


5. Launch HBM. The recovery key will need to be entered:
   1. Paste the recovery key in the field.
   2. Click **Recover**.
   3. On successful recovery, click **OK**.



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.

1. Open the **Security** tab.
2. 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.



7. Log into HBM and uninstall all connected devices. Do not **Factory Default** through the software.
8. Factory default all devices using the pins on the reverse of the unit, see *HID Signo Biometric Reader 25B User Guide* (PLT-04900).
9. Wait one minute for devices to reboot after factory default.
10. Re-install all devices within HBM.
11. Test the communication between devices and HBM.

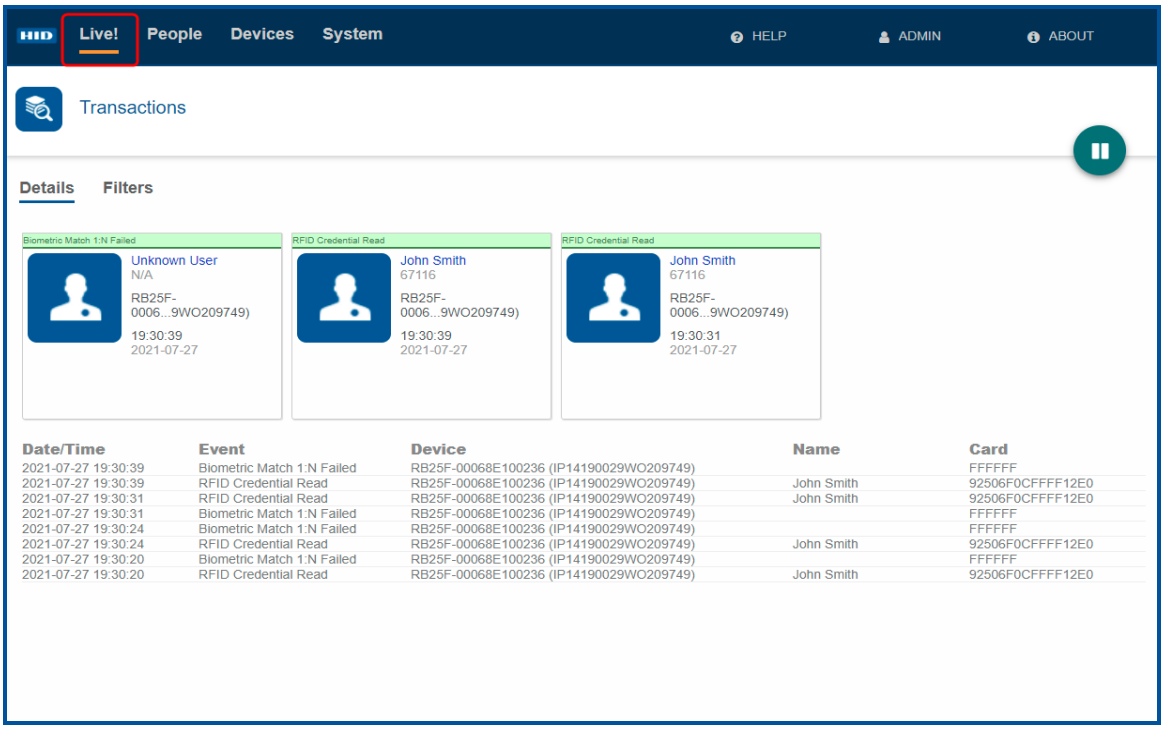
2.27 System monitoring and Reports

This allows you to view live feedback for connected Signo Biometric Reader 25B reader events like credential reads and configuration updates. You can filter the **Live!** feed to view specific parameters of an event.

2.27.1 View HID Biometric Manager events

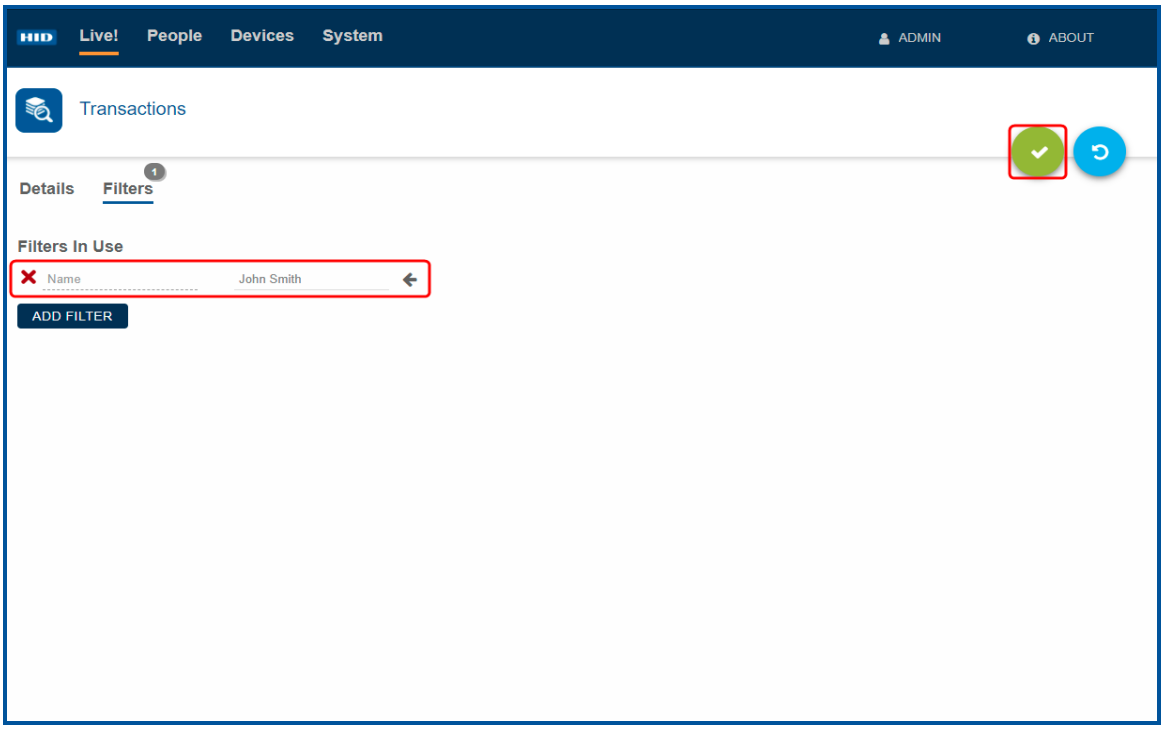
Actions carried out in HID Biometric Manager are logged as events. To view a HID Biometric Manager event click the **Live!** option. To examine individual entries when the network is busy click the pause icon to pause real-time network monitoring.

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



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 to save any added filters.

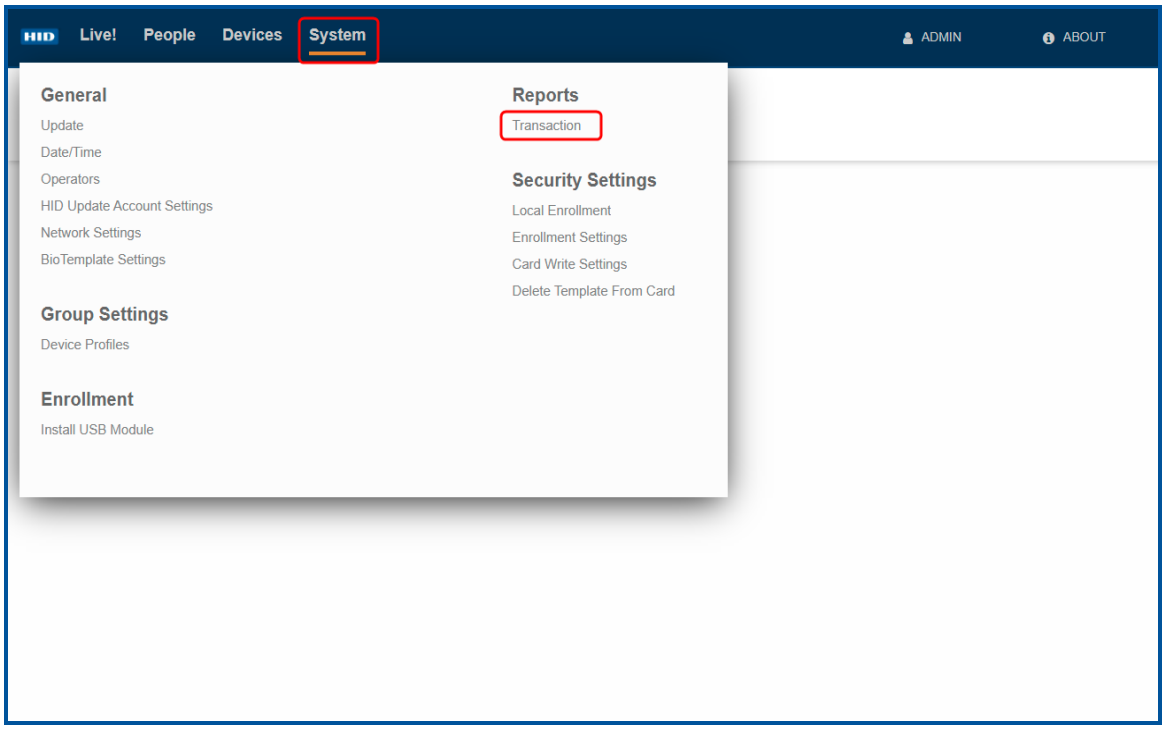
Note: If no filters are used then the default filter is applied. This displays events only for the calendar day.


Live!
People
Devices
System
ADMIN
ABOUT
Transactions
Details
Filters
1
Filters In Use
Name
John Smith
ADD FILTER

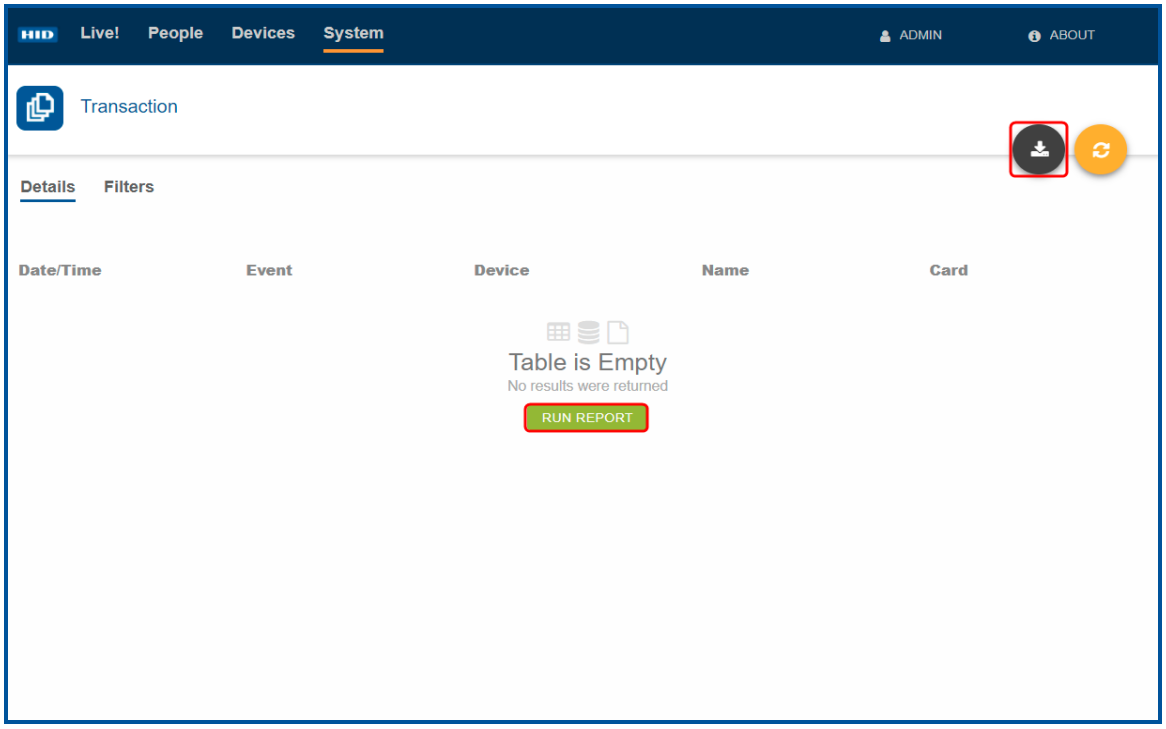
2.27.2 Transaction Reports

To create a report of HID Biometric Manager transactions:

1. Click **System** and select **Transaction** option.

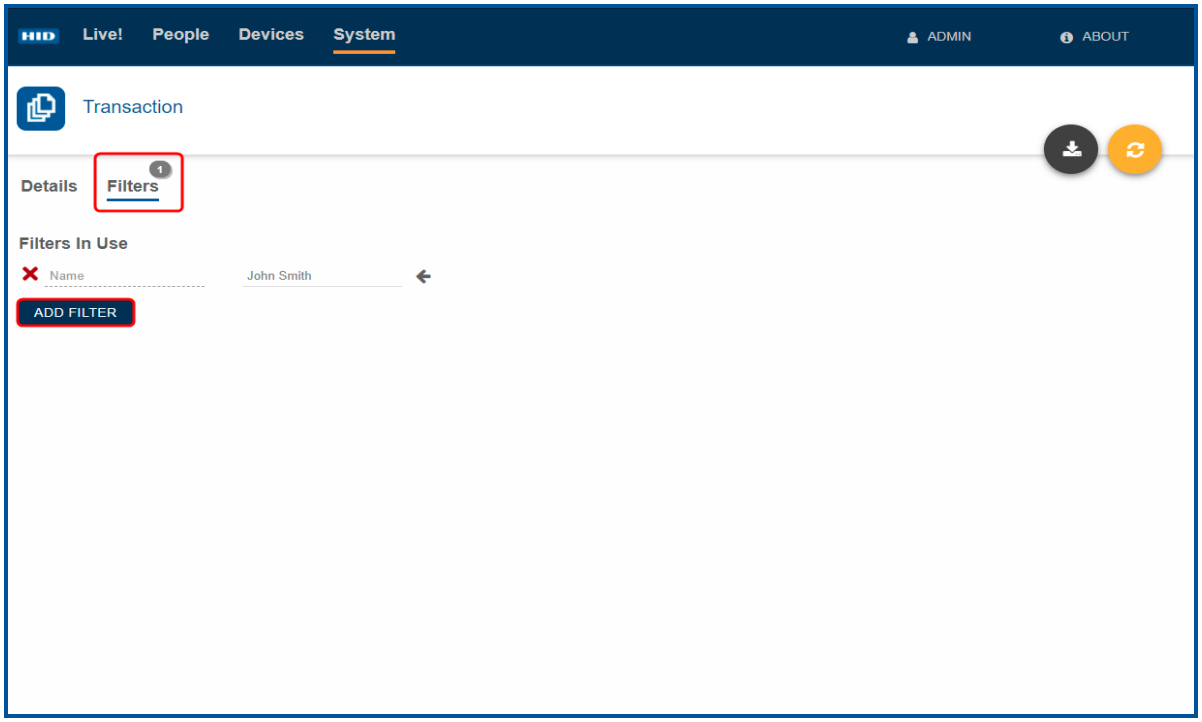


2. Click **RUN REPORT** to create a report of HID Biometric Manager transactions. Once the report is created click the save report icon [⬇] to save the report to a PDF or CSV file.



3. 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 **Device, Date/Time, Event**, or **Person**. Click ✔ 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**

HID Origo set up

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 Origo® Portal. The section also details how to verify HID Reader Manager™ Technician account details in HID Biometric Manager and how to load HID Origo (MOB) keys onto the Signo Biometric Reader 25B.

A.1 Setup prerequisites

In order to setup a connection between HID Biometric Manager and HID Reader Manager for updates and to facilitate loading MOB keys onto the Signo Biometric Reader 25B 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 and creates a primary account administrator. For detailed information on the onboarding process visit the onboarding site at:

https://portal.origo.hidglobal.com/mobile-identities/#/home

For information relating to the HID Mobile Access solution, including the HID Origo 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 HID Origo 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 HID Origo Management 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:

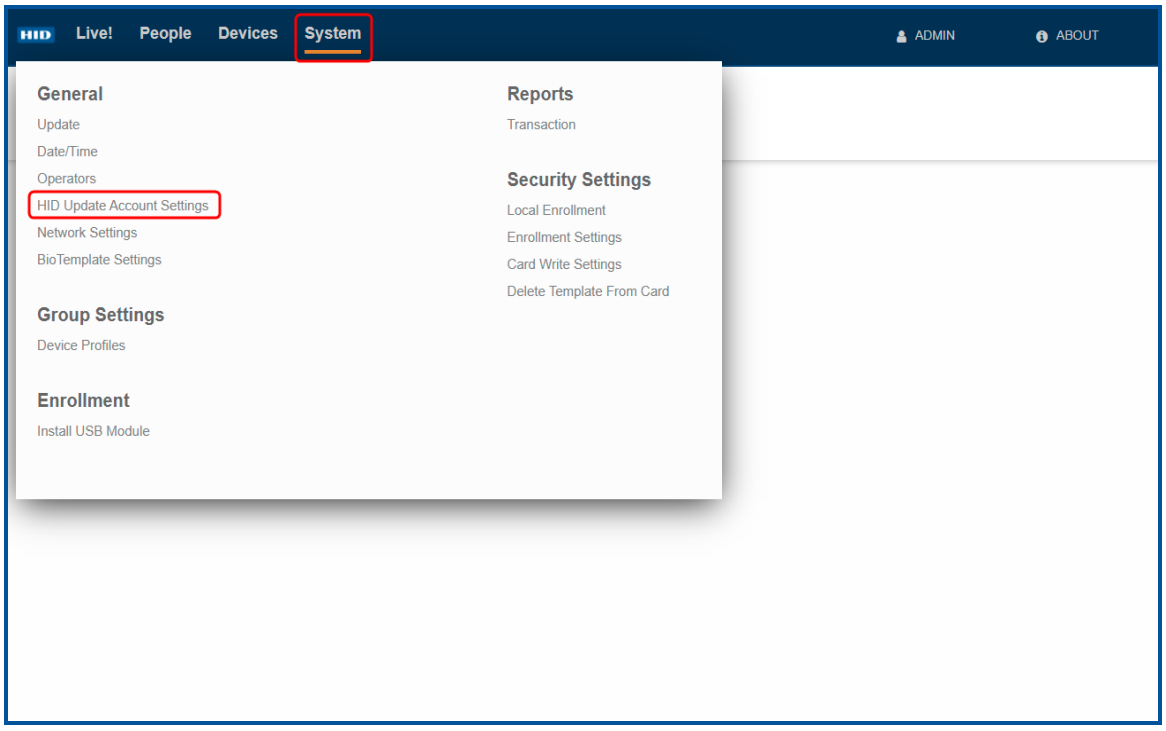
- *HID Mobile Access Frequently Asked Questions* (PLT-02085).
- *HID Mobile Access App User Guide* (PLT-02077).

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

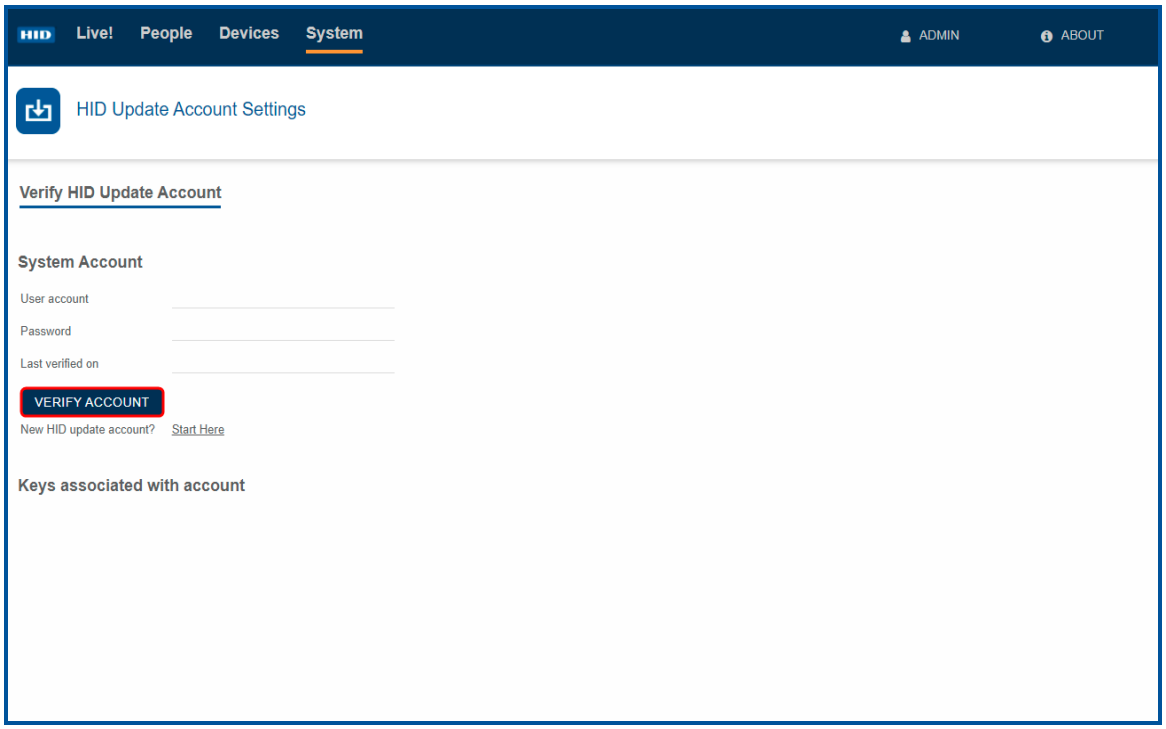
In order to validate a Reader Manager Technician account in HID Biometric Manager an active Reader Manager Technician account must be present, see **A.1.2 HID Reader Manager setup**.

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

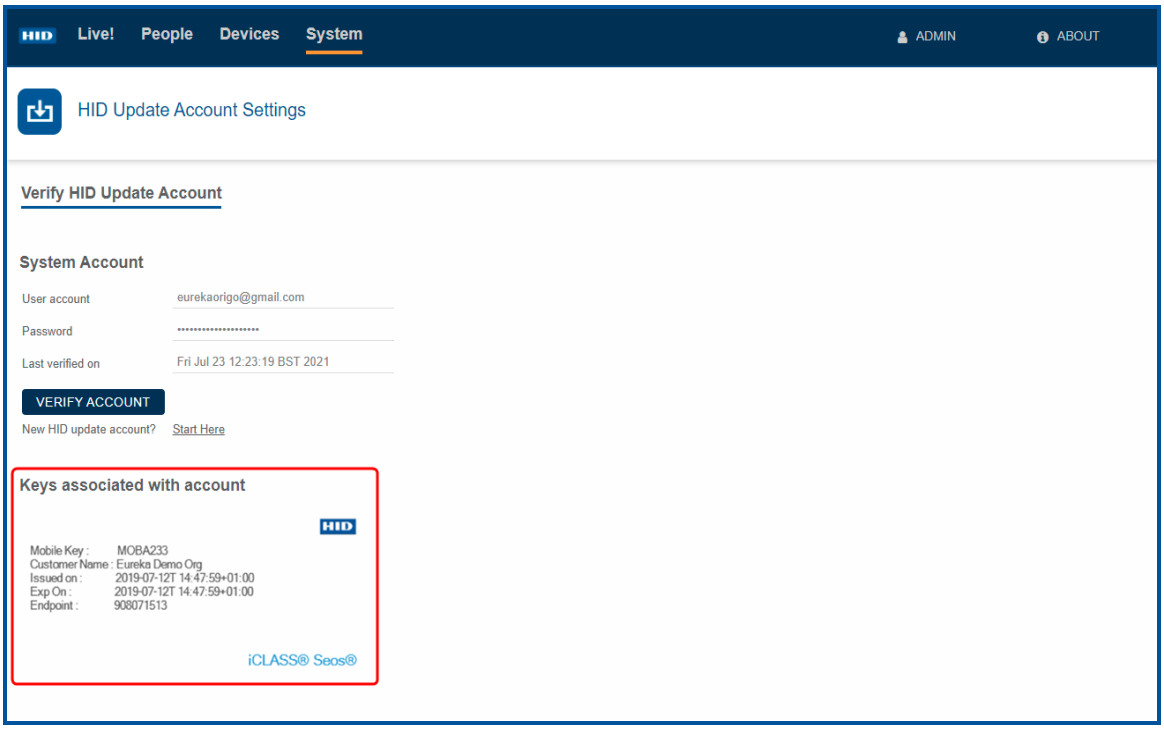
1. Log into HID Biometric Manager.
2. Select **System** and under the **General** section click **HID Update Account Settings**.



3. On the **HID Update Account Settings** page enter the System or Individual account details **User account**/**Password**) and click **VERIFY ACCOUNT**.



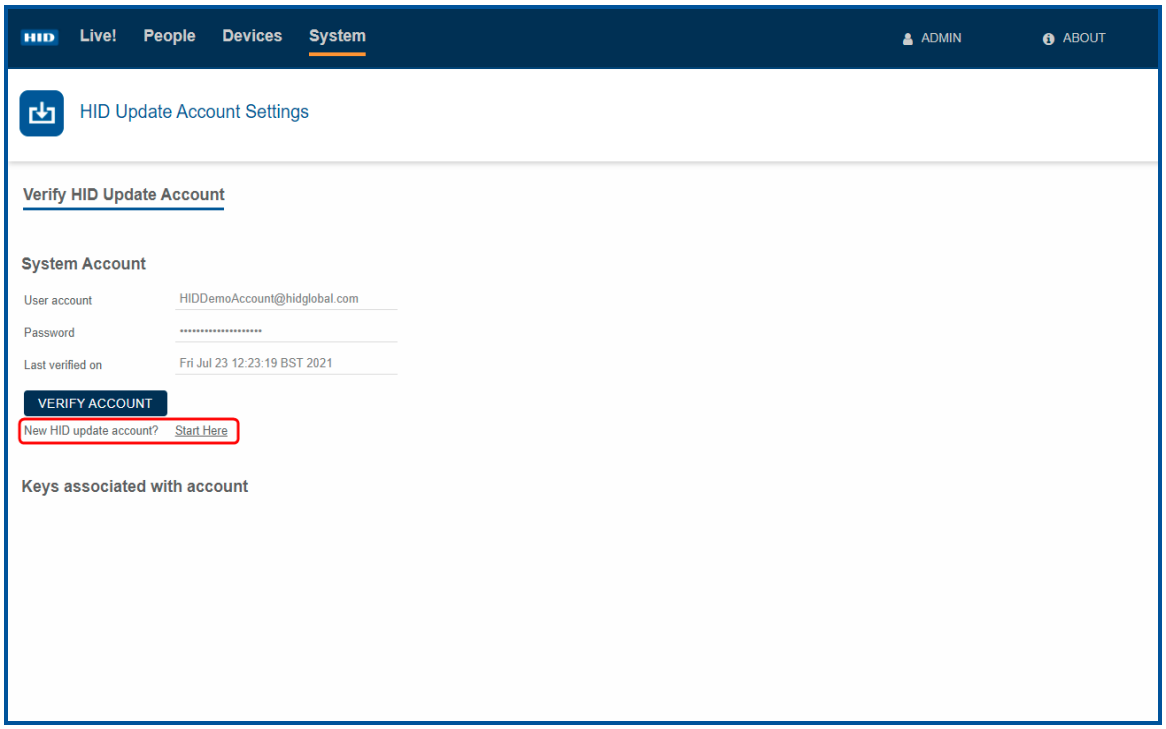
If the Reader Technician account has not been authorized for any MOB keys then no keys are listed under **Keys associated to Account**. If MOB keys have been assigned to the account then these will be listed in.



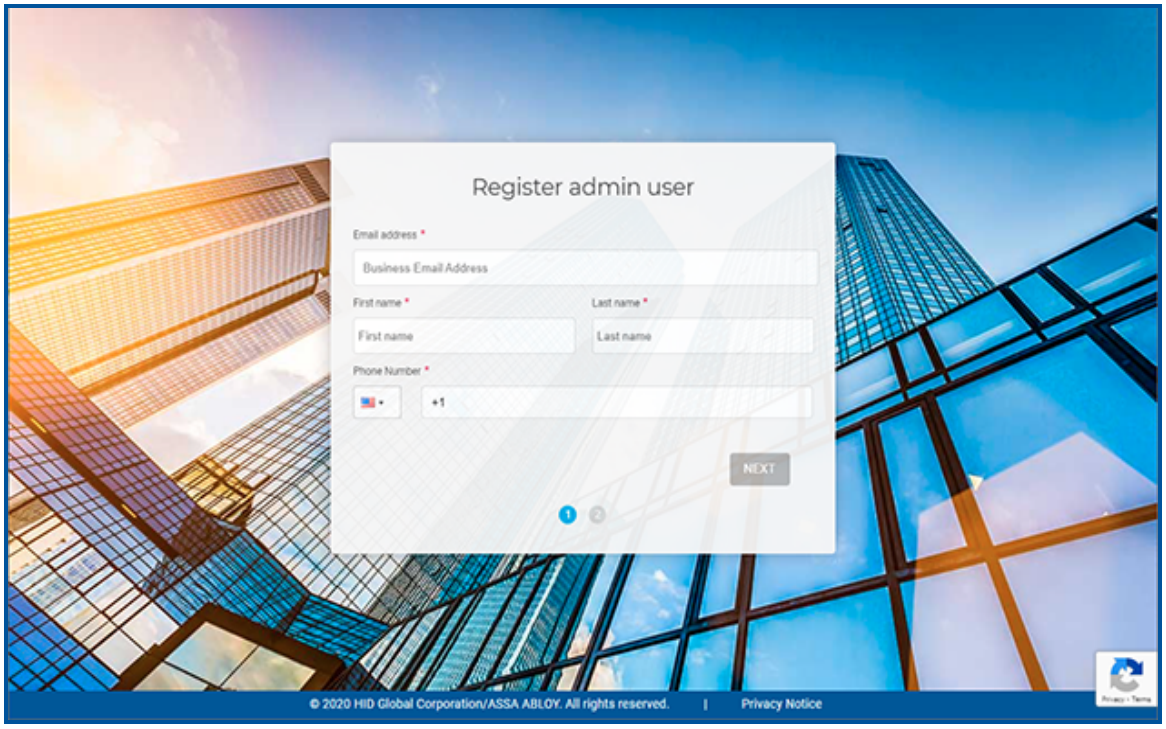
A.2.1 Create an Origo system account in HBM

You can create a new HID Origo system account through the **HBM System** > **HID Update Account Settings** page.

1. Click **Start Here**.



2. Fill in the required information and follow the prompts to create your account.

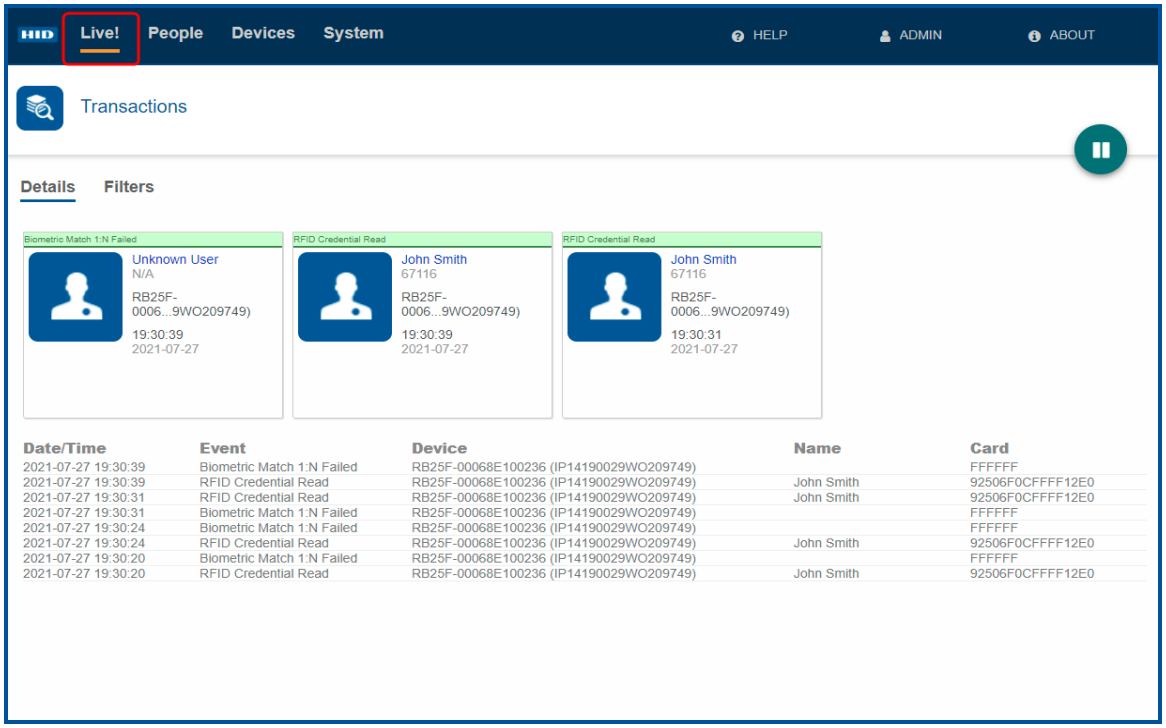


A.3 Test MOB keys are working correctly

As a prerequisite to test that a MOB key working correctly, the HID Origo Management 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 **A.1.3 Mobile Access user setup**.

To test a MOB key in HID Biometric Manager:

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



2. Present the mobile device to the Signo Biometric Reader 25B 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 Signo Biometric Reader 25B 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 Signo Biometric Reader 25B is in finger mode.

Appendix **B**

Fingerprint template encryption

B.1 In-field update for existing installations

To provide greater data security, the Signo Biometric Reader 25B solution encrypts templates stored on the server and device database as a default. This was introduced in HBM version 1.0.886.57608. To get the current software and device firmware to use this feature:

1. Update the HID Biometric Manager software to software version 1.0.1550.62511.
2. Update the firmware of each Signo Biometric Reader 25B device connected to the HID Biometric Manager.
3. After updating the Signo Biometric Reader 25B devices, each device must be reset to their factory default state. See **2.6.6 Reset a device**
4. Uninstall each Signo Biometric Reader 25B device from within HID Biometric Manager and re-install them.

   Note: Steps 3 and 4 ensure a clean move to HBM version 1.0.886.57608 or higher.

   Note: The device profile will sync to make sure all the reader configuration is downloaded to the Signo Biometric Reader 25B device after re-installation and once connection has been established with the HID Biometric Manager.

B.2 New installations

1. Verify that the HID Biometric Manager software is at version 1.0.1550.62511, and Signo Biometric Reader 25B is at firmware version 1.5.1.50.
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.

B.3 Additional information on the Signo Biometric Reader 25B template encryption

- All Signo Biometric Reader 25B 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 Signo Biometric Reader 25B has been updated to firmware version 1.5.0.86, and the Signo Biometric Reader 25B 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 Signo Biometric Reader 25B. 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 decryption keys before it can become fully operational.
2. As part of HBM version 1.0.886.57608 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.

Appendix C

Acronyms and terminology

Term	Definition
Authentication Mode (Signo Biometric Reader 25B)	**Template on Card:** The Signo Biometric Reader 25B 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 Signo Biometric Reader 25B 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 Signo Biometric Reader 25B 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 Signo Biometric Reader 25B 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). **Card Only (or) Finger Only**: The Signo Biometric Reader 25B 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 interoperability among access control and security products.

Term	Definition
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.

Buzzer and LED defaults

Buzzer	State	Duration (Tenth of a second)	LED Color
Anti-passback	1. Initial State 2. Alternative State 3. Total Duration	1 0 9	Cyan Blue
Biometric Match Fail	1. Initial State 2. Alternative State 3. Total Duration	1 0 10	Red Blue
Biometric Match Success	1. Initial State 2. Alternative State 3. Total Duration	1 0 6	Green Blue
Biometric Match Timeout	1. Initial State 2. Alternative State 3. Total Duration	1 0 10	Red Blue
Biometric Scan Fail	1. Initial State 2. Alternative State 3. Total Duration	1 0 10	No color Blue
Biometric Scan Success	1. Initial State 2. Alternative State 3. Total Duration	1 0 10	No color Blue
Biometric Scan Timeout	1. Initial State 2. Alternative State 3. Total Duration	1 0 10	Red Blue
Credential Read Fail	1. Initial State 2. Alternative State 3. Total Duration	0 0 0	Red Amber
Credential Read Success	1. Initial State 2. Alternative State 3. Total Duration	1 0 9	Amber Magenta
Credential Read Timeout	1. Initial State 2. Alternative State 3. Total Duration	0 0 0	Red Amber
Enrollment Mode	1. Initial State 2. Alternative State 3. Total Duration	1 0 9	Cyan Amber
Fingerprint Scanned	1. Initial State 2. Alternative State 3. Total Duration	1 0 8	Black Magenta
Network Communications Error	1. Initial State 2. Alternative State 3. Total Duration	1 0 20	Red Blue
Other Media Read	1. Initial State 2. Alternative State 3. Total Duration	1 0 9	Green Red

Buzzer	State	Duration (Tenth of a second)	LED Color
Power-Up Complete	1. Initial State 2. Alternative State 3. Total Duration	1 0 6	Green Blue
Seos Card Read	1. Initial State 2. Alternative State 3. Total Duration	1 0 8	Magenta Green
Seos Credential Read Failed	1. Initial State 2. Alternative State 3. Total Duration	1 0 8	Red Black
Seos Credential Read Success	1. Initial State 2. Alternative State 3. Total Duration	1 0 8	Magenta Green
Idle	-	-	Red

Revision history

Date	Description	Revision
October 2021	Updates to support HID Biometric Manager version 1.0.1550.62511.	B.2
March 2021	Updates to support Signo Biometric Reader 25B Reader version 1.5.1.44 and HID Biometric Manager version 1.0.1212.60729.	B.1
October 2020	Product rebrand from iCLASS SE® iCLASS SE RB25F to HID Signo® Biometric Reader 25B	B.0
June 2020	Updates to support iCLASS SE iCLASS SE RB25F Reader version 1.5.1.22 and HID Biometric Manager version 1.0.1103.59811. Product rebrand from iCLASS SE RB25F to Signo Biometric Reader 25B.	A.4
December 2019	Updates to support HID Biometric Manager Signo Biometric Reader 25B Reader version 1.5.0.86 and HID Biometric Manager version 1.0.886.57608.	A.3
September 2019	Updates to support Signo Biometric Reader 25B reader version 1.5.0.82 and HID Biometric Manager 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

hidglobal.com

For technical support, please visit: https://support.hidglobal.com

PLT-04029, Rev. B.2

Part of ASSA ABLOY