# HID<sup>®</sup> Biometric Manager<sup>™</sup> Administration Guide

PLT-04029, B.3 August 2022





# Copyright

© 2022 HID Global Corporation/ASSA ABLOY AB. All rights reserved.

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

# Trademarks

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

# **Contacts**

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

## What's new

Date	Description	
August 2022	Updates to support HID Biometric Manager version 1.0.2000.00019.	B.3

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

Introduction	
1.1 Document purpose	
1.2 Intended audience	
1.3 Related material	
1.4 Physical Access Control System overview	
1.5 HID Biometric Manager server application	
1.5.1 System requirements	
1.5.2 Reader Service	
1.6 HID Biometric Manager Web UI	
1.7 Signo Biometric Reader 25B	
1.8 Panels and Door Controllers	
HID Biometric Manager	
2.1 Overview	
2.2 HID Biometric Manager initial setup	
2.2.1 HID Biometric Manager software install	
2.2.2 HID Biometric Manager initial login	
2.2.3 About Section in the UI	
2.2.4 Configure time zone setting	
2.3 Device installation and configuration	
2.3.1 Perform network scan:	
2.3.2 Scan network using an IP range	
2.3.3 Configure device settings	
2.4 Create HID Biometric Manager operators	
2.4.1 Device firmware update	
2.4.2 Individual device firmware update	
2.4.3 Force firmware update	
2.4.4 Reset a device	
2.4.5 Uninstall a device	
2.5 Setting static IP for HBM network	40
2.6 Setting static IP for a specific device	41
2.6.1 Configuring Template expiry date	
2.6.2 Configuring schedule for deleting expired templates	43
2.6.3 Override System Template Expiry	44
2.7 Configure device template encryption	45
2.8 Delete template on card	
2.9 Delete all templates	
2.10 Key management	
2.10.1 Load a MOB key onto a device	

2.10.2 Load HID Elite keys	
2.11 Configure software/firmware update settings	
2.12 Device profiles	
2.12.1 Create a device profile	
2.12.2 Edit a device profile	
2.12.3 Delete a device profile	
2.13 Device health indication	
2.14 Device debug page	
2.15 Tamper settings	
2.16 Enforce Seos read	
2.17 System monitoring and Reports	
2.17.1 View HID Biometric Manager events	
2.17.2 Transaction Reports	
2.18 System Diagnostics	71
Enrollment	
3.1 Enrollment	73
3.1.1 Enroll people	73
3.1.2 Enroll Cards	
3.2 Install SIGNO-B-USB Module	
3.2.1 SIGNO-B-USB Enrollment	
3.2.2 Enroll Biometrics	
3.2.3 Local enrollment	
3.3 Preventing user fingerprint display during enrollment	
3.3.1 Write fingerprint templates to a card	
3.4 Bypass finger TOC	
3.4.1 Enrollment without fingerprints	
3.4.2 Enrollment with fingerprints	
3.5 BioTemplate settings	
3.5.1 Auto download template	
HID Biometric Server Application	
4.1 Resetting administration password	
4.1.1 Data import	
4.1.2 HID Biometric Manager Server application icons	
4.2 Live!	
4.3 Credential Database	
4.4 Backup and recovery	
4.4.1 Generate recovery key	
4.4.2 Backup procedure	101
4.4.3 Restore procedure	

4

Network	
5.1 Network setups examples	
5.2 Network usage	
5.3 Device discovery	
5.4 Secure device communication	
5.5 Chain of trust	
HID Origo set up	
A.1 Setup prerequisites	
A.1.1 HID Mobile Identities setup	
A.1.2 HID Reader Manager setup	
A.1.3 Mobile Access user setup	
A.2 Create an Origo system account in HBM	
A.3 Validate a Reader Manager account in HID Biometric Manager	
A.4 Test MOB keys are working correctly	112
Fingerprint template encryption	
B.1 In-field update for existing installations	
B.2 New installations	
B.3 Additional information on the Signo Biometric Reader 25B template encryption	
Guidelines for setting up MS SQL database	
C.1 Manually attaching the database	
C.2 SQL Server set up	
C.3 Remote SQL server set up	
Acronyms and terminology	

# Section 01



# **1.1 Document purpose**

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

#### The iCLASS SE® RB25F has been rebranded as the HID Signo Biometric Reader 25B.

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

**Note:** Unless specified, all HBM version 1.0.2000.00019 features are available for RB25F customers. The features not compatible with the RB25F will be called out explicitly throughout the document.

For more information on the Signo 25B, 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 25B devices, enroll people in the system, add credentials and biometric data.
- HID Signo 25B Biometric Reader installers: The document provides information relating to the Signo 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 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 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 25B devices and PACS Panel/Door Controllers can be added. HID Biometric Manager can control up to 2,000 Signo 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 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 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 Reader Service

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

# 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 25B readers. It is also used to perform user registration including fingerprint enrollment. Any connected Signo 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 25B device firmware.

# 1.7 Signo Biometric Reader 25B

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

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

See **Authentication Mode (Signo 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 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 25B devices and PACS Panel/Door Controllers can be added. HID Biometric Manager can control up to 2,000 Signo 25B devices.







# 2.1 Overview

HID<sup>®</sup> Biometric Manager<sup>™</sup> 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. HBM 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 HBM software, and creates/administers operator roles within the application see 2.2 HID Biometric Manager initial setup.
- Administrator: This operator role has full access to HBM web application with functions to install and manage Signo 25B devices see 2.3 Device installation and configuration and enroll people in the system, add credentials, collect and store associated biometric data see 3.1 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 25B. This operator role has limited access to user information.
- Enrollment: This operator role has full access to HBM 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 3.1 Enrollment.

# 2.2 HID Biometric Manager initial setup

## 2.2.1 HID Biometric Manager software install

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

#### Notes:

- The user installing the HBM software needs to be logged in on the server as a Windows Administrator.
- The host name must be set before installation. Changing this after installation can impact device communications.
- When using a static IP, it must be set before installation. Changing this after installation can impact device communications.
- 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 Portuguese
- German Russian
- Spanish 
   Simplified Chinese
- French
   Japanese
- Italian
   Korean
- 3. Select the required language and click OK.

Select Setup Language		$\times$
ню	Select the language to use during the installation.	
	English	~
	OK Cancel	

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

🚥 Setup - HID Biometric Manager —		
HID	HID Biometric Manager v99.99.250.58260	
	This will install HID Biometric Manager version v99.99.250.58260 on your computer.	
	It is recommended that you close all other applications before continuing.	
	Click Next to continue, or Cancel to exit Setup.	
	Next > Cancel	

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.

🚥 Setup - HID Biometric Manager	-	×
License Agreement Please read the following important information before continuing.	HI	D
Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.		
HID GLOBAL CORPORATION HID BIOMETRIC MANAGER END USER LICENSE AGREEMENT ("EULA") (v.20190315)		
IMPORTANT - READ CAREFULLY: This End User License Agreemen ("EULA") is a legal agreement between you, either an individual or ar entity on whose behalf you are acting, as the case may be ("Licensee") and HID Global Corporation ("HID") governing the use of software products and modules ("Software") that came with this EULA. whethe	t , , r	
○ I <u>a</u> ccept the agreement		
I do not accept the agreement		
< Back Next >	Cancel	

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

🚥 Setup - HID Biometric Manager —		
HID	Completing the HID Biometric Manager Setup Wizard	
	Setup has finished installing HID Biometric Manager on your computer. The application may be launched by selecting the installed shortcuts.	
	Click Finish to exit Setup.	
	Finish	

For information on the HBM Server application, see HID Biometric Server Application

## 2.2.2 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/HIDBiometric/Manager.html

					0 0 _ 🗆 ×
HID H	ID Biometric Ma	nager Server			
Live!	🛔 Clients	a Security	OS Tools		
Date/Time	Event	Device	Name	Card	
Open Client Connection : I	http://AAHID85WM7Y2:82				▲≣≓

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.



HID	
	HID Biometric Manager   HID Biometric Manager   LOGIN
Copyright © 2021 HID reserved.	Global Corp. All rights

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

Note: Users will be locked out for 30 minutes after seven failed login attempts.

#### 4. Click **System > Operators**.

HID Live! People Devices System	HELP	🛔 ADMIN	() ABOUT
General	Reports		
Update	Transaction		
Date/Time			Q
Operators	Security Settings		
HID Update Account Settings	Local Enrollment		
Network Settings	Enrollment Settings		
BioTemplate Settings	Card Write Settings		
	Delete Template From Card		
Group Settings			
Device Profiles			
Encollment			
Enrollment			
Install USB Module			



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

HID Live! People Devices System	m —		HELP	🛓 ADMIN	ABOUT
Operators					•
Q Search					-
Login Name Operator Profile	Date Created				
admin Administrator		<u>a</u>			

- 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:** The new password must be a minimum of 12 characters. Clicking on the eye icon when entering the new password will display the password.

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

Live! People Devices System	HELP	ADMIN
Operators > admin		
Details Security		
Change Password		
Old Password		
New Password		
Confirm Password		

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

# 2.2.3 About Section in the UI

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

HID	Live!	People	Devices	System			🛔 ADMIN	
	Device	S						٥
Q Sea	arch				About			
					HID HID Biometric Manager Version: 1.0.1495.62485			
					2021 HID Global Corp. All rights reserved.	OK		

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

## 2.2.4 Configure time zone setting

Setting the time zone configures the time zone for the instance of HBM running on the server.

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

HID Live! People Devices System		HELP	🐣 ADMIN	<ul> <li>ABOUT</li> </ul>
General	Reports			
Update	Transaction			
Operators	Security Settings			<b>Q</b>
HID Update Account Settings	Local Enrollment			
Network Settings	Enrollment Settings			
BioTemplate Settings	Card Write Settings			
	Delete Template From Care	b		
Group Settings				
Device Profiles				
En en lles ant				
Enrollment				
Install USB Module				
		_		

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

HID	Live!	People	Devices	System	HELP	🛓 ADMIN	<ul> <li>ABOUT</li> </ul>
	Date/T	ime					
Time	Zone	÷					

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. Date/Time Select E E Time Zone ) 🗲 Time Zone Europe/Kiev Europe/Lisbon Europe/Ljubljana Europe/London Europe/Luxembourg Europe/Madrid Europe/Malta Europe/Mariehamn Europe/Minsk CANCEL 5. <u>Click</u> HID Live! People Devices System HELP () ABOUT Date/Time 5 Time Zone Europe/London ÷

**Powering** Trusted Identities

HID

# 2.3 Device installation and configuration

Device installation and configuration with HBM can only be carried out by the Administrator or Device Administrator role. For initial configuration or when no devices are installed, HBM 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 **3.1 Enrollment**.

## 2.3.1 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 [].

HID Live! People	Devices System		HELP	🛔 ADMIN
Devices				D
Q Search				-
		No devices installed.		

3. Click SCAN NETWORK to view the complete list of available devices.

**Note:** If no devices are found check the ports listed in **5.2 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.



HID Live! People Devices				
Devices	Install			
	Select device to install.		- 1	
Q Search	Q Search		- 1	
Name MAC Ad			- 1	
RB25F-00068E100236 (IP14 00-06-8E-			- 1	
	Table is Empty No results were returned. Check your content and fil	ters		
	SCAN NETWORK	End Address CANCEL	FINISH	

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

Note: The Host Name should not include any underscores.

HID Live! People Devi				
Devices	Install			
	Select device to instal	Ι.		
Q Search	Q Search			
	Host Name	IP Address		
	RB25F-00068E100236	169.254.3.105		
		Start Address E	End Address	
			CANCEL FINISH	

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.

HID	Live! People De	evices System			HELI	P 🛔 ADMIN
	Devices					
Q :	Search					-
	Name	MAC Address	IP Address	Version		
R	RB25F-00068E100236 (IP1-	4 00-06-8E-10-02-36	169.254.3.105	1.5.1.50	e 🕅	

Note: To uninstall a device, see 2.4.5 Uninstall a device.

## 2.3.2 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.

HID Live! People Device				
Devices	Install			
	Select device to install.		- 64	
Q Search	<b>Q</b> Search		- 84	
	Host Name	IP Address		
	RB25F-00068E100236	169.254.3.105	_	
			_	
			_	
			_	
			_	
			_	
			_	
	SCAN NETWORK Use IP Range	Start Address End Address		
		CANCEL	FINISH	

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

## 2.3.3 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.

HID	Live! People De	evices System			9 HELP	admin	<ul> <li>ABOUT</li> </ul>
	Devices						Q
<b>Q</b> s	earch						-
	Name	MAC Address	IP Address	Version			
Ro	RB25F-00068E100236 (IP14.	00-06-8E-10-02-36	169.254.3.105	1.5.1.50	<b>1</b>		
					_		

- 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 **2.12.2 Edit a device profile**.

HID Liv	re! People Devices System	HELP	💄 ADMIN	<ul> <li>ABOUT</li> </ul>
De	vices > RB25F-00068E100236 (IP14190029WO209749)			G
Details	Communication Key Management Advanced			
Device Info	ormation			
Name	RB25F-00068E100236 (IP14190029)			
Description	PEMAINING CHARACTERS:512			
MAC Address	00-06-8E-10-02-36			
Serial Address	IP14190029WO209749			
Version	1.5.1.36			
Profile	Device			

#### 5. Click the **Communication** tab.

HID L	ive! Peo	ple Devi	ces System				HELP	🛔 ADMIN	ABOUT
	)evices >	RB25F-00	068E100236 (	IP14190029WO2097	749)				¢
Details Network	Commun Settings	ication K	(ey Managemer	nt Advanced					
IP Address	169.254.3.1	)5	Static						
Subnet Mask	255.255.0.0								
Gateway	0.0.0.0								
Hostname	RB25F-0006	8E100236							
Dns 1	127.0.0.53								
Dns 2									
Host Co	Wiegand	s Mode	÷						
BLE Set	ttings Access 🗹								
<b>Operation</b> Tap Twist and Go	Modes v								
Range and	d Power Sett	ings							
Tap Range (	dBm)	-40		<b>+</b>					
Twist and Go	Range (dBm)	-74		<b>←</b>					
Transmit Pov	wer (dBm)	-4		<b>←</b>					
WRITE	READ								

- 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 HBM, see HID Origo set up.

**Note:** The default range settings for **Tap, Twist and Go** and **Transmit Power** are displayed in HBM. 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:

HID Live! People Devices System	HELP	🛔 ADMIN	ABOUT
Devices > RB25F-00068E100236 (IP14190029WO209749)			¢
Details     Communication     Key Management     Advanced       SYNC     FACTORY DEFAULT     REBOOT DEVICE			•
Device Security			
Increase security by disabling some on-device services.			
Services that will no longer be available: 1. Firmware Upgrade 2. Static IP Address 3. Remote Connection			
CHANGE PASSWORD REDUCE TEMPLATE SECURITY			
Manage Individual Device Firmware			
Use options below to reinstall device firmware or update firmware from local storage.			
These are non-standard options, navigate to the "System" tab, then "Updates" to check for new versions of firmware.			
Install From Local Drive     Reinstall Firmware     This operation may take approximately 25 minutes.     Requires an HID update account     Please refor to HID Biometric Mananer Administration Guide for setting up an HID update account			
UPDATE FIRMWARE			

- **SYNC:** Syncs all device settings in HBM to the device.
- FACTORY DEFAULT: Restores all device settings to the original factory defaults, see 2.4.4 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 HBM to the selected Signo 25B.

# 2.4 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 HBM web application with functions to install and manage Signo 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 25B. This operator role has limited access to user information.
- Enrollment: This operator role has full access to HBM 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.

Live! People Devices System	HELP	🚔 ADMIN	ABOUT
General	Reports		
Update	Transaction		
Date/Time			Q
Operators	Security Settings		-
HID Update Account Settings	Local Enrollment		
Network Settings	Enrollment Settings		
BioTemplate Settings	Card Write Settings		
	Delete Template From Card		
Group Settings			
Device Profiles			
Enrollment			
Install USB Module			

3. To add an operator, click 😶.

HID Live! Pe	ople Devices Syste	m	HELP	🛓 ADMIN	ABOUT
Operators					
Q Search					
Login Name	Operator Profile	Date Created			
aunin	Administrator				

- 4. On the Operators Details screen enter the following:
  - Login: Enter a login name for this operator.
  - Profile: Select the operator profile, Administrator, Device Administrator, or Enrollment.

HID Live!	People	Devices	System		HELP	🛔 admii
	ators					_
Details						
Login	Enrolment Op	erator				
Profile	Enrolment		•			
Link to	John Smith			•		
First Name	John					
Last Name	Smith					
Password						
Confirm Password	•••••					
				_		

## 2.4.1 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. When the version number is orange, only a partial update has been completed.

HID	Live! People	Devices System			HELP	🛔 ADMIN
	Devices					
Q	Search					•
	Name	MAC Address	IP Address	Version		
Ro	RB25F-00068E100236	00-06-8E-10-02-36	169.254.3.105	1.5.1.22		
Ro	RB25F-00068E100236	00-06-8E-10-02-36	169.254.3.105	1.5.0.82		

Important: A HID Origo connection is needed for a full update to be successful.

Full 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.

HID Live! People Devices System	HELP	🛔 ADMIN	<ul> <li>ABOUT</li> </ul>
General	Reports		
Update	Transaction		
Operators	Security Settings		
HID Update Account Settings	Local Enrollment		
Network Settings	Enrollment Settings		
BioTemplate Settings	Card Write Settings		
	Delete Template From Card		
Group Settings			
Device Profiles			
Enrollment			
Install USB Module			

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

Update       Firmware Update         Updates       A New Version Is Available!         Defines       Defines         Choose How Updates Are IND Biometric Manager       Check for update         Device Firmware       Check for update         V       ID Biometric Manager is up to date         Device Firmware update is no to the RB25F firmware is bringing new features and improvements, listed below.         Note: Please update the firmware of all RB25F connected to the system to latest version 1.5.1.44 and the HID Biometric Manager to the latest version 1.0.1484.60763, as soon a possible.         CHECK FOR UPDATES       New Features:	HID Live! People Devic	ces System	HELP	🛓 ADMIN	ABOUT
Updates       A New Version Is Available!         Post Largz 1.5.1.44 is now available - you have 1.5.1.50.       Post Largz 1.5.1.44 is now available - you have 1.5.1.50.         Worning : Devices will be off-line while firmware update is in progress.       Release Notes         HID Biometric Manager       Check for updates         Device Firmware       Check for updates         Update Status       To fully apply this update to all reader devices an HID Update Account must be entered and validated         This new version of the RB25F firmware is bringing new features and improvements, listed below.       Note: Please update the firmware of all RB25F connected to the system to latest version 1.5.1.44 and the HID Biometric Manager to the latest version 1.0.1484.60763, as soon a possible.         CHECK FOR UPDATES       New Features:	Update	Firmware Update			
Choose How Updates Are I       Release Notes         HID Biometric Manager       Check for updates         Device Firmware       Check for updates         To fully apply this update to all reader devices an HID Update Account must be entered and validated       This new version of the RB25F firmware is bringing new features and improvements, listed below.         Update Status       Note: Please update the firmware of all RB25F connected to the system to latest version 1.5.1.44 and the HID Biometric Manager to the latest version 1.0.1484.60763, as soon a possible.         CHECK FOR UPDATES       New Features:	Updates	A New Version Is Available! rb25f_upgrade.tar.gz 1.5.1.44 is now available - you h Would you like to download and install it now? Warning : Devices will be off-line while firmware updat	ave 1.5.1.50. te is in progress.		
HID Biometric Manager Check for updates Device Firmware Check for updates Check for updates Check for updates Check for updates Update Status ✓ HID Biometric Manager is up to date Device Firmware update is now avail CHECK FOR UPDATES CHECK FOR UPDATES	Choose How Updates Are I	Release Notes			
Configurate device deliption.     ToC with bypass.	HID Biometric Manager Device Firmware Check for updates Check for updates Check for updates Check for updates CHECK FOR UPDATES	To fully apply this update to all reader devices entered and validated This new version of the RB25F firmware is bringin listed below. Note: Please update the firmware of all RB25F cc 1.5.1.44 and the HID Biometric Manager to the la possible. New Features: • Configurable device template encryption. • ToC with bypass.	s an HID Update Account must be ng new features and improvements, onnected to the system to latest version test version 1.0.1484.60763, as soon a	•	
CANCEL			CANCEL		

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

**Powering** Trusted Identities

**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.

Install Firmware			
Progress Report			
Transfering firmware to device.			
Device IP Address 169.254.3.105 Host Name R825F-00068E100236 Serial Address IP14190029W0209749 Version 1.5.1.36			
	System  Install Firmware  Progress Report  Transfering firmware to device.  Pevice PAddress 169.254.3.105 Host Name RB25F-00068E100236 Serial Address IP14190029W0209749 Version 1.5.1.36	every every system every ever	System ● HELP ▲ ADMN   Install Firmware   Progress Report     33%     'ansfering firmware to device.     Porce   P Address   PAddress   RB25F-00068E100236   Serial Address IP14190029W0209749   Version     1.5.1.36

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

#### Notes:

- 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 reader firmware 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.

HID	Live! People	Devices System			HELP	🛓 ADMIN
	Devices					
Q	Search					
	Name	MAC Address	IP Address	Version		
R	RB25F-00068E100236	00-06-8E-10-02-36	169.254.3.105	1.5.1.22		
R	RB25F-00068E100236	00-06-8E-10-02-36	169.254.3.105	1.5.1.22		

## 2.4.2 Individual device firmware update

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

The firmware files are available for download from the HBM Developer Center .

#### Install a firmware update from a local file

- 1. Click Advanced on the Devices tab.
- 2. Select Install From Local Drive.
- 3. Click **UPDATE FIRMWARE**.

Live! People Devices System	HELP	🛔 ADMIN	ABOUT
Devices > RB25F-00068E100236 (IP14190029WO209749)			
Details Communication Key Management Advanced SYNC FACTORY DEFAULT REBOOT DEVICE			
Device Security Increase security by disabling some on-device services. Services that will no longer be available: 1. Firmware Upgrade 2. Static IP Address 3. Remote Connection			
CHANGE PASSWORD REDUCE TEMPLATE SECURITY Manage Individual Device Firmware			
Use options below to reinstall device firmware or update firmware from local storage.			
These are non-standard options, navigate to the "System" tab, then "Updates" to check for new versions of firmware.			

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

Note: The firmware files are available for download from the HBM Developer Center .

5. Click **OK** when the update is complete.

#### **Reinstall firmware**

- 1. Click Advanced.
- 2. Select 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.

## 2.4.3 Force firmware update

Another option for updating the firmware can be performed through the **Device** menu. Under the **Advanced** tab, select **Update Firmware** and use the file explorer to select the correct firmware update.

## 2.4.4 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.

HID Liv	ve! People Dev	vices System			HELP	🛔 ADMIN	ABOUT
De De	evices						
Q Search							
Nan	ne	MAC Address	IP Address	Version			
RB25	5F-00068E100236 (IP14	00-06-8E-10-02-36	169.254.3.105	1.5.1.50			
					—		

3. Click the Advanced tab and click FACTORY DEFAULT.
#### **Powering** Trusted Identities

#### 4. Click CONFIRM.

HID Live! People Devices System	HELP	ADMIN 🚯 ABOUT
Devices > RB25F-00068E100236 (IP7	4190029WO209749)	•
Details Communication Key Management	Advanced	
SYNC     FACTORY DEFAULT     REBOOT DEVICE       Device Security     Increase security by disabiling some on-device services.     Fill       Services that will no longer be available:     1. Filmware Upgrade       2. Static IP Address     3. Remote Connection       CHANGE PASSWORD     REDUCE TEMPLATE SECURE	onfirm Factory Default clory Default will clear all settings, including ip address and port. e device will then be uninstalled. CANCEL CONFIRM	
Manage Individual Device Firmware Use options below to reinstall device firmware or update firmware from to These are non-standard options, navigate to the "System" tab, then "Updates" to che Install From Local Drive Instant From Local Drive C Regulares an HD update account Regulares an HD update account Please refer to HID Biometric Manager Administration Guide for setting up an HID UPDATE FIRMWARE	cal storage. . (or new versions of firmware. update account.	

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

## 2.4.5 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 [10] associated with the device you want to uninstall.

HID	Live! People De	evices System			HELP	🛔 ADMIN	<ul> <li>ABOUT</li> </ul>
	Devices						
<b>Q</b> :	Search						
	Name	MAC Address	IP Address	Version	_		
Ro	RB25F-00068E100236 (IP14.	00-06-8E-10-02-36	169.254.3.105	1.5.1.50	<b>₽</b>		

## **HID Powering** Trusted Identities

#### 3. Click CONFIRM.

HID	Live! People	Devices	System		HELP	🛓 ADMIN	ABOUT
	Devices						
<b>Q</b> 5	earch						
	Name	MAC	Address	Confirm Uninotall Degues			
	RB25F-00068E100236 i	(IP14 00-06-8	E-10-02-36	Common oninstall Request Name RB25F-00068E100236 (IP14190029W0209745 MAC Address 00-06-8E-10-02-36 IP Address 169.254.3.105 CANCEL CONFIRM	L ()		

#### 4. Click OK.

**Note:** If all devices have been uninstalled in HBM, you will have the option to install a devices on the **Devices** screen, see **2.3 Device installation and configuration**.

# 2.5 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 reinstalled.

For all network setting changes, make sure that the Signo 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.

Live! People Devices System	🛔 ADMIN 🚯	ABOUT
Network Settings		
Device connects back to HID Biometric Manager using:		
Hostname : The unit will resolve the hostname using DNS on the network	O AAHID85WM7Y2	
IP Address : The unit will connect to this IP. Either select one of your network adapters from the drop down or enter an IP address manually	<ul> <li>10.41.94.233</li> </ul>	Manual     Entry
SAVE		
Sound Host Sattings		
Host Name AAHID85WM7Y2		

3. Click SAVE.

# 2.6 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.

HID Live! People	Devices System			• HELP	🛔 ADMIN	ABOUT
Devices						
Q Search						-
Name	MAC Address	IP Address	Version	_		
RB25F-00068E100236 (I	P14 00-06-8E-10-02-36	169.254.3.105	1.5.1.50	<b>A</b>		

- 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.

HID Liv	ve! People Device	es System		HELP	🛓 ADMIN	ABOUT
De	evices > RB25F-000	68E100236 (IP141900)	29WO209749)			
Details	Communication Ke	y Management Adva	nced			
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 Cor	nnections Mode					
Mode	Wiegand	<del>&lt;</del>				
BLE Sett	tings					
BLE Mobile Ac	ccess 🗹					
Operation	lodos					
Тар						
Twist and Go						
Range and	Power Settings					
Tap Range (dE	3m) -40	*				
Twist and Go F	Range (dBm) -74	<del>&lt;</del>				
Transmit Powe	er (dBm) -4	<del>&lt;</del>				
WRITE	READ					

5. Click 🕗.

## 2.6.1 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.

Live! People Devices System	🛓 ADMIN	() ABOUT
BioTemplate Settings		
Configure Biometric Template Expiry Date Expiry Unit of Time Never		
SAVE		
Manually Delete All Templates in the Database		

- 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.

## 2.6.2 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.

HID Live! People Devices System		HELP	🛔 ADMIN	() ABOUT
General	Reports			
Update	Transaction			
Date/Time				Q
Operators	Security Settings			
HID Update Account Settings	Local Enrollment			
Network Settings	Enrollment Settings			
BioTemplate Settings	Card Write Settings			
	Delete Template From Card			
Group Settings				
Device Profiles				

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

HID	Live!	People	Devices	System	🛔 ADMIN	ABOUT
B	BioTer	nplate Set	tings			
Co	nfigure	Biometri	c Template	Expiry Date		
Expir	y Unit of Tim	e Weeks		<b>*</b>		
Expir	y Value:	2				
S	AVE					
Col	nfigure	Delete So	chedule Fo	or Expired Templates		
Sche	dule Unit of	Time Never				
Sche	dule Value	00 : 00	×			
S	AVE					
Ma	nually F	)oloto All	Tomplator	in the Database		
IVIA		Pelete All	Templates			
DI	ELETE					

## 2.6.3 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**.

HID Live! People [	Devices System				🛔 ADMIN	
People > John Sr	Enroll Finger					0
	These images are displayed	but are not stored				
John Smith Login Name 67116	Template 1	Template 2	Template 3			
	✓ Override System Temp	late Expiry Unit of Time We	eks 🗲	Value 2	DONE	
				CANCEL		

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

# 2.7 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 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 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.

#### **Powering** Trusted Identities

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

HID Live! People Devices	System	Ø HELP	ADMIN	ABOUT
Devices > RB25F-0006	3E100236 (IP14190029WO209749)			¢
Details Communication Key	Management Advanced			-
SYNC FACTORY DEFAULT Device Security Increase security by disabling some on-device of Services that will no longer be available: 1. Firmware Upgrade 2. Static IP Address 3. Remote Connection CHANGE PASSWORD REDUCE	Confirm To Reduce Template S Press confirm to downgrade the security on the device. This will allow device to work offline without having to c A device reboot will automatically take place after clicke Reboot will take approximately 60 seconds. Warning - This setting can only be undone by uninstalli and then reinstalling the device.	Security	et	
Manage Individual Device F				
Use options below to reinstall device firmware or u These are non-standard options, navigate to the "System" to	pdate firmware from local storage. ab, then "Updates" to check for new versions of firmware.			
Install From Local Drive     Reinstall Firmware     The operation may lake approximately 25 minutes.     Regime and the provident of the	suide for setting up an HID update account.			

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.

# 2.8 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.

D Live! People Devices System		ADMIN	<ol> <li>ABOUT</li> </ol>
General	Reports		
Update	Transaction		
Date/Time			
Operators	Security Settings		
HID Update Account Settings	Local Enrollment		
Network Settings	Enrollment Settings		
BioTemplate Settings	Card Write Settings		
Crown Orthings	Delete Template From Card		
Group Settings			
Device Profiles			
Enrollment			
Install USB Module			

#### 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.

# **2.9 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**.

HID Live! People D	evices System	🛓 ADMIN	<ul> <li>ABOUT</li> </ul>
BioTemplate Setting	ß		
Configure Biometric Te	emplate Expiry Date		
Expiry Unit of Time Weeks	<del>&lt;</del>		
Expiry Value: 2			
SAVE			
Configure Delete Sche	dule For Expired Templates		
Schedule Unit of Time Never	Expired templates		
Schedule Value 00 :00			
SAVE			
Manually Delete All Ter	mplates in the Database		
DELETE			

## 2.10 Key management

HBM allows you to roll MOB and Elite keys to the Signo 25B.

Note: You must have HID Origo System account, and Reader Manager authorization to access the keys.

For information on how to create a system account with Reader Manager authorization, see A.2 Create an Origo system account in HBM

## 2.10.1 Load a MOB key onto a device

To load a Mobile Access (MOB) key onto a Signo 25B device with HBM:

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

HID	Live! People De	evices System			HELP	ADMIN	ABOUT
	Devices						
Q s	earch						
	Name	MAC Address	IP Address	Version	_		
Ro	RB25F-00068E100236 (IP14.	00-06-8E-10-02-36	169.254.3.105	1.5.1.50	<b>1</b>		

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.

Live! People Devices System	🛔 ADMIN	ABOUT
Devices > RB25F-00068E100236 (IP14190029WO209749)		6
Details Communication Key Management Advanced		
Configure Mobile Identity Key		
Set keys specific to your device or organization.		
Mobile Key on Device Select Read CLEAR		
Mobile Key to Write to Device 🗧 WRITE		
Load Elite Key		
Application for on General the Reys.		
Elite Key to Write to Device 🗧 WRITE		

- 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  $\bigcirc$  to finish after the successful pop-up window has disappeared.

HID Live! People De	evices System	🛛 🛔 ADMIN
Devices > RB25F-	00068E1001FB	
Details Communication	Advanced	
SYNC FACTORY DEFAULT	REBOOT DEVICE UPDATE FIRMWARE	
bevice security	nice services	
Services that will no longer be available: 1. Firmware Upgrade 2. Static IP Address 3. Remote connection	Successi	
CHANGE PASSWORD REL	Mobile key has been successfully configured. Please wall for 60 seconds while device reboots.	
Configure Mobile Identity	y Key	
Set keys specific to your device or organiz	zafon.	
Retrieve Configured Mobile Identity Key	GET	
Mobile Key	MOBA233 CLEAR	

## 2.10.2 Load HID Elite keys

This feature allows HID Reader Technician to push HID Elite<sup>™</sup> keys to the customer via the web. SEOS<sup>®</sup> and MIFARE<sup>®</sup> DESFire<sup>®</sup> EV1/EV3 SIO credentials are supported 1 by the HID Elite keys on this device.

#### Notes:

- Standard keys will not work on the Signo 25B once Elite keys have been loaded to the device.
- After a factory reset, the device cannot be checked for standard or Elite key configurations.
- You need to be fully enrolled in HID Elite with an ICE Key reference for Signo 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.

Live! People Devices System	🛔 ADMIN	ABOUT
Devices > RB25F-00068E100236 (IP14190029WO209749)		G
Details Communication Key Management Advanced		
Configure Mobile Identity Key Set keys specific to your device or organization.		
Mobile Key on Device Select Read CLEAR		
Mobile Key to Write to Device 🗲 WRITE		
Load Elite Key Applicable for 8k Seos Ice Keys.		
Elite Key to Write to Device 🗲 WRITE		

<sup>1.</sup> Only available with Signo 25B ordered from the factory after June 2022 with firmware version 1.5.1.56. (NOT available with RB25 or previous Signo 25B devices).



#### 4. Select a key set to load.

HID Live! People Devices System	A ADMIN
Devices > RB25F-000 Elite Keys	0
Details Communication Ar	Č
Set keys specific to your device or organization Mobile Key on Device Select Read	
Mobile Key to Write to Device	
Applicable for DL Seos Ice Keys. Elite Key to Vinite to Device	
CANCEL	

5. With the key set selected, click Write.

# 2.11 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.

HID Live! People Devices System		😧 HELP	·	ADMIN	ABOUT
General	Reports	- 1			
Update Date/Time	Transaction				
Operators	Security Settings	- 1			
HID Update Account Settings	Local Enrollment	- 1			
Network Settings	Enrollment Settings	- 1			
BioTemplate Settings	Card Write Settings	- 1			
	Delete Template From Card	i i			
Group Settings		- 1			
Device Profiles		- 1			
Enrollment		- 1			
		- 1			
Install OSD Module		- 1			
		- 1			
		-			

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

HID Live! People Devices System	HELP	🛔 ADMIN	ABOUT
Update			
Updates			
Choose How Updates Are Installed			
HID Biometric Manager Check for updates			
Device Firmware Check for updates			
<ul> <li>Update Status</li> <li>→ HID Biometric Manager is up to date. (Last checked: 2021-07-27 17:17:12)</li> <li>→ Device Firmware update is now available. (Last checked: 2021-07-27 17:17:15)</li> <li>CHECK FOR UPDATES</li> </ul>			

#### 4. Click System.

5. Select the required update option and click APPLY.

HID Live! People Devic	es System		🛔 ADMIN	
Update	Software Updates	_		
Updates Choose How Updates Are In HID Biometric Manager Check for updates	Choose How Updates Are Installed Over the check for updates Do not check for updates. Not recommended. Over updates are available. Over updates are available.	oad or install. The system will notify you		
Device Firmware Check for updates Update Status HID Biometric Manager is up to date. Device Firmware update is now availa CHECK FOR UPDATES				
		CANCEL APPL*		

6. Click **CHECK FOR UPDATES** to check if software/firmware updates are available. **Update Status** information is displayed on the screen.

- If new HBM software is available and selected, the installation progress is displayed in your browser. Once the installation is complete, the HBM Server application will automatically shut down and re-start. You will be prompted to log back into the HBM.
- If new device firmware is available, see 2.4.1 Device firmware update.

HID Live! F	People Devices System	HELP	🛔 admin	ABOUT
Update				
Updates				
Choose How U	Ipdates Are Installed			
HID Biometric Manager	Check for updates			
Device Firmware	Check for updates			
Update Status <ul> <li>HID Biometric Mat</li> <li>Device Firmware to CHECK FOR UPD/</li> </ul>	nager is up to date. (Last checked: 2021-07-27 17:17:12) ipdate is now available. (Last checked: 2021-07-27 17:17:15) TES			

## **HID** Powering Trusted Identities

# 2.12 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. HBM comes with a default device profile named **Devices** and installed devices are automatically placed in this default device profile.

## 2.12.1 Create a device profile

To create a new device profile:

1. Click System and select the Device Profiles option.

HID Live! People Devices System		🛔 ADMIN	ABOUT
General	Reports		
Update	Transaction		
Date/Time			
Uperators	Security Settings		
HID Opdate Account Settings	Local Enrollment		
RioTemplate Settings	Enrollment Settings		
Dio rempiate octango	Card write Settings		
Group Settings Device Profiles Enrollment Install USB Module			



2. Click 😳 to add a new device profile.

HID Live! People De	evices System		HELP	🛓 ADMIN	ABOUT
Device Profiles					+
Q Search					New
Name	Description	Devices			
Device		1			

- 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 2.12.2 Edit a device profile.

HID Live! People	Devices System		HELP	🚨 ADMIN	ABOUT
Device Profiles					•
Q Search					-
Name	Description	Devices			
Device		1			
Lobby Entrance		0			

# 2.12.2 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 [

HID Live! People	Devices System		HELP	🛔 ADMIN	ABOUT
Device Profiles					
Q Search					
Name	Description	Devices			
Device		1			
Lobby Entrance		0	<b>*</b>		

- 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.

HID Live! People Devices Syst	em				🛔 ADMIN	
Device Profiles > Lobby Entranc	9					
Details Audio/Visual Authentication	Biometri	c Settings				
Details       Audio/Visual       Authentication         Event       Idle       Idle	Audio/Visu Color Flashing Beep Duration (s)	al On Beep Twice 0.8	¢ ¢	SAVE		

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**.

Notes:

- Click CREATE SCHEDULE to create a new authentication schedule.
- 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.



HID Live! Peop	le Devid	es System			🛔 ADMIN	
Device Profile	es > Lobi	Authentication Sch	nedules			
Details Audio/Visu	al Auth	Select Schedule				
Q Search		Name	Dates			
Mode	Days	Default Schedule				
Card + Finger	None	Lobby Entrance	2021/07/27 - 2021/07/30			
		CREATE SCHEDULE		CANCEL NEXT		

- 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.

HID Live! People	Devices System			HELP	🛓 ADMIN	ABOUT
Device Profiles >	Lobby Entrance					
Details Audio/Visual	Authentication	Devices	Advanced			
Q Search						
Name I	P Address	Version				
RB25F-00068E100236 (IP14 1	69.254.3.105	1.5.1.50				

- 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	I HELP	🛔 ADMIN	ABOUT
Device Profiles > Lobby Entrance			
Details Audio/Visual Authentication Devices Advanced Enabled Card Types			ĊĊ
IClass Z Enforce Sees PACS Z			
Security Level Low 🗲			
Rescan Delay (ms) 2000			
Live Finger Detection Identify Erroll 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			

## 2.12.3 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 [iii] associated with the device profile.

HID Live! People	Devices System		HELP	🛔 ADMIN	ABOUT
Device Profiles					
Q Search					-
Name	Description	Devices			
Device		0			
Lobby Entrance		0			
Lobby Entrance		1	ø 💼		

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

HID Live! People Device	es System	0	HELP	ABOUT
Device Profiles				•
Q Search				
Name	Description	Devices		
Device		0	-	
Lobby Entrance	Delete recor	d 'Lobby Entrance'		
Lobby Entrance	Are you sure you	want to permanently delete this record?		
		CANCEL CONFIRM		

# **2.13 Device health indication**

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

lcon	Status	Definition
Ro	High level communications in place and device ready.	The device is ready to be used and there are no issues.
Ro	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.
Ro	No communications with device.	Communication has been lost between the device and HBM. The device has lost power or a tamper event has taken place.
R	High level communications in place but device is busy.	Communication between the connected devices and HBM is stable but the device is experiencing a high level of usage.

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

ню	Live! People	Devices System			HELP	ADMIN	ABOUT
	Devices						
٩	Search						-
R	Name RB25F-00068E100236 (IP	MAC Address	IP Address 169.254.3.105	<b>Version</b> 1.5.1.50			

# 2.14 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**.

Settings Control	Read	Write	HID	Powering Trusted Identities		
Misc	-	Network				-
Date - Time Uptime Serial Number FW Version	27 Mar 2020 - 12:29:19 00:09:13 IP14190019WO209705 1.5.1.11	DHCP Hostname	1	✔ Signo 25	58	
Digital Inputs						-
Wiegand Green Led Wiegand Red Led Wiegand Buzzer Wiegand Hld Anti Tamper Wiegand Tamper Factory Default		LOW LOW LOW LOW LOW LOW				

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

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

## **Powering** Trusted Identities

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 RB25F. It is exclusive to the Signo 25B only.

Settings Control		Powering Trusted Identities
Outputs		-
	Select relay - Relay 1 Activate Relay	

**Note:** The internal relay will toggle for five seconds.

# 2.15 Tamper settings

The Signo 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 HBM 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 🕑 .

HID Live! People	Devices System	HELP	🛓 ADMIN	ABOUT
Device Profiles >	Lobby Entrance			
Details Audio/Visual	Authentication Devices Advanced			
Enabled Card Types				Â
Seos 2 Mifare 2 Iclass 2 Enforce Seos PACS 3 Fingerprint Sensor Security Level Low Rescan Delay (me) 2000	*			
Live Finger Detection Identify Enroll Verify				
Presentation Timeout				
Template on Card (ms) 10000				
SE BIO Settings Biodiversifier				
Tamper Settings				

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 HBM, the Device must be uninstalled from HBM and then re-installed.

# 2.16 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.

HID Live! People Devices System	HELP	🛔 ADMIN	ABOUT
Device Profiles > Device			9
Details Audio/Visual Authentication Devices Advanced			
Seos       ✓         Mifare       ✓         iClass       ✓         Enforce Seos PACS       ✓         Fingerprint Sensor       ✓         Security Level       Low       ✓         Rescan Delay (ms)       2000       ✓			
Live Finger Detection Identify Enroll Verify			
Template on Card (ms) 10000			

#### 2. Click 💙.

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

## 2.17 System monitoring and Reports

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

## 2.17.1 View HID Biometric Manager events

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

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

HID Live! Peo	ople Devices Syste	em	<b>0</b> H	IELP	🛔 ADMIN	ABOUT
Transaction	15					
Details Filters						
Biometric Match 1:N Failed	RFID Credential	Read	RFID Credential Read			
Unknow	vn User	John Smith	John Smith			
BB25E		BB25E-	BB25E-			
0006	9WO209749)	00069WO209749)	00069WO20	9749)		
19:30:3	9	19:30:39	19:30:31			
2021-0	1-21	2021-01-21	2021-07-27			
Date/Time	Event	Device		Name		Card
2021-07-27 19:30:39	Biometric Match 1:N Failed	RB25F-00068E100236	(IP14190029WO209749)			FFFFF
2021-07-27 19:30:39	RFID Credential Read	RB25F-00068E100236	(IP14190029WO209749)	John Smith		92506F0CFFFF12E0
2021-07-27 19:30:31	RFID Credential Read	RB25F-00068E100236	(IP14190029WO209749)	John Smith		92506F0CFFFF12E0
2021-07-27 19:30:31	Biometric Match 1:N Failed	RB25E-00068E100236	(IP14190029WO209749)			FFFFF
2021-07-27 19:30:24	RFID Credential Read	RB25F-00068E100236	(IP14190029WO209749)	John Smith		2506F0CFFFF12E0
2021-07-27 19:30:20	Biometric Match 1:N Failed	RB25F-00068E100236	(IP14190029WO209749)			FFFFF
2021-07-27 19:30:20	RFID Credential Read	RB25F-00068E100236	(IP14190029WO209749)	John Smith		92506F0CFFFF12E0

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 **O** 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.

## 2.17.2 Transaction Reports

To create a report of HID Biometric Manager transactions:

1. Click System and select Transaction option.

HID Live! People Devices System		🛔 ADMIN	<ul> <li>ABOUT</li> </ul>
<b>General</b> Update Date/Time Operators HID Update Account Settings Network Settings BioTemplate Settings	Reports         Transaction         Security Settings         Local Enrollment         Enrollment Settings         Card Write Settings         Delete Template From Card		
Group Settings Device Profiles Enrollment Install USB Module			

2. Click **RUN REPORT** to create a report of HBM transactions. Once the report is created click the save report icon [4] to save the report to a PDF or CSV file.

HID Live! People	Devices System			🛔 ADMIN	<ul> <li>ABOUT</li> </ul>
Transaction					
Details Filters					
Date/Time	Event	Device	Name	Card	
		Table is Empty No results were returned RUN REPORT			

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 **O** 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.

HID Live! People	Devices System		<ul> <li>ABOUT</li> </ul>
Transaction			
Details Filters			
Filters In Use			
🗙 Name	John Smith	<b>+</b>	
ADD FILTER			

## 2.18 System Diagnostics

Allows you to package HBM logs in a zip file for transfer to HID technical support for help with troubleshooting.

Note: Only users with administrator access can create a diagnostic bundle.

1. Click ADMIN and then click Diagnostics Bundle.

HID	Live! People De	evices System		Ø HELP	
	Devices				Administrator Edit Profile   Sign Out
<b>Q</b> s	earch				Diagnostics Bundle
	Name	MAC Address	IP Address		
R	RB25F-00068E100236 (IP14	00-06-8E-10-02-36	169.254.3.105		

- 2. Select a diagnostics bundle level:
  - Full Diagnostics Bundle.
  - Minimum Diagnostics Bundle.

Note: Each level states what is included in the bundle.

- 3. Click **GENERATE**.
- 4. If successful, you will see a success message, and the file location of the diagnostics bundle.



# Section 03 Enrollment




# **3.1 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:** Please make sure that the enrollment reader and all connected readers are at the same firmware level for template compatibility.

# 3.1.1 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.

HID	Live!	People	Devices	System		HELP	🛔 ADMIN	ABOUT
1	People	)						•
•	Q Search							
					le enrolled.			

4. Enter the persons details (First Name/Last Name).

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 💙.

HID Live! People Devi	ces System	Ø HELP	🛔 ADMIN	ABOUT
People				
	Details			
	First Name John			
	Last Name Smith			
	ID 984030			
🚨 Login Name				
984030 ID				

7. The enrolled person record is displayed on the **People** screen. To add additional people, click <sup>•</sup> 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.

HID	Live!	People	Devices	System			HELP	ADMIN	<ul> <li>ABOUT</li> </ul>
1	People								•
◄	Q Search								-
	Name		ID	Sta	tus				
J	John Smith		984030	Activ	e	e 🖉			

## 3.1.2 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. Click **READ CARD** on the **Details** screen. If more than one reader is installed, select a device from the displayed list.
- 2. Within five seconds, present a card to the Signo 25B device.

Note: The card types supported by the device is configured in the device profile settings, see 2.12.2 Edit a device profile.

HID Live! People Devices System	HELP	ADMIN	ABOUT
People > John Smith > Cards			G
Details			
Format 🗲			
READ CARD         WRITE TO CARD         Scanning         Jace card on device			

# 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.

Entry Live! People Devices System	HELP	ADMIN	ABOUT
People > John Smith > Cards			
Details			
Credential Identifier 92506F0CFFFF12E0			
READ CARD WRITE TO CARD			

The operator can now collect and add biometric data associated with this enrolled person, see 3.2.2 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.

HID Live! People Devices System	HELP	🛔 ADMIN	<ol> <li>ABOUT</li> </ol>
People > John Smith > Cards			G
Details			
Format 🗲			
READ CARD WRITE TO CARD			

#### 2. Select the required Credential Format.

HID Live! People Devic	es System		🛔 ADMIN	
People > John Smith	Select			6
Details	Q Search			
	Name			
Format	H10301 26 Bit Raw			
	H10302 37 Bit Raw			
READ CARD WRITE TO CARD	H10304 37 Bit Raw			
		CANCE		

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

4. Click

HID Live!	People Device	es System	HELP	🛔 ADMIN	ABOUT
Peop	e > John Smith >	<ul> <li>Cards</li> </ul>			
Details					
Format	H10301 26 Bit Raw	+			
Credential Number	12345				
Facility Code	1				
READ CARD	WRITE TO CARD				

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

HID Live! People Devices System	HELP	🔒 ADMIN	<ul> <li>ABOUT</li> </ul>
People > John Smith > Cards (02026073)			
Details			
Credential Identifier 02026073			
Format H10301 26 Bit Raw			
Credential Number 12345			
Facility Code 1			
READ CARD WRITE TO CARD			

# 3.2 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 3.2.2 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 25B fingerprint reader connected.

## 3.2.1 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.

Notes:

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

HID H	D Biometric Man	ager Server		
🖵 Live!	🛔 Clients	a Security	OS Tools	
Web Server         Configure security settin         Enable HTTP         Enable HTTPS         Use certificate from         Device Communicatio         Allow Non-Secure C         Enable         Save	Igs applicable to the web server HTTP Port HTTPS Port key store webserver ns iommunications	82 443		
Open Client Connection : h	ittp://AAHID85WM7Y2:82			₩ 20



- 3. Tick the Enable HTTPS check box.
- 4. Select the Key Store tab.
- 5. Click webserver.

HID HI	D Biometric Ma	nager Server		
🖵 Live!	🛔 Clients	a Security	😋 Tools	
rtificates: bserver trificateauthority	Levine Construction of the	HID85WM7Y2 thm: SH4512wthRSA, OID = 1.2.8 vublic key, 1024 bits: 79425514170710340243939549602 t 05537 Mon Nov: 09 151027 GMT 2020, 0 ct 28 151027 GMT 2070] D55VM772 49054actb be655a52] ons: 3 2937 Criticality=false ges [	40 113549 1.1.13 293656678674366739009682077314567	Actions: 70160781824222027255786 Actions: A

- 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.



## **3.2.2 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 25B.

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

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

**Note:** HBM will use the SIGNO-B-USB reader by default. To use the Signo 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 25B devices.

Notes:

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

HID Live! People Devi	ces System	HELP	🛓 ADMIN	<ul> <li>ABOUT</li> </ul>
People > John Smith				
2	Details Cards Biometrics Q Search ENROLL	I		
Login Nation 984030	Table is Empty No results were returned. Check your content and filters			

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.



HID	Live!	People	Devices	System			🛔 ADMIN	
1	People	e > John	<sup>S</sup> Enrol	l Finger				00
John Seaton Seaton Seaton	S.Smith Name 130		Select	fingers to enroll.	Right	CANCEL	Empty Enrolled Selected	

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 2.3.3 Configure device settings.

HID Live! People	Devices System	HELP	ADMIN
People > Joe Bi	995		00
Arr Roger Boots	Encode Biometric         Image: Search       Search         Imag		

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.

Powering Trusted Identities

**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.

HID Live! People	Devices System			D 🛔 ADMIN	
People > John S	Enroll Finger	_	_		
	Enroll left index finger These images are displayed but a	re not stored			
John Smith Lagin Name 98030	Template 1 Template 2	xpiry Unit of Time Never	Template 3	0	

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.

Powering

Trusted Identities

HID Live! People	Devices System		
People > John S	Enroll Finger		
John Smith Logen Name 980 10	These images are displayed but are not stored Template 1 Template 1 Template 2 Template 2 Template 2 Template 2 Place finger on sensor	Template 3	
	Override System Template Expiry Unit	of Time <u>Never</u> Value 0	NEXT

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.

## 3.2.3 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.

#### Notes:

- 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.
- 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.

HID Live! People Devices	System	🛔 AD	
Local Enrollment Enr	oll Finger		
Local Enrollment allows you to write temp Any templates captured under Local Enro Enroll templates ENROLL BIOMETRICS Write enrolled templates to car WRITE TO CARD	Left Right	Empty Enrolled Selected	estore.
		CANCEL NEXT	



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

HID Live! People De	evices System			🛔 Admin	
Local Enrollment	Enroll Finger Enroll left index fi These images are displayed	<b>nger</b> d but are not stored			
Local Enrollment allows you to write temp Any templates captured under Local Enro Enroll templates ENROLL BIOMETRICS Write enrolled templates to car WRITE TO CARD	Template 1	Template 2	Template 3	stor	8.
				CANCEL DONE	

- 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.

HID	Live!	People	Devices	System		ADMIN	ABOUT		
1	Local I	Enrollmen	t						
Local En Any temp	Local Enrollment allows you to write templates to a card for users that are not enrolled in the system. Any templates captured under Local Enrollment are saved on the selected card ONLY.Templates do not get saved to the database, thus are not available for backup and restore.								
ENRO	DLL BIOMI	ETRICS	card		Write To Card Click Start once you ready to present your card to the device				
WRIT	E TO CAF	D	caru		CANCEL START				

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 25B reader and will not be added to the database.

# **3.3 Preventing user fingerprint display during enrollment**

During fingerprint enrollment the User Interface (UI) displays the fingerprint being enrolled. To prevent the fingerprint 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.

HID	Live!	People	Devices	System	🛔 ADMIN	ABOUT		
?	Enrollr	ment Setti	ngs					
Cor Enabl Displa	Configure Finger Print Display Settings Enable or Disable the setting below to toggle between displaying of fingerprint images and a tick symbol when enroling a user. Display Fingerprints							
Cor Enabl	e or Disable	USB Enrollmer	oliment Se	ttings#				
Enab	VE	ollment 🗆						

- 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.

Enroll Finger								
Enroll left middle fir These images are displayed b	Enroll left middle finger These images are displayed but are not stored							
Template 1	Template 2 Template 3		V					
Override System Template Expiry Unit of Time Never Value 0 CANCEL DONE								

4. Click DONE.

## **3.3.1 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.

#### Notes:

- Template on Card supports SEOS<sup>®</sup> and MIFARE<sup>®</sup> DESFire<sup>®</sup> EV1/EV3 SIO credentials. 1
- There is no support for template on card with custom DESFire credentials or credentials with custom keys.
- 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.

Live! People Devices System	HELP	🔒 ADMIN	() ABOUT
People > John Smith > Cards (92506F0CFFFF12E0)			
Details			
Credential Identifier 92506F0CFFFF12E0			
READ CARD WRITE TO CARD			

<sup>1.</sup> Only available with Signo 25B ordered from the factory with SP2.5 (NOT available with RB25F).

#### **HID Powering** Trusted Identities

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

HID Live! People	Devices System			
People > John S	Write To Card Select fingers to write. A maximum of two fingers can be written to the	card.		•
Credential Identifier 92506F0CFFFF	Left	Right	Empty Enrolled Selected	
		CANCEL	WRITE TO CARD	

5. You will have approximately five seconds to present the supported card to the Signo 25B device 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.

HID Live! People Devices	System		HELP	📥 ADMIN
People > Joe Bloggs > Cards (687)	37251781)			00
Details				
Credential Identifier 68737251781				
READ CARD WRITE TO CARD	[		7	
	E	Card has been written.		
	l			

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 25B.

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



# **3.4 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.

HID	Live!	People	Devices	System			🛔 ADMIN	8	ABOUT
	Card V	Vrite Settii	ngs						
Bypas Save	Enable	er TOC S Bypass Finger	<b>ettings</b> TOC Feature						

## 3.4.1 Enrollment without fingerprints

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

- 1. Select the 3.4 Bypass finger TOC.
- 2. Click People and select the required user.
- 3. Click **Cards** and select the required card.
- 4. Deselect TOC Bypass.

HID Live! People Devices System	HELP	🛔 ADMIN	3 ABOUT
People > User > Cards (000002A6)			
Details			
Credential Identifier 000002A6			
Format H10301 26 Bit Raw			
Credential Number 339			
READ CARD WRITE TO CARD			

- 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.

#### Notes:

- If the **TOC Bypass** is selected, an alert message will appear stating that no templates have been enrolled when **WRITE TO CARD** is selected.
- If the **3.4 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.

## 3.4.2 Enrollment with fingerprints

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

- 1. Select the 3.4 Bypass finger TOC.
- 2. Click People and select the required user.
- 3. Click **Cards** and select the required card.
- 4. Select TOC Bypass.

HID Live! People Devices System	HELP	ABOUT
People > User > Cards (000002A6)		
Details		
Credential Identifier 000002A6		
Format H10301 26 Bit Raw		
Credential Number 339		
Facility Code 0		
READ CARD WRITE TO CARD		

- 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.

# 3.5 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.

## **3.5.1 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**.

HID Live! People Devices System	HELP	🛔 ADMIN	<ul> <li>ABOUT</li> </ul>
Device Profiles > Device			
Details Audio/Visual Authentication Devices Advanced			
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			

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

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

HID Live! People Devices	System	HELP	🛔 ADMIN	ABOUT
Device Profiles > Device				
Details Audio/Visual Authent Rescan Delay (ms) 2000	ication Devices Advanced			
Live Finger Detection Identify  Final  Final  Verify  Verify	Authentication Mode Change This action will remove the possibility to use the Authentication mod only and Card or finger for this device profile. It will also delete all present for this device profile. To continue please click Confirm	les: Card + finger, Finger schedules with those modes		
Presentation Timeout Template on Card (ms) 10000	(	CANCEL CONFIRM		
SE Bio Settings Biodiversifier 0				
Tamper Settings Factory Default				
Template Location Automatic Download Of Template On Device				

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.

# Section 04 HID Biometric Server Application



# 4.1 Resetting administration password

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

				 0 0 <u> </u>
	Biometric Mar	nager Server		
Live!	🛔 Clients	â Security	OC Tools	
Key Store Communication	ns Account			
Admin Account: Reset the admin password Password Confirm Password	rd			
Open Client Connection : http	o://AAHID85WM7Y2:82			₩ 20

This method can be used to change the administrator password, as shown in 2.2.2 HID Biometric Manager initial login

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

## 4.1.1 Data import

The HBM Data Import component allows credential and credential holder information to be imported into the HBM database from a third party PACS headend. This ensures that the output of the Signo 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.

HID HI	D Biometric Ma	anager Server			
🖵 Live!	🛔 Clients	a Security	Q <sup>o</sup> Tools		
Import People Privacy	Settings				
Card Type :				H10302 37 Bit Raw	~ ^
			Destination		
"Firstname"			<lqnore col<="" source="" td=""><td>lumn&gt;</td><td>~</td></lqnore>	lumn>	~
"Lastname" "IDNumber"			<li>Ignore Source Coll Active</li>	umn>	
			First Name		
			ID Last Name		
			Login Name Raw PACS Data		
en Client Connection : h	ttp://AAHID85WM7Y2:82				

# 4.1.2 HID Biometric Manager Server application icons

lcon	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



# 4.2 Live!

The **Live!** server application displays a live feed of updates and events happening in HBM. It is also available in the HBM explorer window.

HID HIC	) Biometric Manager S	erver			
🖵 Live!	🛔 Clients 🛛 🗂 Se	curity 🕫 Tools			
Date/Time	Event	Device	Name	Card	
022-08-11 13:25:04	Biometric Match 1:N Succeeded	25B-00068E102B39 (IP44210053W	Predeshni Moodley	0000DE1A	^
022-08-11 13:24:58	Biometric Match 1:N Succeeded	25B-00068E102B39 (IP44210053W	Tubby Moodley	0001E05E	
022-08-11 13:24:53	Biometric Match 1:N Succeeded	25B-00068E102B39 (IP44210053W	Predeshni Moodley	0000DE1A	
022-08-11 13:24:43	Biometric Match 1:N Succeeded	25B-00068E102B39 (IP44210053W	Tubby Moodley	0001E05E	
022-08-11 13:24:38	Biometric Match 1:N Succeeded	25B-00068E102B39 (IP44210053W	Predeshni Moodley	0000DE1A	
022-08-11 13:23:24	Configuration Updated	25B-00068E102B39 (IP44210053W			
022-08-11 13:23:24	Configuration Updated	25B-00068E102B39 (IP44210053W			
022-08-03 10:00:25	Tables Initialised	258-00068E102B39 (IP44210053W			
022-08-03 10:00:28	Unit Power Up	258-00068E102B39 (IP44210053W			
022-08-03 10:01:14	Configuration Updated	25B-00068E102B39 (IP44210053W			
022-08-03 10:08:18	Unit Power Up	258-00068E102B39 (IP44210053W			
022-08-03 10:08:30	Configuration Updated	25B-00068E102B39 (IP44210053W			
022-08-03 10:09:17	Unit Power Up	25B-00068E102B39 (IP44210053W			
022-08-03 10:09:23	Configuration Updated	25B-00068E102B39 (IP44210053W			
022-08-10 09:23:07	Unit Power Up	25B-00068E102B39 (IP44210053W			
N22-NR-10 N9-23-13	Configuration Updated	258-00068E102839 (IP44210053W			~
2022-08-10 09-23-13 Open Client Connection : htt	Configuration Undated	258-000685102839/IID44210053W			<b>A</b> 3

# 4.3 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 **4.1.1 Data import**. It also stores configuration data and transaction logs for all installed Signo 25B devices.

HBM uses a local database as the default database during installation. HBM allows you to use your own SQL database, running on the same, or a different server.

Note: You must have Microsoft SQL Server Management Studio or similar installed on your computer.

For a new install, copy the files from the **Empty** folder to the computer running the SQL server (This does not have to be the same computer running HBM).

With HBM running, right click the system tray icon and click database. From there you can select SQL server and fill in each field. Click Test Database Connection. If the test passes click **Save & Restart**.



# 4.4 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-enroll the users.

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

Note: The backup and recovery feature is only available with software version 1.0.2000.00015 or higher.

## 4.4.1 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 beginning 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.

	) Biometric Mai	nager Server			00_0×
Live!	Clients	a Security	🛱 Tools		
Key Store Communicatio	Account	HID8SWM7Y2 htm: SH4512avithRSA, OID = 1.2.1 32337549774289906334072393a 65537 us Jul 20 095145 B5T 2021, 3 Jul 20 095145 B5T 2021, 3 Jul 20 095145 B5T 2071] D8SWM7Y2 98704c78 3705826d] ons: 3 937 cmicality=false tes [	840.113549.1.1.13 46908815701604725791274936492678241	Actions:	Refresh port Certificate port Certificate move Certificate rate Certificate rate Recovery Key
Open Client Connection : http	p://AAHID85WM7Y2:82				≒≣≜

- 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.

## 4.4.2 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.



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.

🔚 🗇 ENG

• Backup daily or weekly.

HID

📕 🚛 🕼 ENG

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.

## 4.4.3 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 HBM 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 HBM Server application.

- 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.

HID HIC	) Biometric Ma	nager Server		
🖵 Live!	Clients	a Security	O <sub>0</sub> <sup>0</sup> Tools	
Certificates: webserver certificateauthonity	Details: [ [ Subject CN=A4 Signature Agent Key: Sun RSA p modulus 1125 public exponen Validity (From: Ten We Issuer: CN=A4H Selectionstants [1] Objectit 2:5 BacConstants CAtrue PathLen:10 ] <<	HID85WM7Y2 time SHA512MinRSA, OID = 1.2 ublic key, 1024 bits 9456066751615958629200439563 tes Jul 20 095144 BST 2021, 4 Jul 20 095144 BST 2021, d Jul 20 095144 BST 2021, d Jul 20 095144 BST 2021, DB55WM7Y2 - 05160202 0544 BST 2021, 00515 2021	2 840 113549 1.1 13 3132658582085 1605149586634765466339	Actions: 398722410692144957178475378 398722410692144957178475378
pen Client Connection : htt	tp://AAHID85WM7Y2:82			۵.

- 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.

Note: Return to 4.4.1 Generate recovery key after completing the above steps.

# Section 05 Network



# 5.1 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 25B devices, it defaults to hostname Signo 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 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 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 25B.

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

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

Signo 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 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 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.

# 5.2 Network usage

Protocol	Port	Source	Destination	Direction	Comment
ICMP		Server	Device	Outgoing	Only ICMP ping Type 0 is supported.
ТСР	82	Client	Server	Outgoing	Client Server Outgoing HTTP from browser client to server.
ТСР	443	Client	Server	Outgoing	Client Server Outgoing HTTPS from browser client to server.
ТСР	443	Server	Internet	Outgoing	Connection to Azure. <u>https://hidbiomanager.azurewebsites.net/</u> Used for FW update.

This table shows the HID Biometric Manager network usage.

Protocol	Port	Source	Destination	Direction	Comment
ТСР	443	Server	Internet	Outgoing	<ul> <li>RCAM<sup>1</sup> connection to Origo.</li> <li><u>https://prod-rfp.firebaseio.com/</u></li> <li><u>https://prod-readermanager.hidglobal.com/</u></li> <li>Used to roll to Elite and for FW update.</li> </ul>
ТСР	1819	Server	Server	-	RCAM to HBM. This all happens on the same physical computer.
ТСР	3000	Server	Device	Outgoing	One time use (per device) for install. Server needs to tell device about MQTT settings to talk to it.
ТСР	8883	Device	Server	Outgoing	MQTT
UDP	10500	Server	Device	Outgoing/Incoming	Device Discovery and Device Network Settings.

# **5.3 Device discovery**

The Signo 25B and the HBM server application must be installed on the same network for the device to be discoverable and installed, to be managed by HBM. The Signo 25B device ships with DHCP mode ad the default for network communication, so the device installed on a network will have its IP assigned by the DHCP server. A network administrator can setup the Signo 25B with static IP. In both cases, the device needs to be discoverable from the host (server).

# 5.4 Secure device communication

The HID Biometric Manager software is server based software paired with the RB25F and Signo 25B, accessed through a WebUI client. The HBM server and the fingerprint device communicate through mutually authenticated MQTT. This creates an end to end chain of trust between the server and the device, without this mutual trust the device and server cannot communicate.

# 5.5 Chain of trust

Trust is established during installation of the device. The server has a CA certificate and a unique certificate is generated the first time the server software is started. During device installation, the device presents its certificate to the software instance on the server, is done during device installation (referred to as the server in this note). The certificate is signed by the Certificate Authority and returned to the device so a trusted communication is established between the device and that server instance, meaning the device and server will only trust devices signed using its CA certificate.

Note: The CA certificate is specific to the host that generated the certificate.

The certificate SAN fields show the IP/DNS name that is expected. Contact HID technical support to reset the software to initial state. If the device is removed and connected to a different instance of the server, communication will be lost. In this case, reset the Signo 25B to the factory default settings, and install to the new server.

<sup>&</sup>lt;sup>1.</sup> Reader Configuration and Management (RCAM)

# Appendix A HID Origo set up



#### **Powering** Trusted Identities

This section provides details on the prerequisites that must be in place in order to setup a connection between HID Biometric Manager<sup>™</sup> and the HID Origo<sup>®</sup> Portal. The section also details how to verify HID Reader Manager<sup>™</sup> 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 HBM and HID Reader Manager for updates and to facilitate loading MOB keys onto the Signo 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 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.

People Devices System			🛓 ADMIN	ABOUT				
HID Update Account Settings								
ite Account								
t								
HIDDemoAccount@hidglobal.com								
Fri Jul 23 12:23:19 BST 2021								
NT start Here								
d with account								
	People     Devices     System       date Account Settings       t       HIDDemoAccount@hidglobal.com       Fri Jul 23 12:23:19 BST 2021       vr       Int?       Start Here       d with account	People     Devices     System   date Account Settings       t     HIDDemoAccount@hidglobal.com       Fri Jul 23 12:23:19 BST 2021   If Start Here d with account	People     Devices     System   date Account       t     HIDDemoAccount@hidglobal.com   Fri Jul 23 12:23:19 BST 2021       T   Month account	People Devices System     date Account     te     HDDemoAccount(Bhidglobal.com     Fit Jul 23 12 23 19 BST 2021      To make the second the sec				

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

		11790	
Re	egister admin user		
Email address *			
Business Email Address			
First name *	Last name *		
First name	Lastname		
Phone Number *			
<b>1</b> ••••			
		хт	
	00		
x / x / x / x / x / x / x / x / x / x /			

### A.3 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.

HID Live! People Devices System	1	🛔 ADMIN 🚯 ABOUT
General Update	Reports Transaction	
Operators HID Update Account Settings Network Settings BioTemplate Settings Group Settings Device Profiles	Security Settings Local Enrollment Enrollment Settings Card Write Settings Delete Template From Card	
Enrollment Install USB Module		

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

HID	Live!	People	Devices	System	🛔 ADMIN	ABOUT
CT.	HID Up	odate Acc	ount Setting	S		
Verify H	HID Upd	ate Accou	int			
System	Accou	nt				
User acco	unt					
Password						
Last verifie	ed on					
VERIF	Y ACCOU	INT				
New HID u	update acco	ount? <u>Start F</u>	tere			
Keys as	ssociate	d with ac	count			

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.

HID Live! Pe	ople Devices Sy	system				🛔 ADMIN	ABOUT		
HID Update	HID Update Account Settings								
Verify HID Update	Account								
System Account									
User account	eurekaorigo@gmail.com								
Password	•••••								
Last verified on	Fri Jul 23 12:23:19 BST 202	21							
VERIFY ACCOUNT New HID update account?	<u>Start Here</u>								
Keys associated wi	ith account								
Mabile Key : MCBA23 Custamer Name : Euraka D Issuad an : 2019-07 : Exupon : 2019-07 : Endpoint : 90807151;	3 ano Org 27 14 47:59+01:00 27 14 47:59+01:00 3 iCLASS® St	HID Seos®							

### A.4 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 HBM:

1. Log into HBM and click the Live! option to view HBM events.

HID Live!	People Device	es System			😗 HELP		🛔 ADMIN	() ABOUT
Trans:	actions							•
Details Filt	ers							
Biometric Match 1:N Faile	ad	RFID Credential Read		RFID Credential Read				
	Unknown User		John Smith		John Smith			
	N/A		67116		67116			
	RB25F-		RB25F-		RB25F-			
•	0006900209749)	•	00069WO209749)	•	0006900209749	)		
	19:30:39		19:30:39 2021-07-27		19:30:31			
	2021 07 27		20210121		20210727			
Date/Time	Event		Device			Name		Card
2021-07-27 19:30:	39 Biometric Mate	ch 1:N Failed	RB25F-00068E100236	(IP14190029WO20	9749)			FFFFF
2021-07-27 19:30:	39 RFID Credent	al Read	RB25F-00068E100236 (	(IP14190029WO20 (IP14190029WO20	9749)	John Smith		92506F0CFFFF12E0
2021-07-27 19:30:	31 Biometric Mate	ch 1:N Failed	RB25F-00068E100236	(IP14190029WO20 (IP14190029WO20	9749)	John Shidi		FFFFFF
2021-07-27 19:30:	24 Biometric Mate	ch 1:N Failed	RB25F-00068E100236	(IP14190029WO20	9749)			FFFFF
2021-07-27 19:30:	24 RFID Credent	al Read	RB25F-00068E100236	(IP14190029WO20	9749)	John Smith		92506F0CFFFF12E0
2021-07-27 19:30:	20 Biometric Mate	ch 1:N Failed	RB25F-00068E100236 (	(IP14190029WO20	9749)	John Smith		FFFFFF 02506E00EEEE12E0
2021-07-27 15.30.	20 RFID Cledelik	ai Keau	RD23F-00060E100236	(IF 1415002511020	5145)	John Shiur		32306F0CFFFF12E0

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

# $\begin{array}{c} \text{Appendix B} \\ \text{Fingerprint template encryption} \end{array} \end{array}$

### **B.1 In-field update for existing installations**

To provide greater data security, the Signo 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 HBM software to software version 1.0.2000.00019.
- 2. Update the firmware of each Signo 25B device connected to the HBM.
- 3. After updating the Signo 25B devices, each device must be reset to their factory default state. See **2.4.4 Reset a device**
- 4. Uninstall each Signo 25B device from within HBM and re-install them.

### Notes:

- Steps 3 and 4 ensure a clean move to HBM version 1.0.886.57608 or higher.
- The device profile will sync to make sure all the reader configuration is downloaded to the Signo 25B device after re-installation and once connection has been established with the HBM.

### **B.2 New installations**

- 1. Verify that the HBM software is at version 1.0.2000.00019, and Signo 25B is at firmware version 1.5.1.56.
- 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 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 25B has been updated to firmware version 1.5.0.86, and the Signo 25B has gone through a re-install process, it must connect with the HBM in order for the encryption key to be sent to the Signo 25B. There are two important points of note:

- Once the update is complete, the device will only allow **Template on Device Authentication** until the AES-256 encryption keys are sent from the HBM. If the authentication mode was set to **Finger Only** or **Finger + Card** the device will need to make a connection with the HBM 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 HBM is running on is destroyed, it is not possible to recover them.

## Appendix C

Guidelines for setting up MS SQL database



### C.1 Manually attaching the database

The database must be attached manually through the SQL Server Management Studio.

- 1. Open SQL Server Management Studio
- 2. Select the Server Name and right click on Databases.
- 3. Select Attach.
- 4. Select Add from the Attach Databases tab, and browse to the database folder and select the mdf file.
- 5. An entry is added to the **Databases To Attach** table.
- 6. Navigate to the Owner column in the table.
- 7. Select **sysdba** from the dropdown menu.
- 8. Select **OK** to save and close.

### Notes:

- You may need to create the sysdba user in SQL Server Management Studio first.
- A common problem during this step, is that the SQL server does not have permission to access the database files. There are two options to resolve this.
- a. Change the account that the SQL Server service uses. Open Services under Administrative Tools in Control Panel. Find the SQL Server Service and open its properties. Change the "Log on As" account to "Local System Account".
- b. Change the file permissions on the database folder in Windows Explorer. Right-click on the Database folder. On the Security tab, edit the permissions to include the user account that the SQL Server service is running as.

### C.2 SQL Server set up

Run the Microsoft SQL Server installer.

- 1. Select **Mixed Mode Authentication**. You can now log on to SQL Server using Windows authentication, or as a defined SQL Server user.
- 2. If you are using an existing SQL Server installation, you can change the server authentication options in SQL Server Management Studio by right-clicking on the server in object explorer, and selecting **Properties**.
- 3. Select Security under the Properties tab. Change the Server Authentication to SQL Server and Windows Authentication mode.

### C.3 Remote SQL server set up

The SQL server can run on a different server to the software, and connect to a remote server via the host name of the IP address. By default, SQL Server Express blocks remote connections.

- 1. Open SQL Server Configuration Manager (SSCM).
- 2. Select SQL Server Network Configuration.
- 3. Select **Protocols** and double click TCP/IP.
- 4. On the **Protocol** tab, change **Enabled** to **Yes**.
- 5. On the IP Addresses tab, change Active and Enabled to Yes for the IP addresses required for connection.
- 6. Change all **TCP Port**s to **1433**.

Note: This can be done by setting the TCP Port to 1433 for the IP All option.

- 7. Select SQL Native Client on the SSCM main page.
- 8. Select Client Protocols and double click TCP/IP.
- 9. Change the Default Port to 1433 and Enabled to Yes.

Note: Please contact your system database administrator or IT support for additional guidance.

# Appendix D Acronyms and terminology



Term	Definition
Authentication Mode (Signo 25B)	<b>Template on Card:</b> The Signo 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.
	<b>Card + Finger:</b> The Signo 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.
	<b>Finger Only:</b> The Signo 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).
	<b>Card Only:</b> The Signo 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).
	<b>Card Only (or) Finger Only</b> : The Signo 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.



Term	Definition
OSDP	Open Supervised Device Protocol (OSDP) is an access control communications standard developed by the Security Industry Association (SIA) to improve interoperability among access control and security products.
PAD	Pressure Attack Detection.
PD	Presence Detection.
ROC	Receiver Operating Characteristic.
SDK	Software Development Kit.
SIA	Structure Image Acquisition.
Тар	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.
	The users enrolled biometric template is written to a predetermined address in the application area of the supported credentials.
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	<ol> <li>Initial State</li> <li>Alternative State</li> <li>Total Duration</li> </ol>	1 0 9	Cyan Blue
Biometric Match Fail	<ol> <li>Initial State</li> <li>Alternative State</li> <li>Total Duration</li> </ol>	1 0 10	Red Blue
Biometric Match Success	<ol> <li>Initial State</li> <li>Alternative State</li> <li>Total Duration</li> </ol>	1 0 6	Green Blue
Biometric Match Timeout	<ol> <li>Initial State</li> <li>Alternative State</li> <li>Total Duration</li> </ol>	1 0 10	Red Blue
Biometric Scan Fail	<ol> <li>Initial State</li> <li>Alternative State</li> <li>Total Duration</li> </ol>	1 0 10	No color Blue
Biometric Scan Success	<ol> <li>Initial State</li> <li>Alternative State</li> <li>Total Duration</li> </ol>	1 0 10	No color Blue
Biometric Scan Timeout	<ol> <li>Initial State</li> <li>Alternative State</li> <li>Total Duration</li> </ol>	1 0 10	Red Blue
Credential Read Fail	<ol> <li>Initial State</li> <li>Alternative State</li> <li>Total Duration</li> </ol>	0 0 0	Red Amber
Credential Read Success	<ol> <li>Initial State</li> <li>Alternative State</li> <li>Total Duration</li> </ol>	1 0 9	Amber Magenta
Credential Read Timeout	<ol> <li>Initial State</li> <li>Alternative State</li> <li>Total Duration</li> </ol>	0 0 0	Red Amber
Enrollment Mode	<ol> <li>Initial State</li> <li>Alternative State</li> <li>Total Duration</li> </ol>	1 0 9	Cyan Amber
Fingerprint Scanned	<ol> <li>Initial State</li> <li>Alternative State</li> <li>Total Duration</li> </ol>	1 0 8	Black Magenta
Network Communications Error	<ol> <li>Initial State</li> <li>Alternative State</li> <li>Total Duration</li> </ol>	1 0 20	Red Blue
Other Media Read	<ol> <li>Initial State</li> <li>Alternative State</li> <li>Total Duration</li> </ol>	1 0 9	Green Red



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

## **Revision history**

Date	Description	Revision
August 2022	Updates to support HID Biometric Manager version 1.0.2000.00019.	B.3
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

© 2022 HID Global Corporation/ASSA ABLOY AB. All rights reserved. PLT-04029, Rev. B.3

Part of ASSA ABLOY