HID® Linq™ On Premise

User Guide

HID Linq On Premise Release: 1.3.0.37
PLT-08128, A.1
July 2025

Copyright

Trademarks

Contacts

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

What's new

Date	Description	Revision
July 2025	Updated to support HID Linq On Premise software version v1.3.0.	A.1

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

Section 01

Introduction

1.1 Document purpose

This document provides information to install and configure HID® Linq™ On Premise, connect to HID Signo™ readers, search and apply device Configuration Identifiers (Configuration IDs), create Configuration IDs, update HID Signo reader firmware, and manage custom keys stored in a local keystore within HID Linq On Premise.

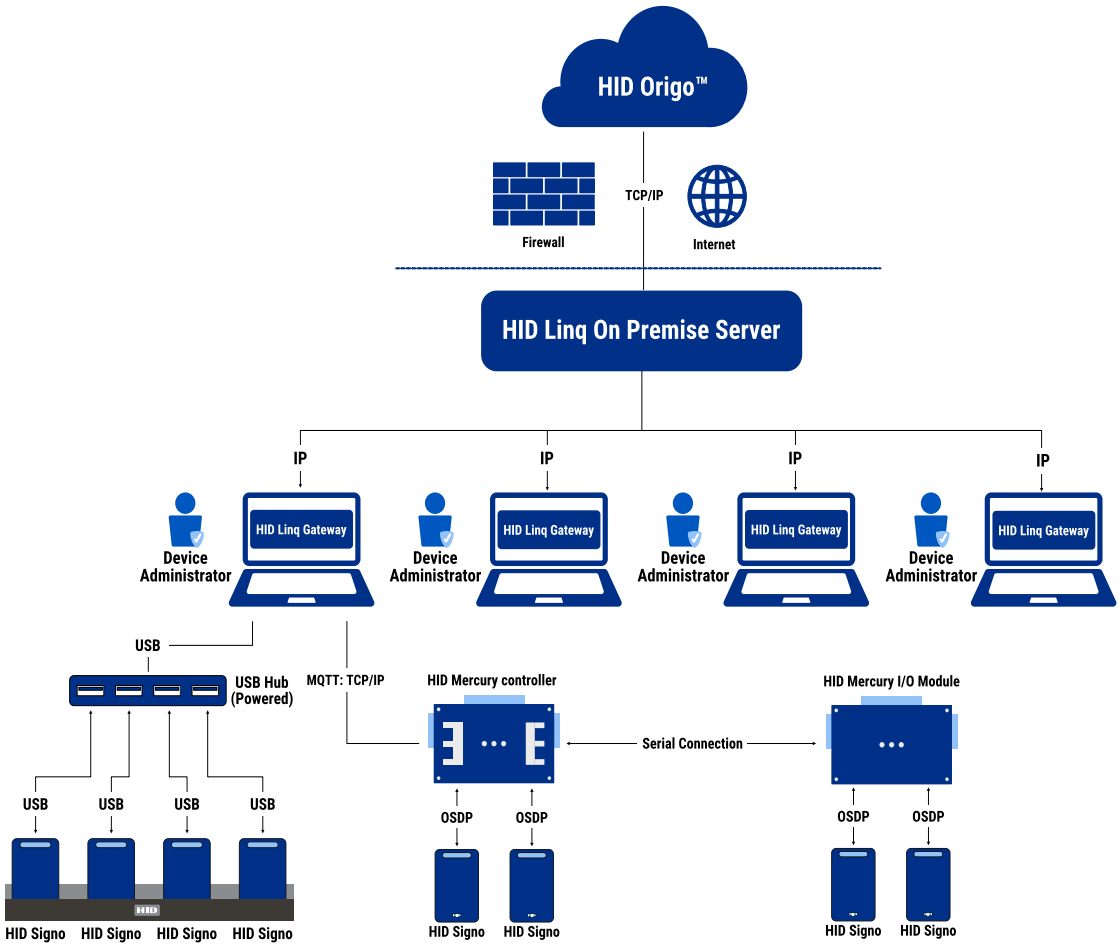
1.2 Intended audience

This document is intended for **System Administrators** and **Device Administrators** performing the following tasks:

- Connecting to HID Signo readers via the HID Signo Provisioning Accessory or HID Signo Programming Stand
- Updating Signo reader firmware and configurations via USB

1.3 HID Linq On Premise overview

HID Linq On Premise is a server-based application installed on the users premises enabling the configuration and firmware update of multiple HID Signo readers via controller or serial connection. HID Origo™ connection is optional.



HID Linq On Premise operates online via HID Origo device management services to access a library of reader Configuration IDs and reader firmware update files. It also operates offline using a custom keystore, or local configuration store.

The main components of the HID Linq On Premise solution are:

- **HID Linq On Premise:** A server-based application which connects to HID Signo readers via HID Mercury™ controllers, or directly via serial connections. HID Linq On Premise allows you to search and apply known Configuration IDs to connected HID Signo readers (via OSDP), create configuration IDs, and perform reader firmware updates (when available).
- **HID Linq Gateway:** A utility app that provides a secure connection between HID Linq On Premise and HID Signo readers. If you are connecting via a Mercury controller, additional set up is required to establish a secure connection.
- **HID Signo readers:** HID Linq On Premise is compatible with HID Signo 20, 20K, 40, and 40K readers.

1.4 System requirements

- Windows 10 64-bit Enterprise Edition 21H22 or newer.
- Windows 11 64-bit Enterprise Edition 21H22 or newer.
- 8 GB RAM.
- 20 GB available disk space.
- Web browser (Google Chrome recommended).

1.4.1 Hardware requirements

Caution: When connecting the reader via USB-C, **DO NOT** connect the reader to an external power source.

Important: It is best practice to use a powered USB hub when connecting a single reader, over a direct connection to the computers USB port.

- HID Signo Programming Stand (SIGNO-STAND-4) to connect up to four HID Signo readers to your PC.

  Note: Four USB-C to USB-A cables included. Contact your HID Sales representative to order the HID Signo Programming Stand.
- USB-C to USB-A cable(s) (if not ordering the HID Signo Programming Stand).
- Externally powered USB 3.0 hub for use with the HID Signo Programming Stand.

  Important: The hub must be externally powered, and able to provide a minimum of 500 mA per port.

1.4.2 Version information

Software	Version
HID Linq On Premise	1.3.0.37
HID Linq Gateway installer	1.3.0.6
HID Origo Management Portal	8.36.0

1.4.3 Signo reader firmware updates

Current Firmware version	Target Firmware Version
R10.0.10.4	R10.0.10.4 (Re-apply latest firmware version)
R.10.0.9.1	R10.0.10.4 (Upgrade)
R10.0.8.5	
R10.0.7.5	
R10.0.5.7	
R10.0.5.6	
R10.0.4.2	
R10.0.3.1	
R10.0.3.0	
R10.0.2.5	
R10.0.2.4	
R10.0.2.2	
R10.0.1.7	
R10.0.1.3	
R10.0.0.31	

1.4.4 Supported controllers and I/O modules

The listed HID® Mercury™ and HID® Aero® controllers and Serial Input/Output (SIO) modules are supported for use with HID Linq On Premise.

Note: HID Linq On Premise only works with HID controllers and SIO modules with the following minimum firmware versions.

Controllers	Minimum firmware version
Mercury LP1501	2.4.0
Mercury LP1502	2.4.0
Mercury LP2500	2.4.0
Mercury LP4502	2.4.0
Mercury MP1501	2.6.0
Mercury MP1502	2.6.0
Mercury MP2500	2.6.0
Mercury MP4502	2.6.0
Aero X1100	2.4.0
Aero x1100A	2.4.0
Serial Input/Output modules	
Mercury MR50-S3	3.2210
Mercury MR52-S3	3.22.10
Mercury MR52-S3B	3.22.10
Aero X100	3.22.10
Aero X100A	3.22.10

Caution: Firmware upgrade via HID controllers is not currently supported.

Note:

- Only HID Signo readers connected to Mercury via OSDP are supported. Readers connected via Wiegand are not supported by HID Linq On Premise. Please use HID Reader Manager™ to configure readers connected via Wiegand.
- S2 boards are not supported for the update of readers via HID Linq On Premise.
- Only authentic HID controllers are supported.
- HID Linq Gateway must also be installed alongside HID Linq On Premise, and on any PC used to remotely access HID Linq On Premise, to connect to HID Signo readers.
- You will need your HID Linq On Premise username and password, together with the IP address of the PC running HID Linq Gateway during the controller set up.

1.4.5 Signo offline soft charge profile

This allows you to perform any offline functionalities and requires a dedicated offline HID Signo reader with an unprogrammed soft charge profile. Select this profile when ordering any HID Signo reader (excluding HID Signo 25B).

Please see the **Readers and Credentials How to Order Guide** for more information.

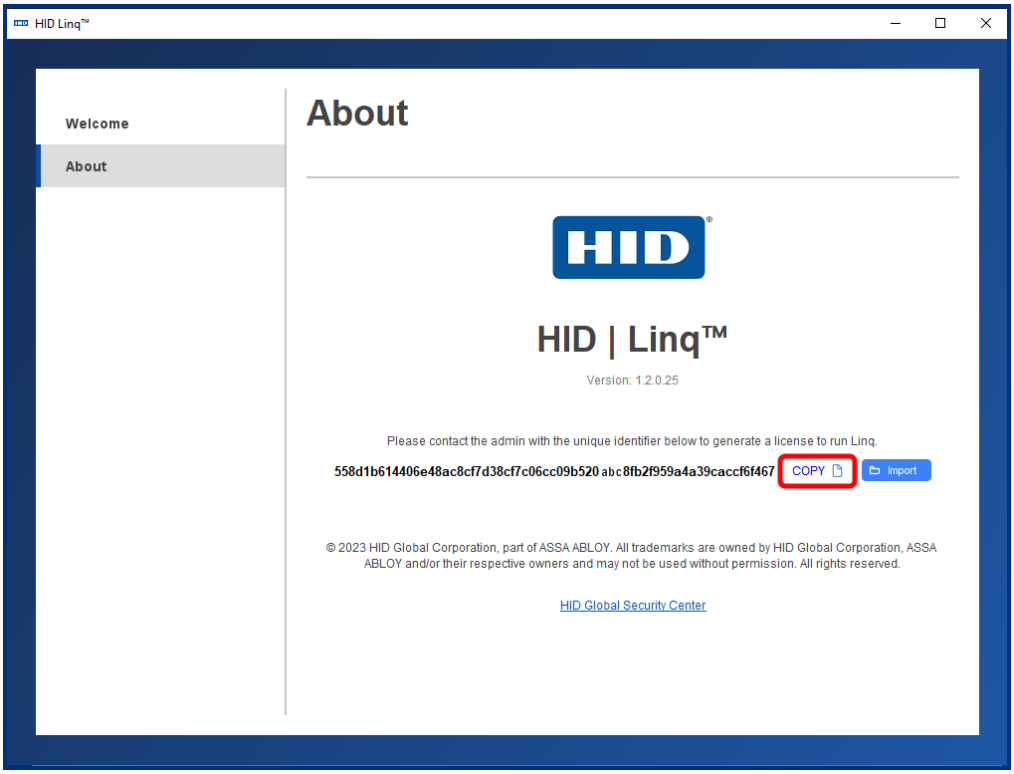
Please see the *Readers and Credentials How to Order Guide* (PLT-02630) for more information.

1.5 Licensing

HID Linq On Premise requires licensing to comply with legal requirements and grant access to all features.

1.5.1 Obtain a license

1. Click the **About** tab in the left-hand menu.
2. Click **COPY** to copy the unique identifier.



3. Send your unique identifier to your HID representative. HID will send your license files.
4. Save your license files to **C:\ProgramData\HID Global\Linq Device Manager**.
5. Click **Import** and select the license files received from HID.
6. Navigate to the **Welcome** tab in the left-hand menu. Click **LAUNCH**.

Section 02

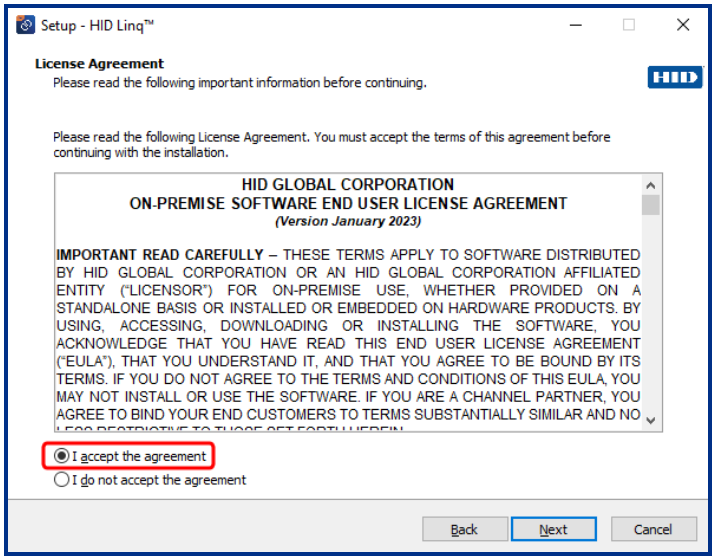
Install HID Linq On Premise

2.1 Install HID Linq On Premise

To install HID Linq On Premise on a server, or individual PC:

> **Important: You must be logged in to the PC as an administrator to install HID Linq On Premise.**

1. Double-click the setup file to launch the installation wizard.
2. Click **Next**.
3. Select **I accept the agreement** and click **Next**.



4. Check the **HID Linq™** box and **Setup SQL Server** box and click **Next**.
5. Enter an **SQL SA Password** and an **SQL Server Connection Password** and click **Next**.

   > **Note:** Make a note of the **SQL Server Connection Password**. It is needed later in the installation process.

6. Follow the on-screen prompts and click **Install** to begin the installation.
7. Click **Finish** to launch the application.
8. Enter and confirm a **Master password** and click **OK**.
9. Enter the **SQL Server Connection Password** created in step 5 and click **OK**. The HID Linq On Premise launch window is displayed.
10. Click **Launch** to launch the HID Linq On Premise web browser.

    > **Note:** Click **Advanced** > **Proceed to localhost (unsafe)** in the browser warning.

11. Enter the default credentials and click **SIGN IN**.

    > **Note:**
    > - **Username**: admin
    > - **Password**: password

12. Enter and confirm a new password.
13. Click **SET PASSWORD AND CONTINUE**.

2.1.1 Download a recovery key

HID Linq On Premise supports a Microsoft SQL database for storing encrypted user information. The backup and recovery feature allows you to move HID Linq On Premise to a different PC or server.

1. Click **DOWNLOAD**.
2. The recovery key is downloaded to your **Downloads** folder.
3. Save the recovery key in a secure location for future use.

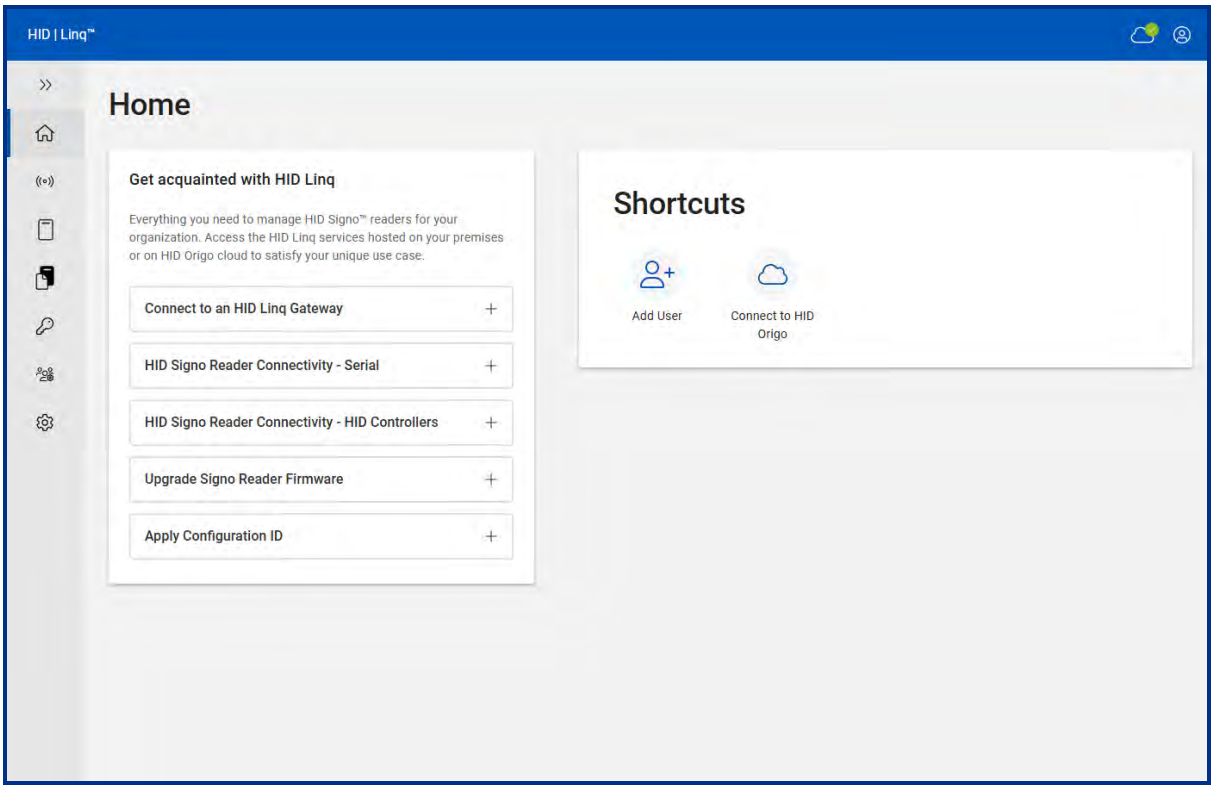
Section 03

Home page and navigation

3.1 Home page

The home page is displayed once you have logged in and includes:

- **Navigation tabs:** To access different pages within HID Linq On Premise. See **3.2 Navigation** for more information.
- **General tips section:** For brief descriptions of HID Linq On Premise features.
- **Shortcuts section:** Quick access to common tasks.



3.2 Navigation

Icon	Description
	Home tab: Displays task guidance and shortcuts to common actions. See 3.1 Home page for more information.
	Live Events tab: Displays real time feedback on reader status and events (for example, card read success and firmware updates). See 4.12 Live events for more information.
	Readers tab: Displays connected Gateways and HID Signo readers, together with their installation status. Add or remove devices from the Readers tab.
	Device Configuration Templates tab: Create, search, and apply existing online and offline device configuration templates.
	Keystore tab: View, add or manage the local keystore and key sets.
	Users tab: Displays all current users and their role. The Users tab allows you to add new users, manage existing users, and reset a user's password.
	Settings tab: Allows you to add an existing HID Reader Manager Technician account credentials, update HID Linq On Premise, and perform a system recovery.

Section 04

System administration

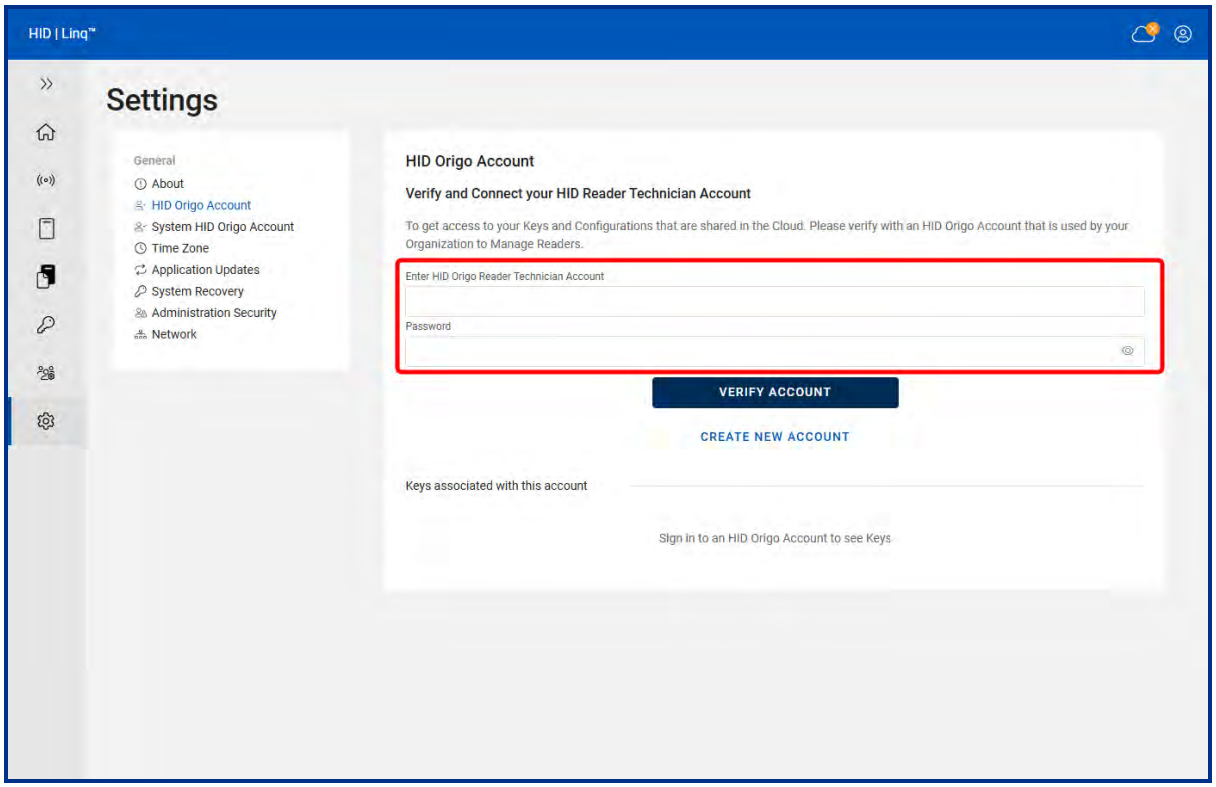
4.1 HID Origo account

Verify your HID Origo account to access your online keys and Configuration IDs and apply them to your readers.

Note:
- HID Origo connection is not required to apply local configurations or access the HID Linq Custom Keystore.
- Enter your existing HID Reader Manager Technician account credentials to view keys associated with your account.

Verify your account:

1. Navigate to the **Settings** tab in the left-hand menu.
2. Click **HID Origo Account**.
3. Enter the **E-Mail Address** and **Password** for your HID Reader Manager Technician account.



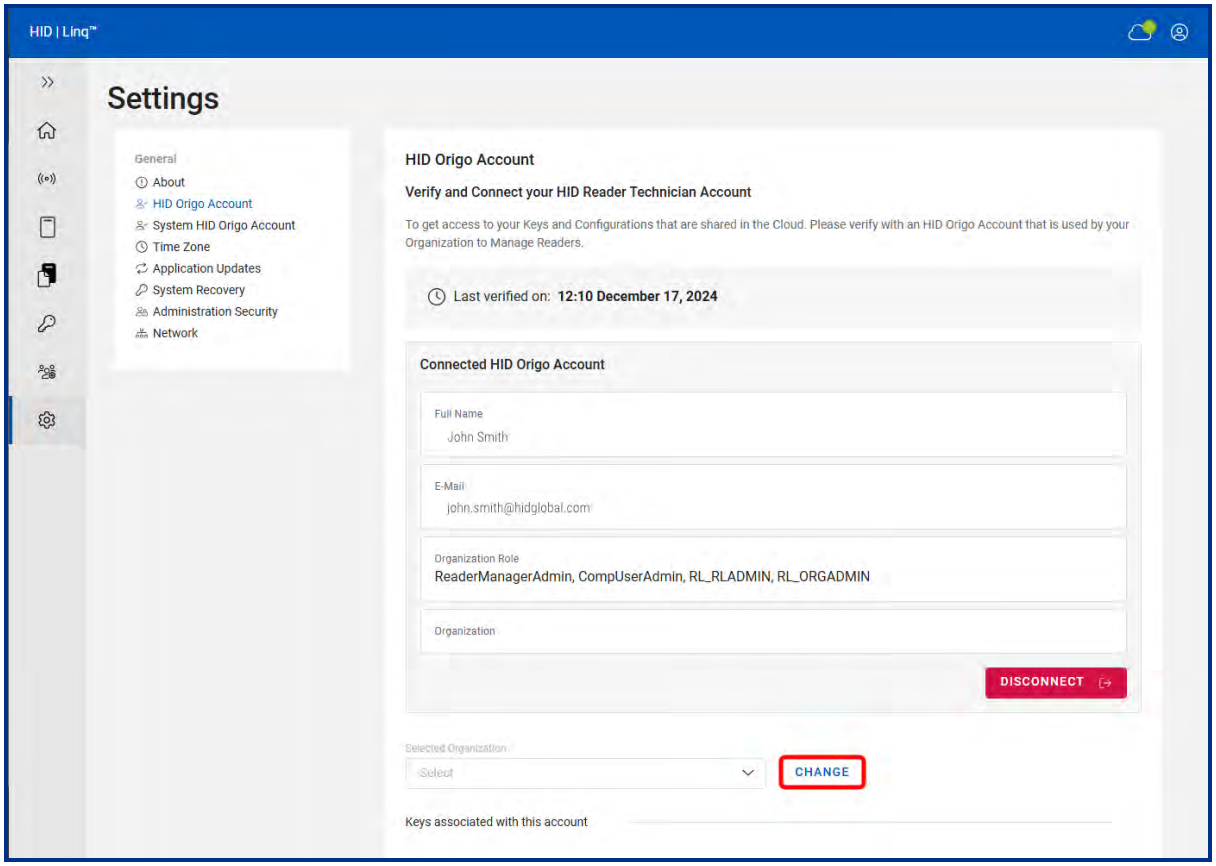
4. Click **VERIFY ACCOUNT**.

Note: Contact your organization's HID Reader Manager Portal Administrators if you need a new HID Origo account.

4.1.1 Change organization

Reader Technicians associated with multiple organizations can switch between organizations in HID Linq On Premise.

1. Navigate to the ⚙ **Settings** tab in the left-hand menu.
2. Click **HID Origo Account**.
3. Click **CHANGE**.



4. Select the required organization from the **Select Organization** drop-down list.
5. Click **SAVE**.

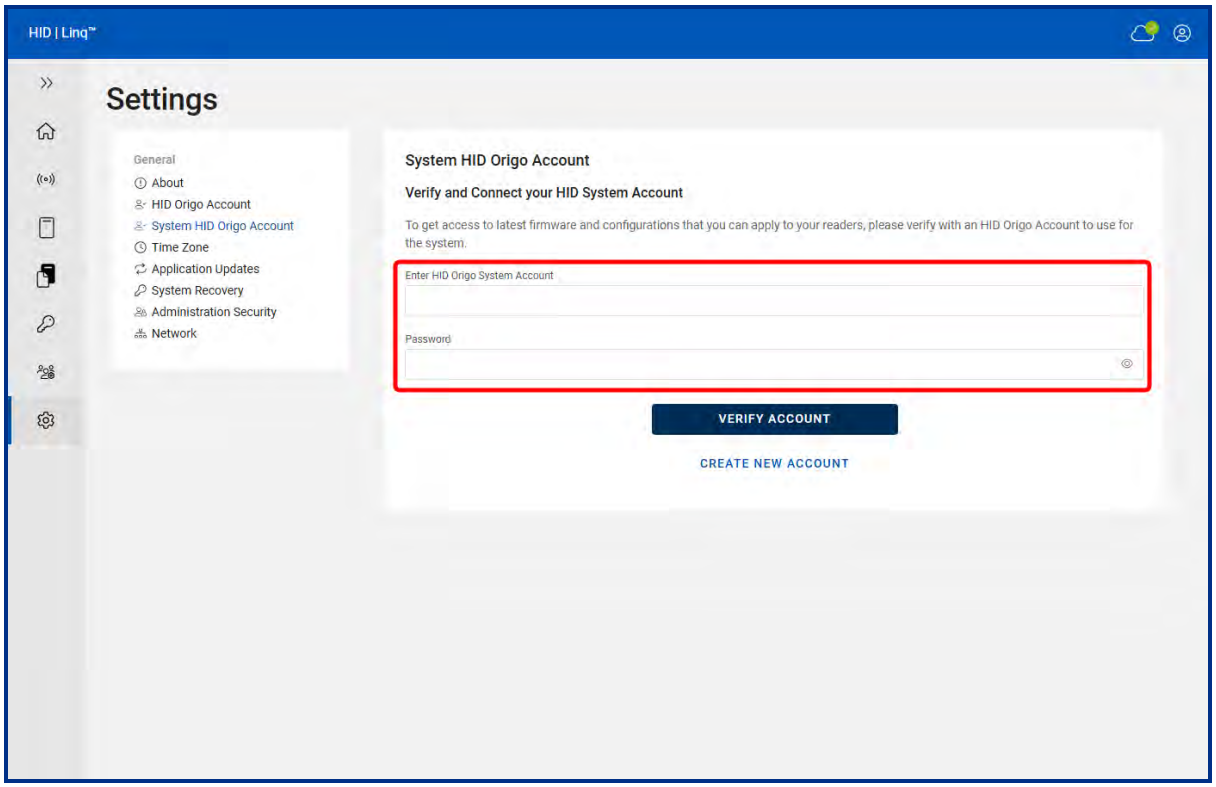
4.2 System HID Origo account

Verify your System HID Origo account to access the latest firmware and Configuration IDs and apply them to your readers.

> **Note:** Enter your existing HID System account credentials to view keys associated with your account.

Verify your account:

1. Navigate to the ⚙ **Settings** tab in the left-hand menu.
2. Click **System HID Origo Account**.
3. Enter the **E-Mail Address** and **Password** for your HID Origo System account.



4. Click **VERIFY ACCOUNT**.

> **Note:** Contact your organization's HID Reader Manager Portal Administrators if you need a new HID Origo account.

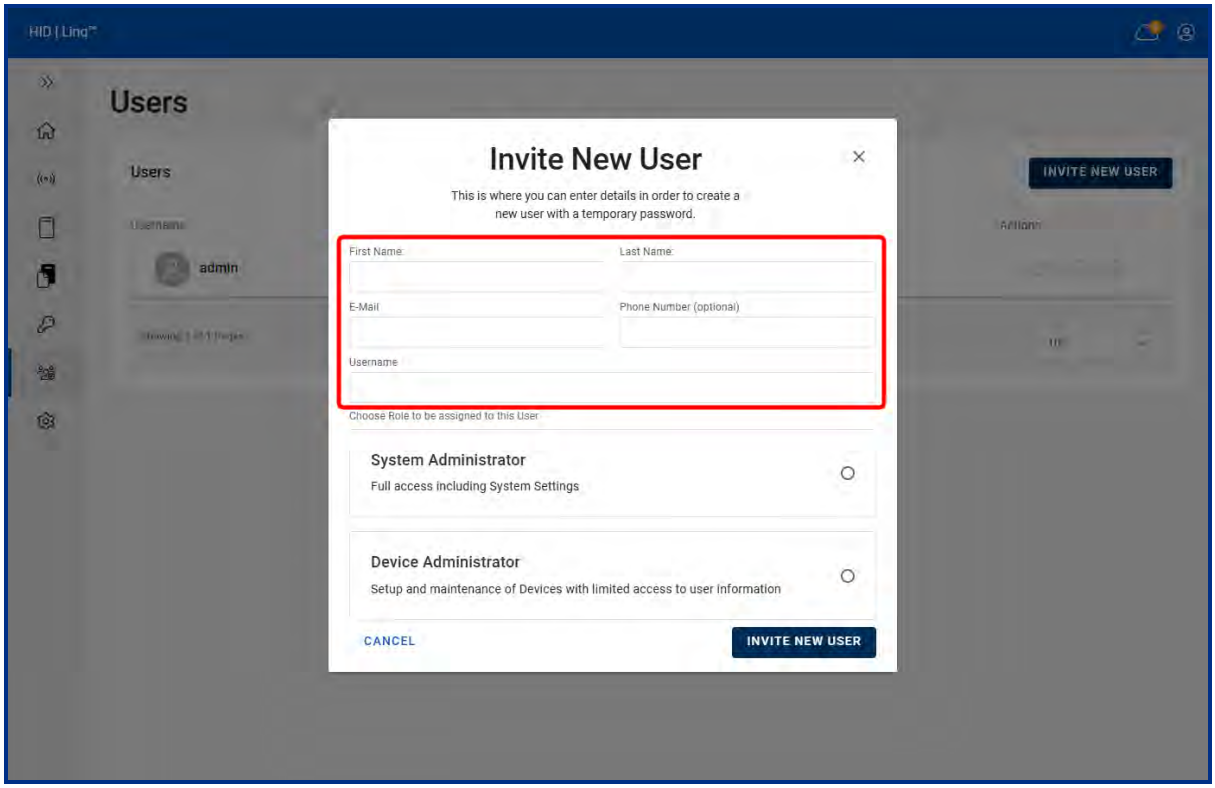
4.3 User roles

User Role	Privileges	Description
System Administrator	Super user	• Download, install, and set up HID Linq On Premise • Add and manage other users • Configuration and management of readers • Create Origo and Local Configuration IDs
Device Administrator	Device management only	• Configuration and management of readers

Note:
- There is no limit to the number of System Administrator or Device Administrator users in HID Linq On Premise.
- System Administrators or Device Administrators can be HID Reader Manager Technician account holders with access to HID keys. These users must validate their HID Reader Manager credentials in HID Linq On Premise to gain access to the keys.

4.4 Add a user

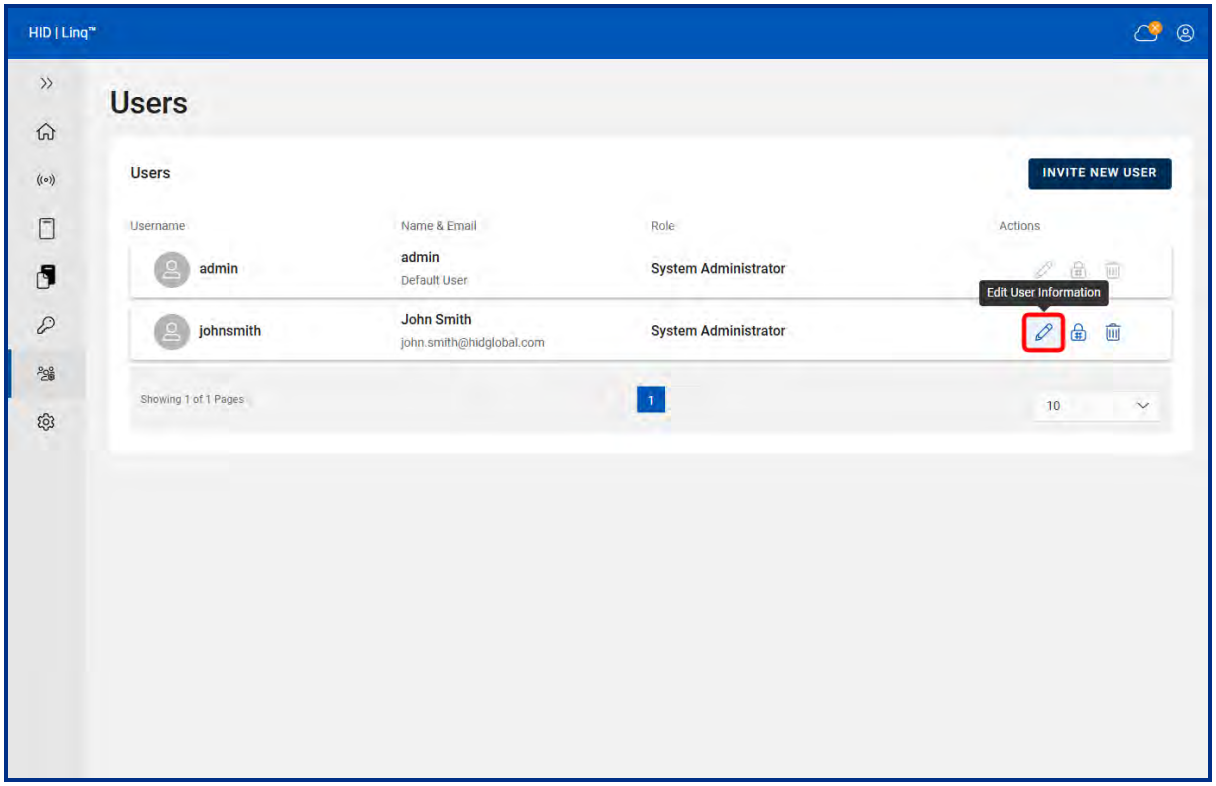
1. Navigate to the **Users** tab in the left-hand menu.
2. Click **INVITE NEW USER**.
3. Enter the new users information.



4. Select the required user role.
   - System Administrator
   - Device Administrator
5. Click **INVITE NEW USER**.
6. Copy and save the new users password.
7. Click **DONE**.
8. Email the new user their login details and the URL specific to the created instance of HID Linq On Premise.

4.5 Edit a user

1. Navigate to the **Users** tab in the left-hand menu.
2. Click the **Edit User Information** icon for the required user.

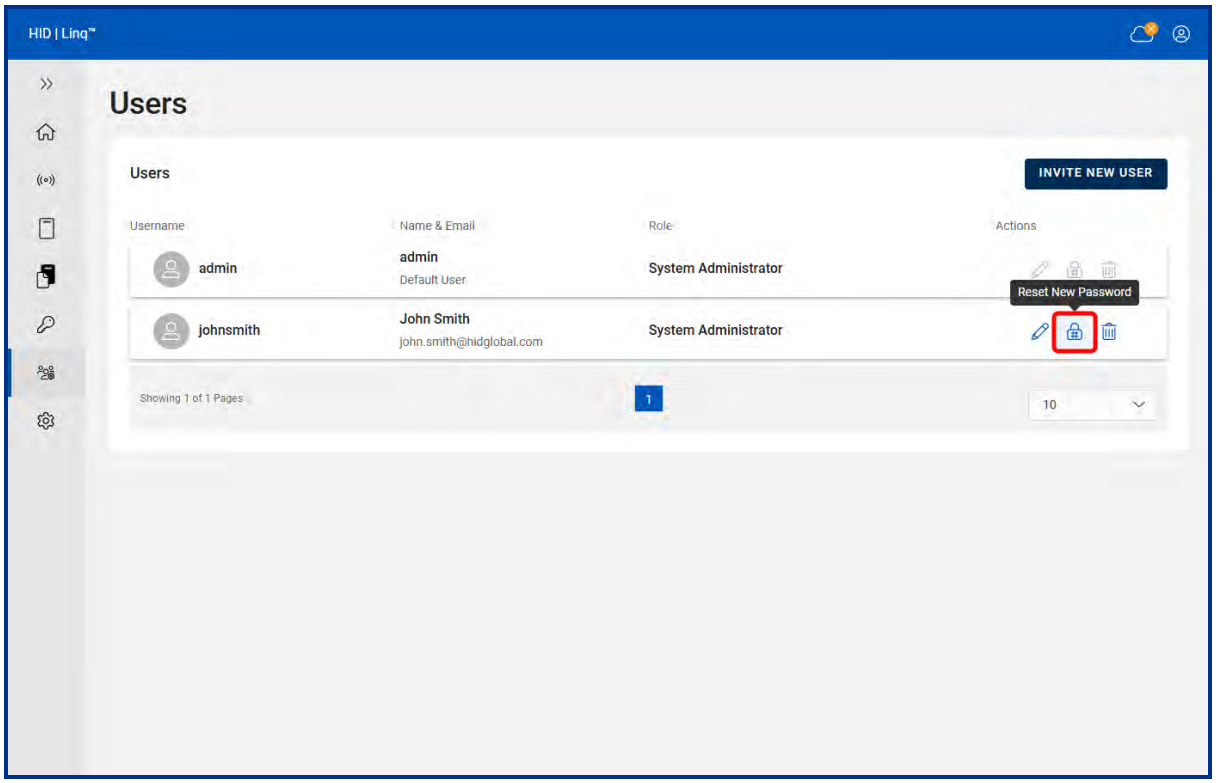


3. Edit the required details and roles.
4. Click **SAVE**.

4.6 Reset a user's password

Note: Only an Administrator can reset another user's password.

1. Navigate to the **Users** tab in the left-hand menu.
2. Click the **Reset New Password** icon for the required user.

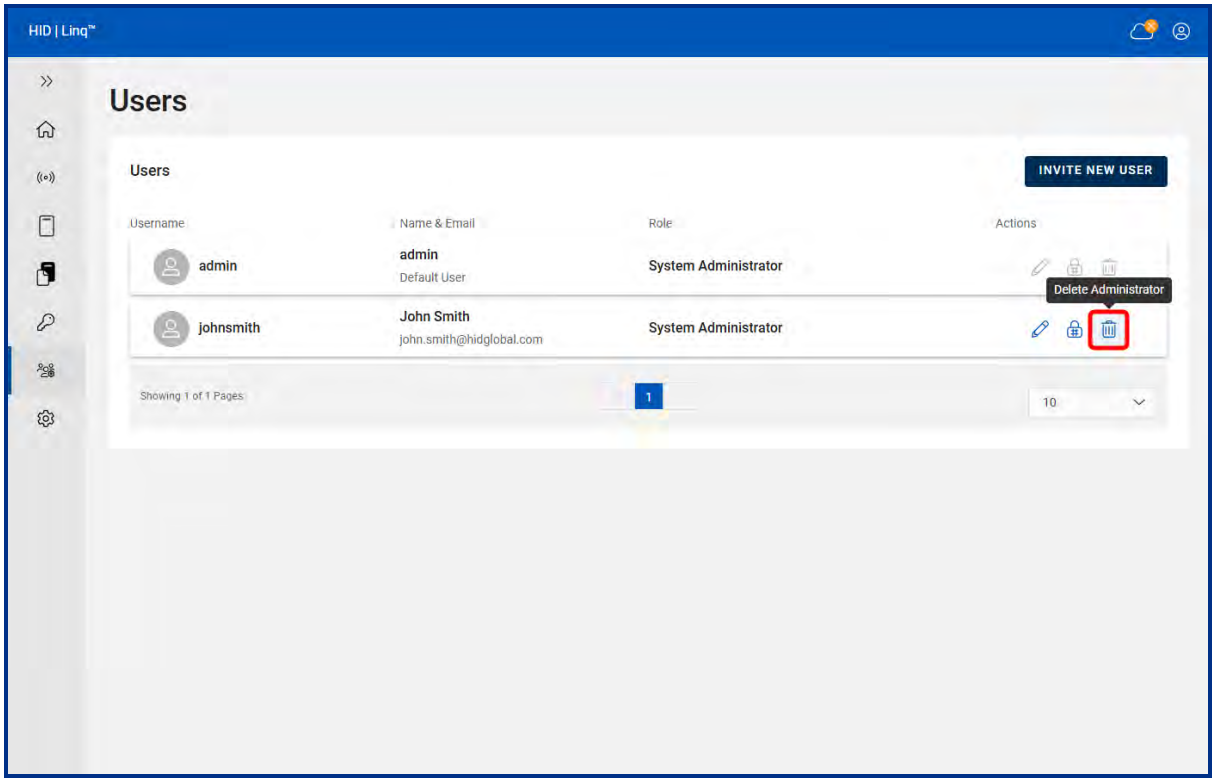


3. Click **RESET AND GENERATE NEW PASSWORD**.
4. Click **COPY PASSWORD**.
5. Email the user their new password.

Note: The user must log in using the temporary password. They will be prompted to enter a new password at log in.

4.7 Delete a user

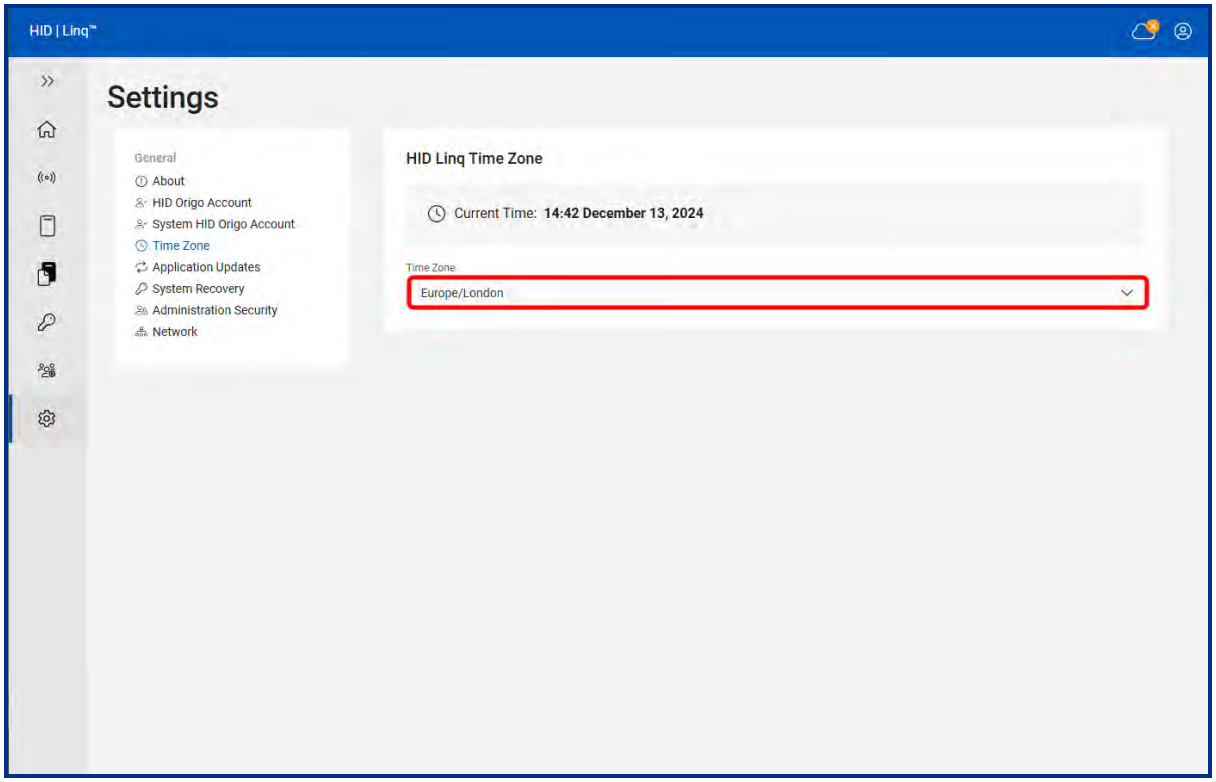
1. Navigate to the **Users** tab in the left-hand menu.
2. Click the **Delete Administrator** icon for the required user.



3. Click **DELETE ADMINISTRATOR**.

4.8 Set your time zone

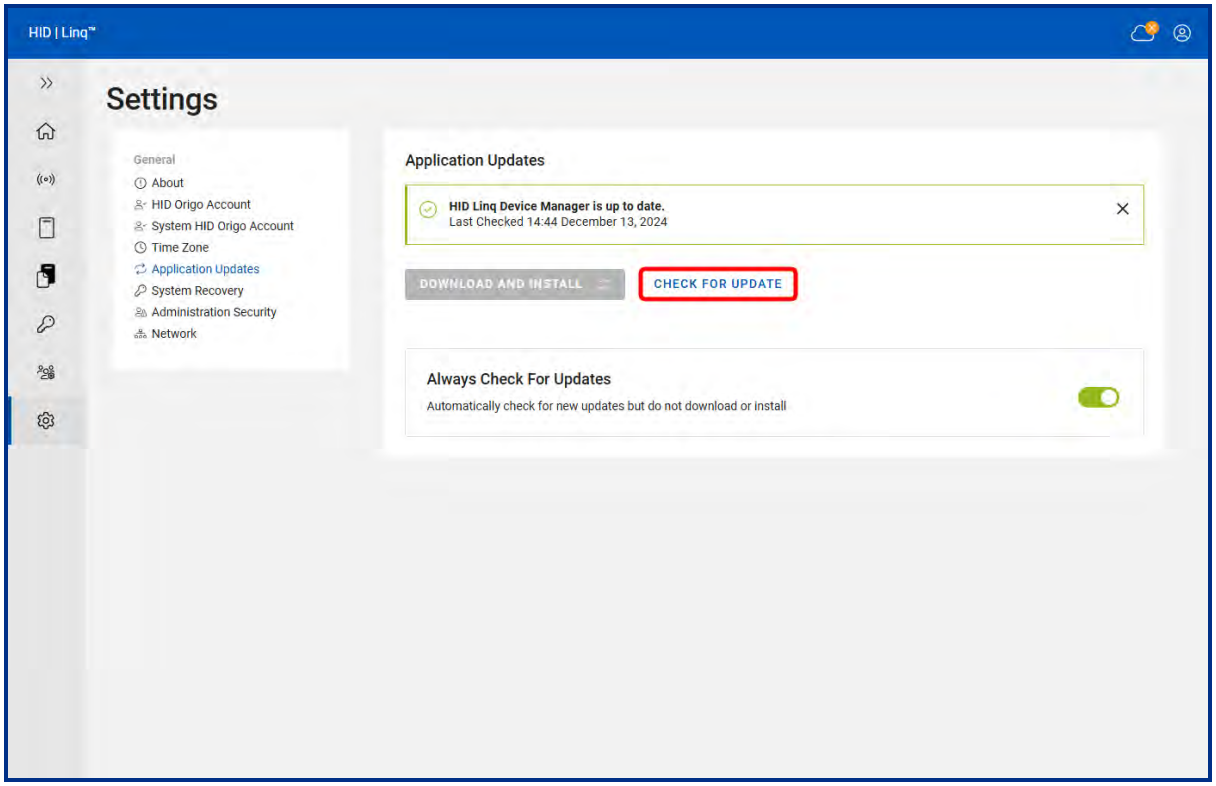
1. Navigate to the **Settings** tab in the left-hand menu.
2. Click **Time Zone**.
3. Select the required **Time Zone** from the drop-down menu.



4.9 Update HID Linq On Premise

Note:
- Only a System Administrator can update HID Linq On Premise.
- Offline users must contact HID Technical Support for HID Linq On Premise update information.

1. Navigate to the **Settings** tab in the left-hand menu.
2. Click **Application Updates**.
3. Click **CHECK FOR UPDATE**.



4. If an update is found, click **DOWNLOAD AND INSTALL**.

Note: Click the **Always check for Updates** toggle to automatically check for software version updates.

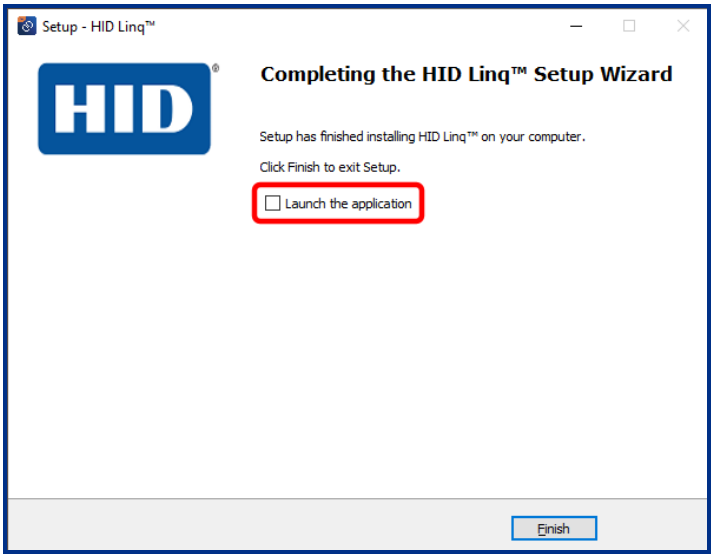
4.10 System backup and recovery

The system backup and recovery allows you to move the HID Linq On Premise install to a different computer using a recovery key.

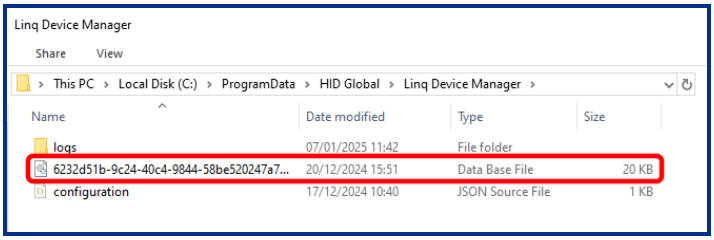
1. Double-click the setup file to launch the installation wizard on the new computer.
2. Click **Next**.
3. Select **I accept the agreement** and click **Next**.
4. Check the **HID Linq™** box and **Setup SQL Server** box and click **Next**.
5. Enter an **SQL SA Password** and an **SQL Server Connection Password** and click **Next**.

   > **Note:** Make a note of the **SQL Server Connection Password**. It will be needed later in the installation process.

6. Follow the on-screen prompts and click **Install** to begin the installation.
7. Uncheck the **Launch the application** box and click **Finish**.



8. Copy your **HID_LINQSERVER.mdf** and **HID_LINQSERVER_log.ldf** recovery files, and paste them to the new **C:\Program Files\HID Global\Linq Device Manager\database** folder, to overwrite the new files.
9. Copy and paste the required database file to the new **C:\ProgramData\HID Global\Linq Device Manager** folder.



10. Navigate to **C:\Program Files\HID Global\Linq Device Manager\bin** and double click **Configure.exe**.
11. Enter and confirm a new **Master password** and click **OK**.
12. Enter the **SQL Server Connection Password** created in step 5 and click **OK**. The HID Linq On Premise launch window is displayed. Click **Yes** to continue.

    > **Note:** Close the **Database Setup** window that is displayed.

13. Navigate to **C:\Program Files\HID Global\Linq Device Manager\bin** and double click **Start.exe**.
14. Enter the **Master password** and click **OK**.

15. Click **Launch** to launch the HID Linq On Premise web browser.

    > **Note:** Click **Advanced** > **Proceed to localhost (unsafe)** in the browser warning.

16. Login to HID Linq On Premise using your existing credentials.
17. The **Recovery Backup Key** window is displayed. Click **CHOOSE FILE**.

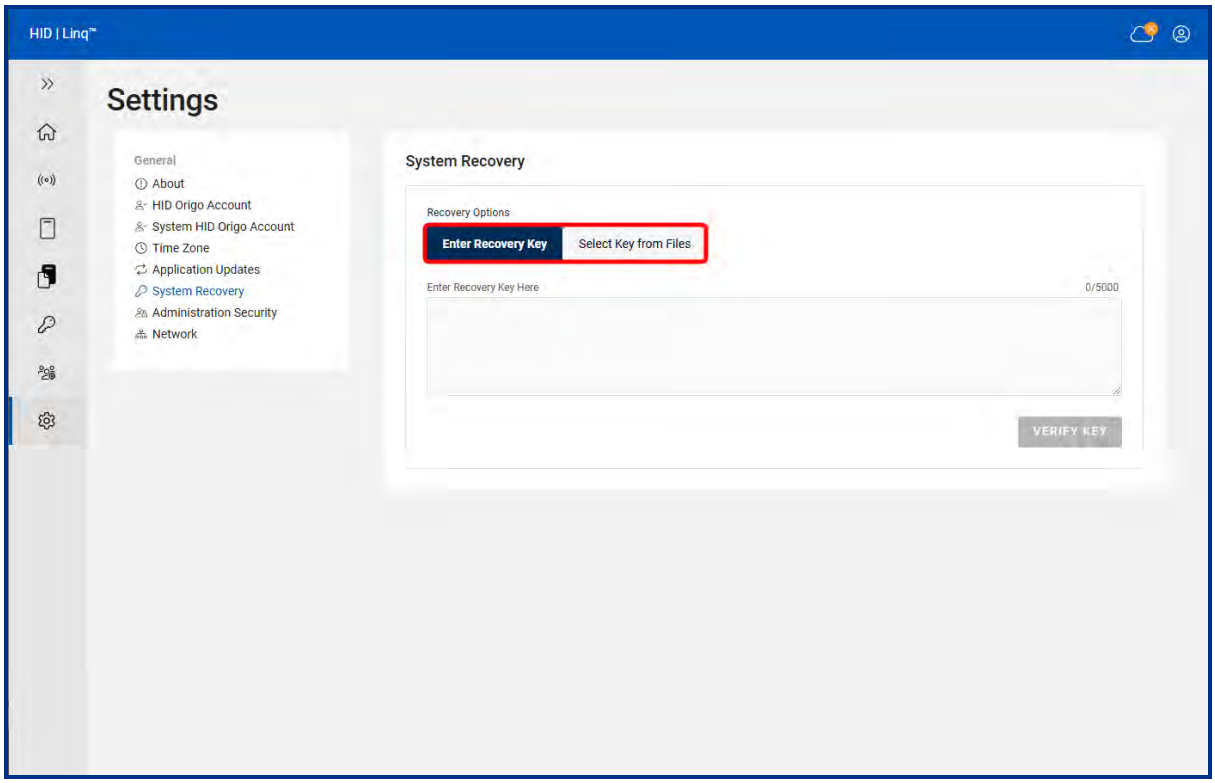
    > **Note:** If the **Recovery Backup Key** window is not displayed, see **4.10.1 Manually perform a system recovery** for more information.

18. Locate and upload the required **LDM_Recovery_Key.pem** file. Click **VERIFY KEY**.
19. Enter the **Master password** and click **OK**.
20. Enter the **Master password** and click **OK**.
21. Restart HID Linq On Premise. Navigate to **C:\Program Files\HID Global\Linq Device Manager\bin** and double click **Start.exe**.
22. Enter the **Master password** and click **OK**.
23. Click **Launch** to launch the HID Linq On Premise web browser.
24. Login to HID Linq On Premise using your existing credentials. Verify that your existing keystore, users and settings are visible.

4.10.1 Manually perform a system recovery

Note: Only a System Administrator can perform a system recovery.

1. Navigate to the **Settings** tab in the left-hand menu.
2. Click **System Recovery**.
3. Either:
   a. Click **Enter Recovery Key** and paste your key into the **Enter Discovery Key Here** field, or
   b. Click **Select Key from Files**, then **CHOOSE FILE** and upload the required **LDM_Recovery_Key.pem** file.



4. Click **VERIFY KEY** and follow the on-screen prompts.

4.11 Set administrative security options

This window allows you to view and manage administrative security settings, including:

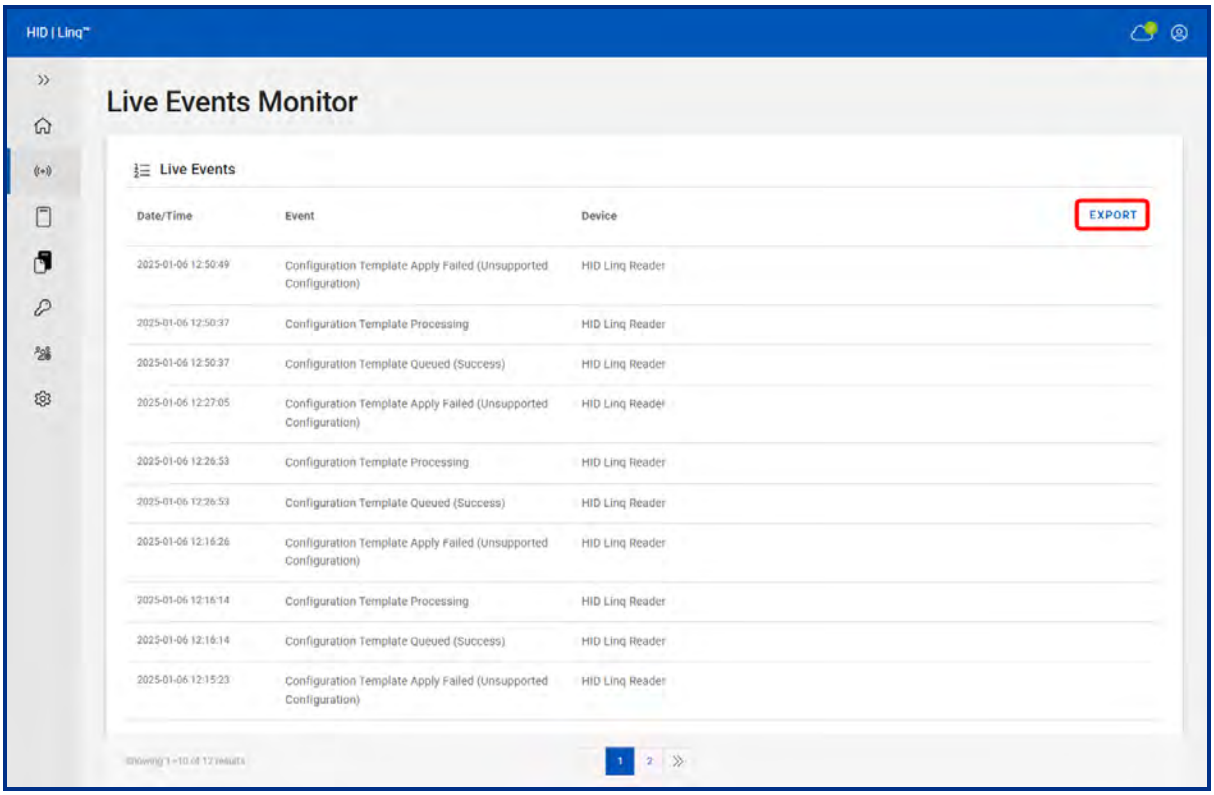
- How long a temporary password is valid
- How long an Administrator password is valid
- How often a password change prompt is displayed
- The time duration until an inactive user is automatically logged out

1. Navigate to the **Settings** tab in the left-hand menu.
2. Click **Administration Security**.
3. Click **CHANGE** to adjust the required setting.
4. Adjust the settings as required and click **SAVE** to apply the changes.

4.12 Live events

The **Live Events Monitor** displays a chronological list of live events from the current session, and events generated by other connected users.

Click **EXPORT** to export the live events data to a CSV file. Each event has a correlation ID that can be cross referenced against the HID Linq system logs. See **D.1 Logs** for more information on logs.



Note: Exporting live events provides further debugging information.

4.13 Change the HID Linq Gateway security profile

The HID Linq Gateway has two security profiles:

Security Profile	Behavior
Normal	HID Linq Gateway runs as an application and requires a manual restart every time the PC is powered off.
Relaxed	HID Linq Gateway runs as a service and does not require a manual restart every time the PC is powered off.

Note: It is recommended to use the Normal security profile as it is more secure.

Who can change the HID Linq Gateway security profile?

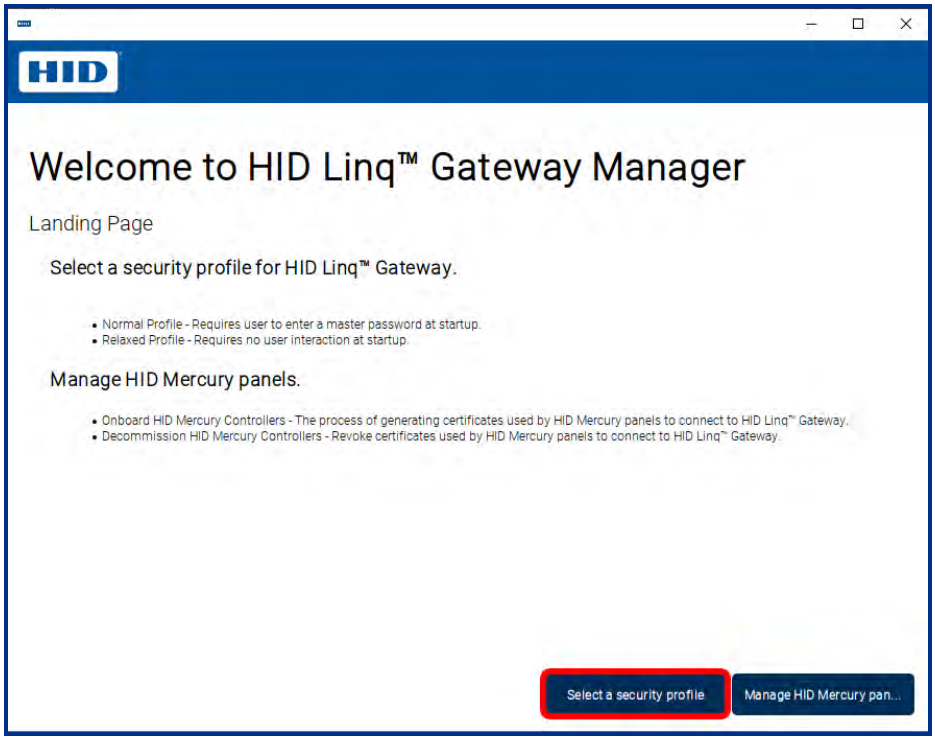
	Reader Manager Portal Administrator	Reader Technician
Permission	Yes	Yes
Multiple reader capability	N/A	N/A

Note: Please see **C.4 Security profiles** for more information on the two security profiles before changing the security profile.

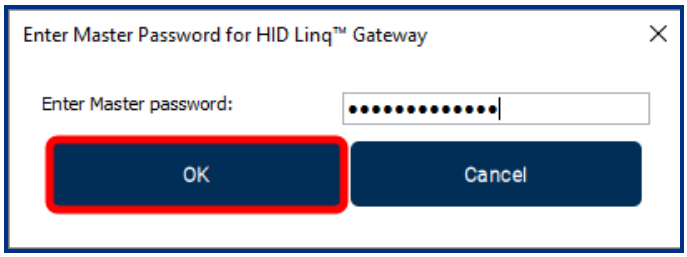
To change security profiles from Normal to Relaxed:

1. Exit the HID Linq Gateway in the Windows server tray.
2. Navigate to **C:\Program Files\HID Global\HID Linq™ Gateway\1.3.0.6**.
3. Double click **Configuration.exe**.
4. Enter the master password.

5. Click **Select a security profile**.



6. Click **Enable Relaxed Profile**.
7. Enter the master password and click **OK**.

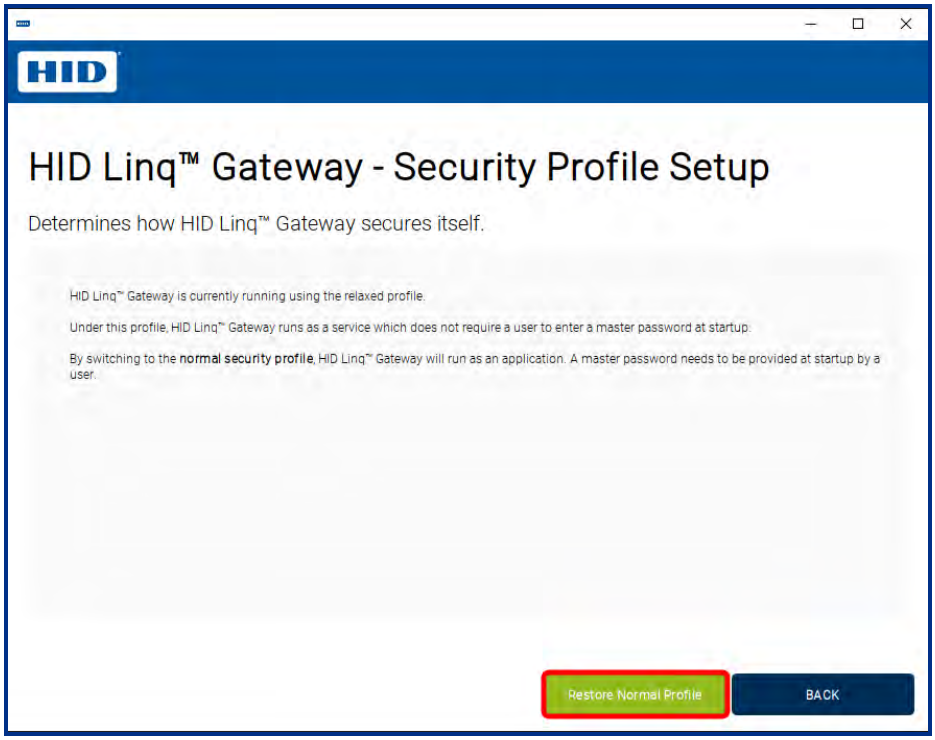


8. Click **OK** to finish.

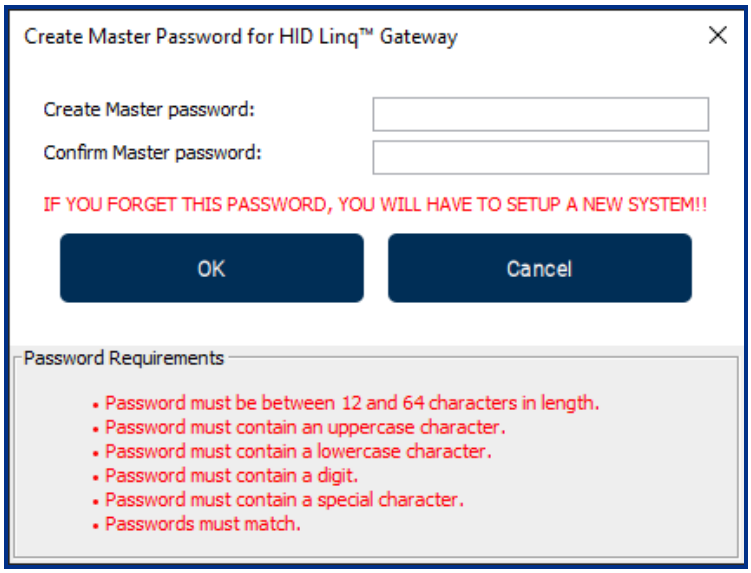
To change security profiles from Relaxed to Normal:

1. Navigate to **C:\Program Files\HID Global\HID Linq™ Gateway\1.3.0.6**.
2. Double click **Configuration.exe**.
3. Click **Select a security profile**.

4. Click **Restore Normal Profile**.



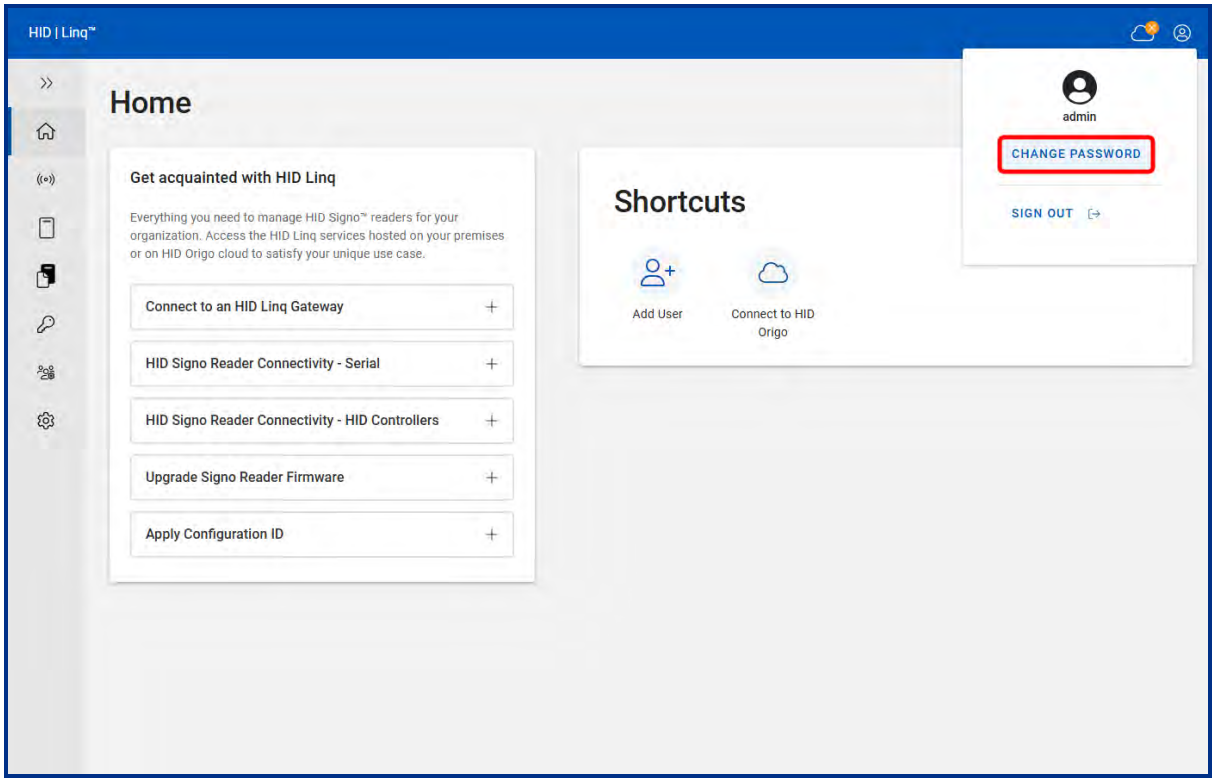
5. Enter and confirm the master password and click **OK**.



6. Click **OK** to finish.

4.14 Change your password

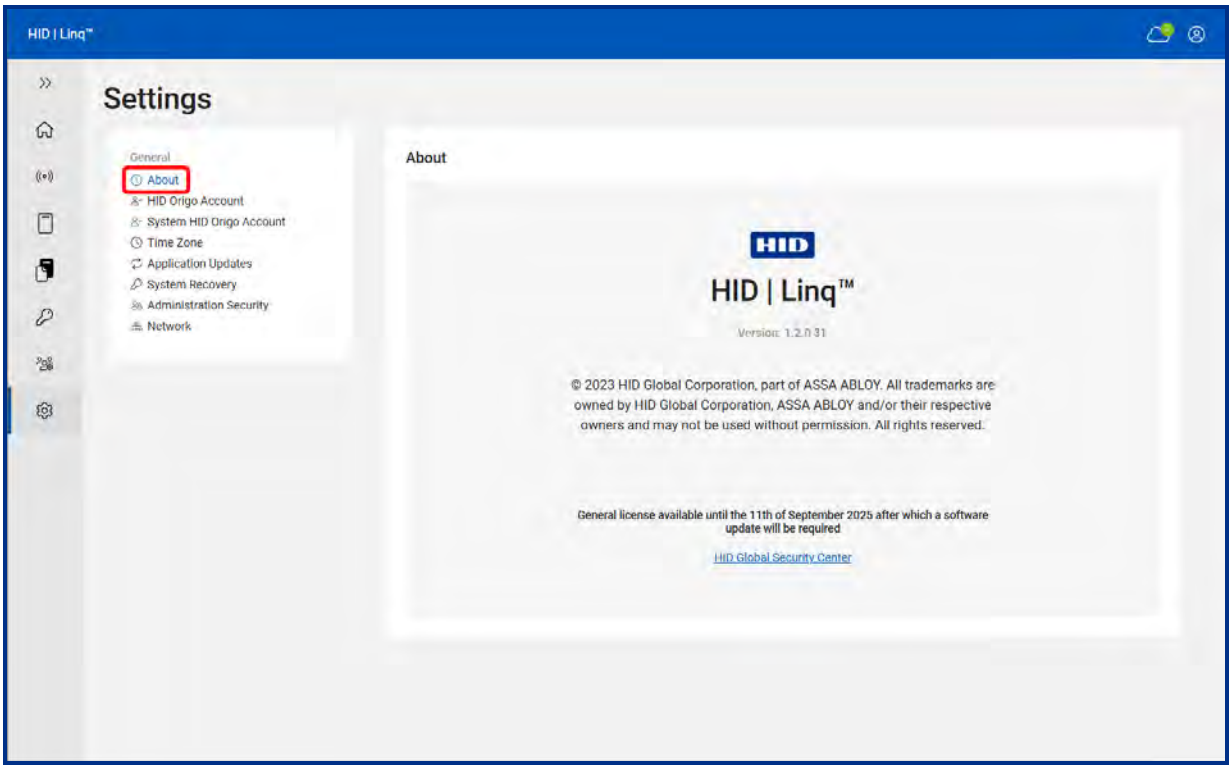
1. Click the **Profile** icon in the header.
2. Click **CHANGE PASSWORD**.



3. Enter your **Current Password**.
4. Enter a **New Password** that meets the security requirements.
5. Confirm the new password.
6. Click **SET NEW PASSWORD**.

4.14.1 About

This window displays the software version and information.



4.15 Sign out

1. Click the **Profile** icon in the header.
2. Click **SIGN OUT**.

Section 05

Download and install HID Linq Gateway

5.1 HID Linq Gateway

Install, set up and run HID Linq Gateway to provide a secure connection between HID Linq On Premise and connected HID Signo readers. HID Linq Gateway can run as an application or as a service, depending on your security requirements.

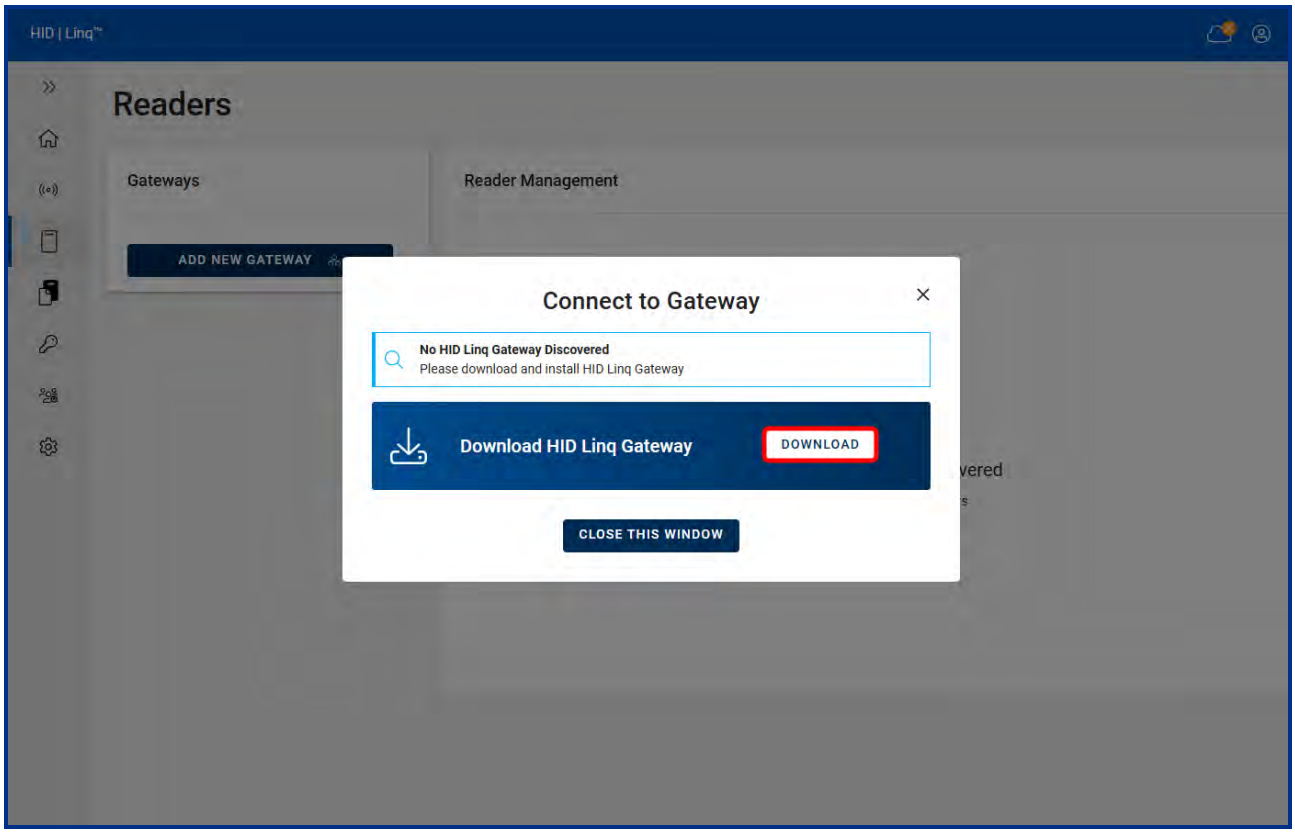
Who can download, set up and run HID Linq Gateway?

	Reader Manager Portal Administrator	Reader Technician
Permission	Yes	Yes

5.2 Download HID Linq Gateway

To download HID Linq Gateway, log in to HID Linq On Premise.

1. Navigate to the **Readers** tab in the left-hand menu.
2. Click **ADD NEW GATEWAY**.
3. Click **DOWNLOAD**.



Note: Only download one instance of HID Linq Gateway.

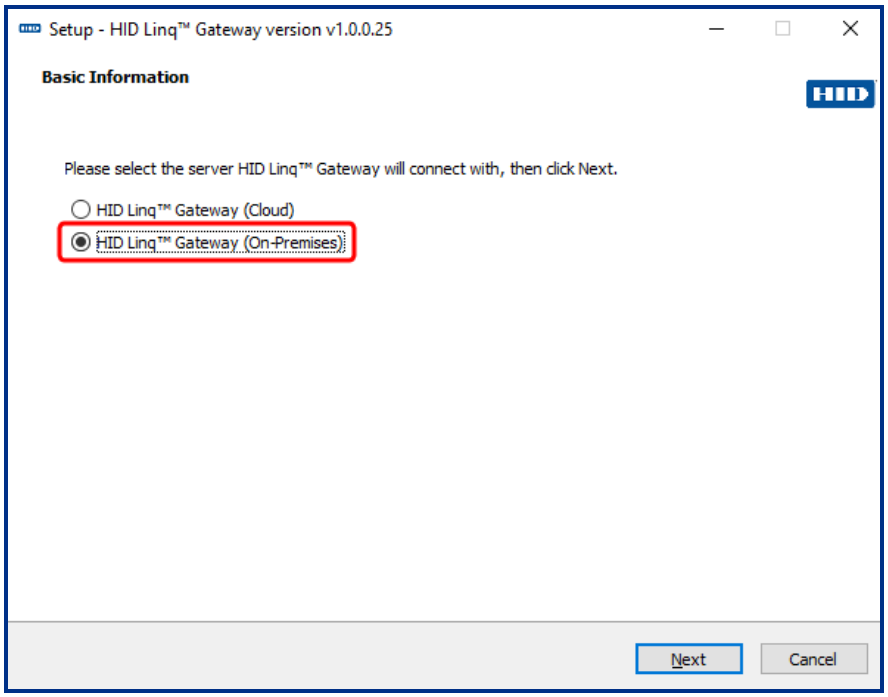
5.3 Install HID Linq Gateway

HID Linq Gateway must be installed to your machine to provide a secure connection between HID Linq On Premise and connected HID Signo readers. HID Linq Gateway can only be downloaded to a Windows OS and requires a minimum of Windows 10 or newer.

Important:
- To connect to HID Signo readers, HID Linq Gateway must be installed alongside HID Linq On Premise, and on any PC used to remotely access HID Linq On Premise.

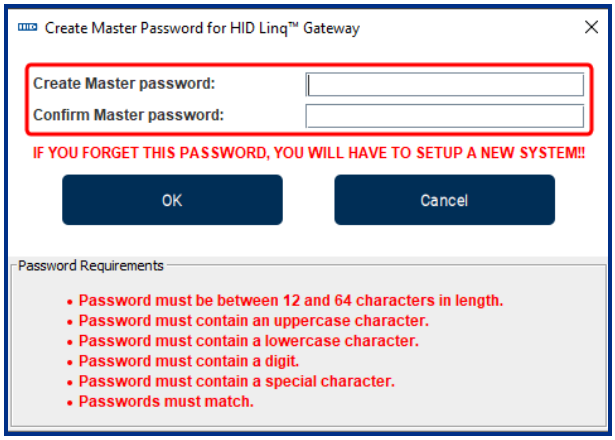
Note: Only one instance of HID Linq Gateway can be installed per PC. If you download a new version, you must uninstall and delete the previous version before installing the newest download.

1. Navigate to your **Downloads** folder.
2. Double-click the setup file to launch the installation wizard.
3. Select **HID Linq™ Gateway (On-Premises)** and click **Next**.



4. Click **Install**.
5. Click **Finish** to complete the installation.
6. Enter a **Gateway Name** and click **CONNECT TO GATEWAY**.

7. Enter and confirm a master password for your HID Linq Gateway and click **OK**.



8. Click **Yes** in the pop-up window.

5.4 Create a new gateway

Create a new gateway to discover readers connected to the computer. Gateways created in HID Linq On Premise are accessible to other HID Linq On Premise users on the same network. Only create a gateway for a specific computer on the network, which must only be activated on the computer it is created for.

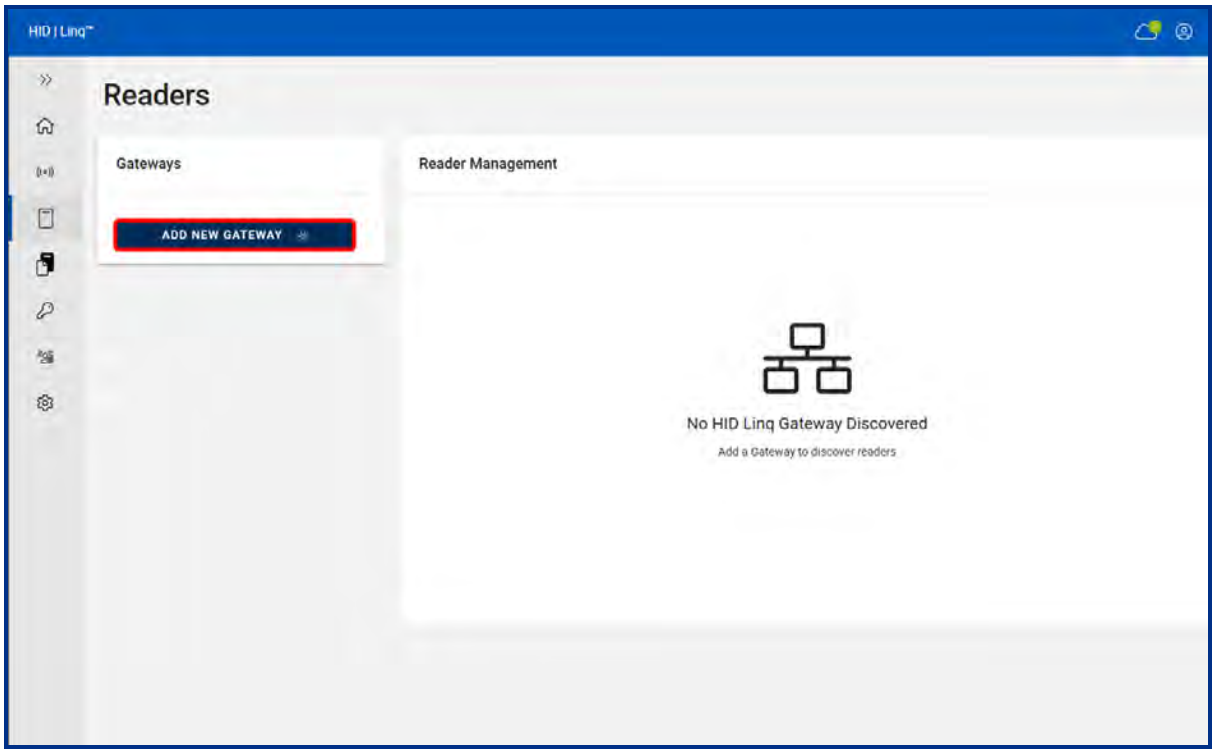
> **Note:** All computers on the network must have the HID Linq Gateway application installed. See **5.3 Install HID Linq Gateway** for more information.

For example:

- **User A** creates **Gateway 1**, **Gateway 2**, and **Gateway 3** in HID Linq On Premise on **Computer 1**. **User A** must only activate **Gateway 1** on **Computer 1**.
- **User B** must log in to HID Linq On Premise on **Computer 2**. Gateways **1**, **2** and **3** are visible. **User B** must only activate **Gateway 2** on **Computer 2**.
- **Gateway 3** must only be activated on **Computer 3** by **User C**.

To create a new gateway

1. Navigate to the **Readers** tab in the left-hand menu.
2. Click **ADD NEW GATEWAY**.



3. Enter a **Gateway Name**.
4. Click **CONNECT TO GATEWAY**.
5. Click **CONTINUE** to finish.

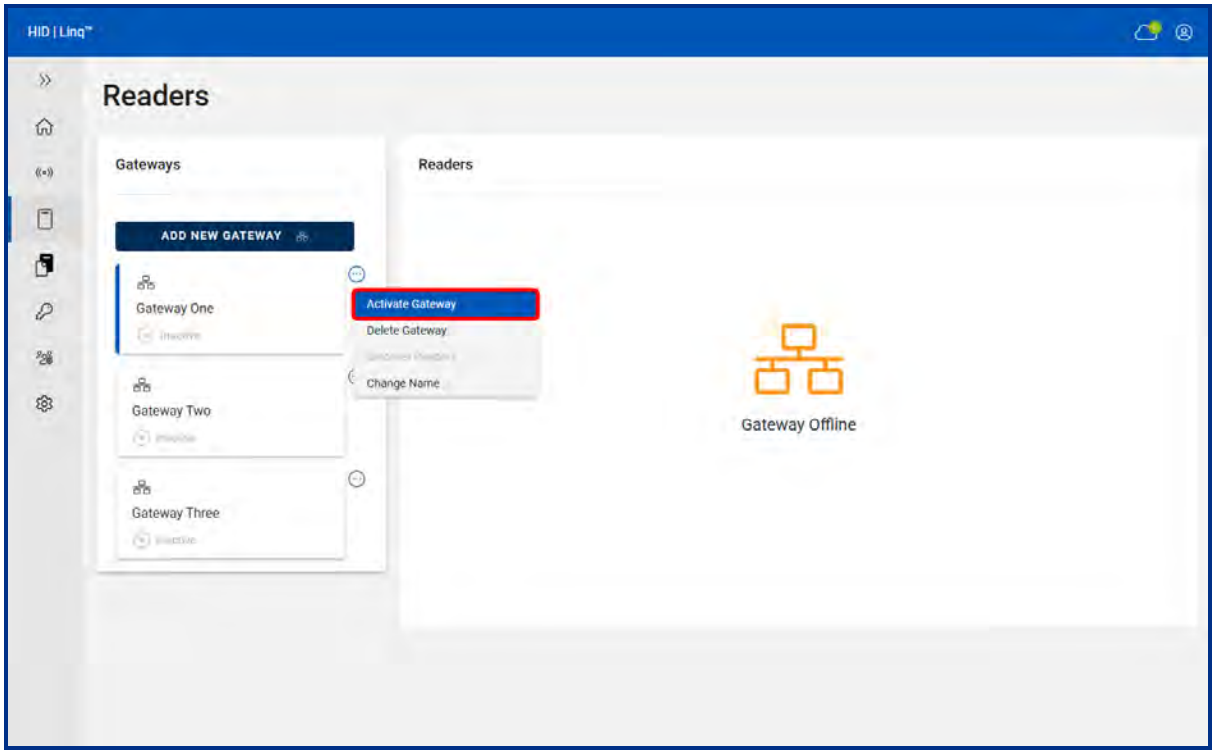
5.4.1 Activate a gateway

Activating a gateway starts the HID Linq Gateway application in the background of the current computer and allows you to connect that gateway to a computer. Activation is a one-time operation per computer.

> **Important: Only activate one gateway per computer on the server.**

To select an existing gateway:

1. Navigate to the **Readers** tab in the left-hand menu.
2. Click the ⋯ icon of the required gateway and click **Activate Gateway**.



3. Click **ACTIVATE GATEWAY**.
4. Click **OK** in both pop-up windows that are displayed.
5. Enter the HID Linq Gateway **Master password** and click **OK**.
6. Click **CONTINUE** to finish.

5.5 Connect gateway to IP address

The **Network** tab allows you to configure how the HID Linq Gateway connects to the server.

5.5.1 Hostname

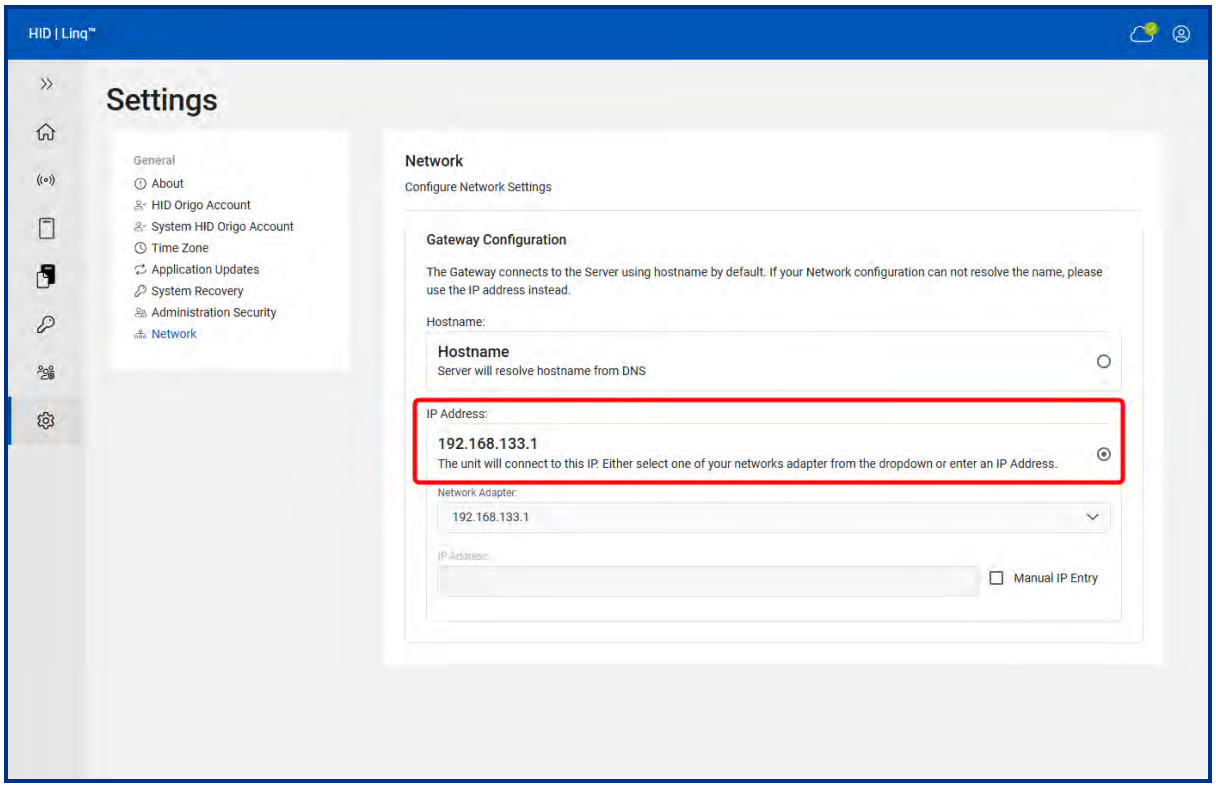
Select **Hostname** to connect the HID Linq Gateway to the server via a hostname, determined by DNS. The HID Linq Gateway is connected via a hostname by default.

5.5.2 IP Address

This allows you to use an IP address if the network does not support the use of a hostname.

> **Note:** The IP address must remain constant. Reserve the IP address only for this purpose.

1. Select **IP Address** to connect the HID Linq Gateway to the server via an IP address.



2. Select the required IP address from the **Network Adapter** drop-down list.

> **Note:** Alternatively, check the **Manual IP Entry** box and enter the required IP address.

5.6 Rename a Gateway

Note: The HID Linq Gateway is referenced by the host name of the machine it is downloaded on by default.

1. Navigate to the **Readers** tab in the left-hand menu.
2. Click the icon of the required gateway.
3. Click **Change Name**.
4. Enter the new gateway name.

   Note: Gateway names are limited to **letters**, **numbers**, **hyphens**, and **underscores**.
5. Click **SAVE**.

5.7 Port forwarding

HID Linq On Premise needs the following ports to be open:

Port	Reason
22	Connecting to HID Signo readers to push a firmware update.
443	Connecting via HTTPS.
8885	Connecting to Mercury controllers via MQTT. Only required on the PC that HID Linq Gateway is installed on.
9090	Communication between HID Linq On Premise and HID Linq Gateway.

Note: If you are running another service which uses the same ports, see **F.1 Port conflict troubleshooting**

5.8 Uninstall HID Linq Gateway

If you forget your HID Linq Gateway master password, you must uninstall HID Linq Gateway.

Important:
- If you are moving HID Linq On Premise to a different computer, navigate to the **C:\Program Files\HID Global\Linq Device Manager\database** folder and save the primary database files **HID_LINQSERVER.mdf** and **HID_LINQSERVER_log.ldf**, and the recovery key downloaded during installation.
- Navigate to **C:\ProgramData\HID Global\Linq Device Manager** and save the required local keystore files.

Follow the standard Windows uninstall process to remove HID Linq On Premise and HID Linq Gateway:

1. Open Windows **Add or remove programs**.
2. Select the app or program in the displayed list and select **Uninstall**.
3. Follow the on-screen instructions.
4. Once the above steps are complete, navigate to **C:\Program Files\HID Global** and delete the **Linq Device Manager** folder.
5. Navigate to **C:\ProgramData\HID Global** and delete the **Linq Device Manager** and **HID Linq™ Gateway** folders.

   Note: You may need to set Windows File Explorer to display hidden files to see and access the **Program Data** folder.

5.9 Delete a Gateway

1. Navigate to the **Readers** tab in the left-hand menu.
2. Click the icon of the required gateway.
3. Click **Delete Gateway**.
4. Click **DELETE**.

Section 06

Connect to HID Signo readers via HID Programming Stand

6.1 Overview

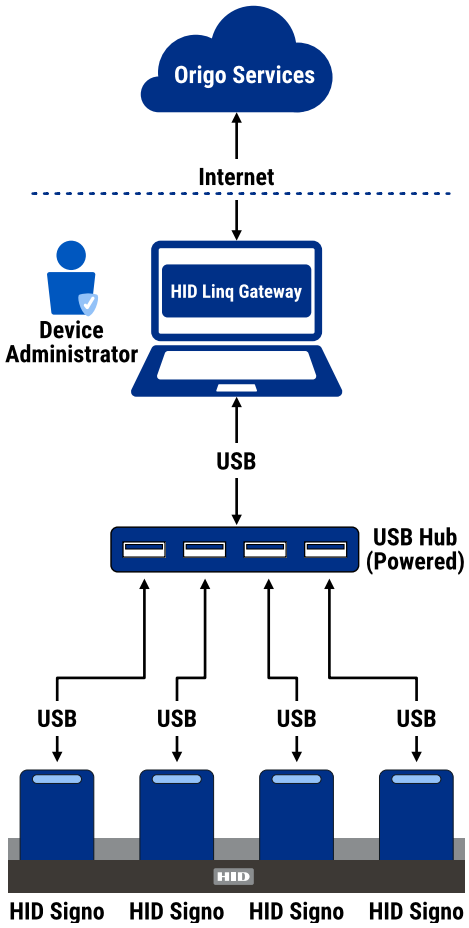
This section explains the required steps to connect a single, or multiple HID Signo readers to the PC using the HID Signo Programming Stand allowing the system installer to configure the reader(s) on a bench before installation.

Note:
- The maximum recommended number of readers per hub is four. The maximum recommended number of hubs per PC is two.
- It is recommended to use a powered USB hub for optimal connectivity.
- Local Configuration updates via USB do not require a HID Origo connection.

In summary, the following steps need to be taken:

1. Disconnect the power supply from the reader(s).
2. Plug a HID Signo Provisioning Accessory into each reader.
3. Place the reader(s) on the HID Signo Gang Stand.
4. Connect each reader to a powered USB hub (not supplied).
5. Connect the serial cable to the serial adapter module.
6. Connect the USB hub to a spare USB port on your PC.

Caution: When connecting the reader via USB-C, **DO NOT** connect the reader to an external power source.



6.2 Connect to HID Signo readers via the HID Signo Programming Stand

WARNING: DO NOT CONNECT THE ADAPTER OR CABLE WHILE THE READER IS POWERED ON.

Note: For more information, including images, refer to the *HID Signo Programming Stand Install Guide* (PLT-07195).

Who can connect HID Signo readers to the HID Signo Programming Stand?

	Reader Manager Portal Administrator	Reader Technician
Permission	Yes	Yes
Multiple reader capability	Yes	Yes

To connect HID Signo readers via the HID Signo Programming Stand:

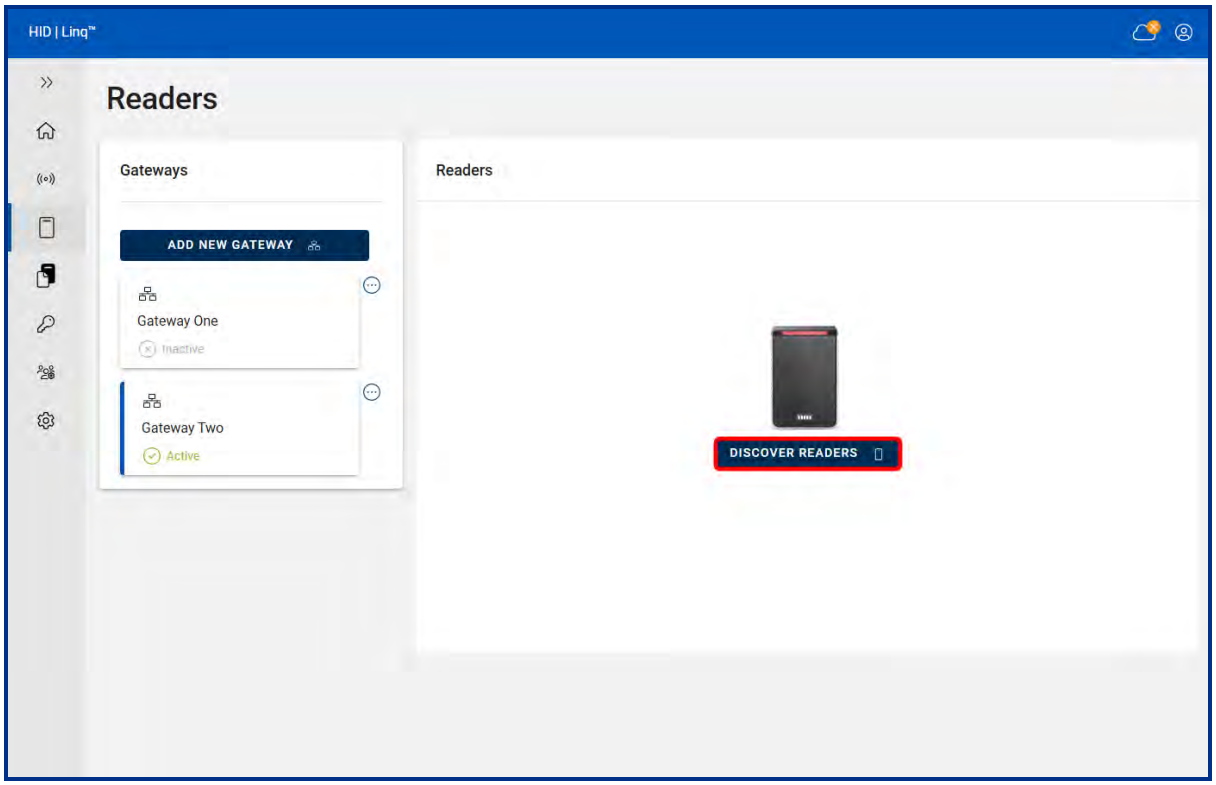
1. Disconnect the power supply from the HID Signo reader(s).
2. Remove the grommet from the back of the HID Signo reader(s) to access the adapter port.

   Note: Keep the grommet(s) in a safe place as each must be replaced following the removal of the Signo Provisioning Accessory.
3. Connect each Signo Provisioning Accessory.
4. Place the HID Signo reader(s) on the Signo Programming Stand.

   Note:
   - If the reader is fitted with a mounting plate, remove the mounting plate before placing the reader on the stand.
   - For readers with a pluggable pigtail, remove the pigtail before placing the reader on the stand.
   - For readers with a non-removable pigtail, to prevent short circuits ensure that the wires are separated before inserting the Signo Provisioning Accessory and applying power via the USB-C.
5. Insert a USB-C to USB-A cable (not supplied) into each Signo Provisioning Accessory.
6. Insert each USB-C to USB-A cable into the powered USB hub.
7. Connect the USB hub to a spare USB port on your PC.
8. Connect the USB hub to a 12 VDC power supply.

   Caution: When connecting the reader via USB-C, **DO NOT** connect the reader directly to an external power source.
9. In HID Linq On Premise, navigate to the **Readers** tab and connect to the required Gateway.

10. Click **DISCOVER READERS** to confirm it is visible.



6.3 Disconnect HID Signo reader(s)

> **Note:** For more information, including images, refer to the *HID Signo Programming Stand Install Guide* (PLT-07195).

1. Power off the USB hub.
2. Disconnect the USB-C cable from each Signo Provisioning Accessory.
3. Remove the Signo Provisioning Accessory module from each HID Signo reader adapter port.

   > **Note:** Carefully use a flat head screwdriver to release the Signo Provisioning Accessory.
4. Re-insert the grommet into the adapter port on the back of each HID Signo reader.

> **Important: Failure to replace the grommet correctly will void the IP rating for the reader.**

Section 07

Connect to HID Signo readers via HID controllers

7.1 Connect to a controller

This section explains the required steps to set up a HID Mercury LP controller to enable communication with HID Linq. HID Mercury MP series controllers and HID Aero controllers are compatible with HID Linq Cloud and the process to connect them is the same. For images of the HID Mercury and HID Aero controller DIP switches, please see **B.2 HID Controller DIP switches**.

Note:

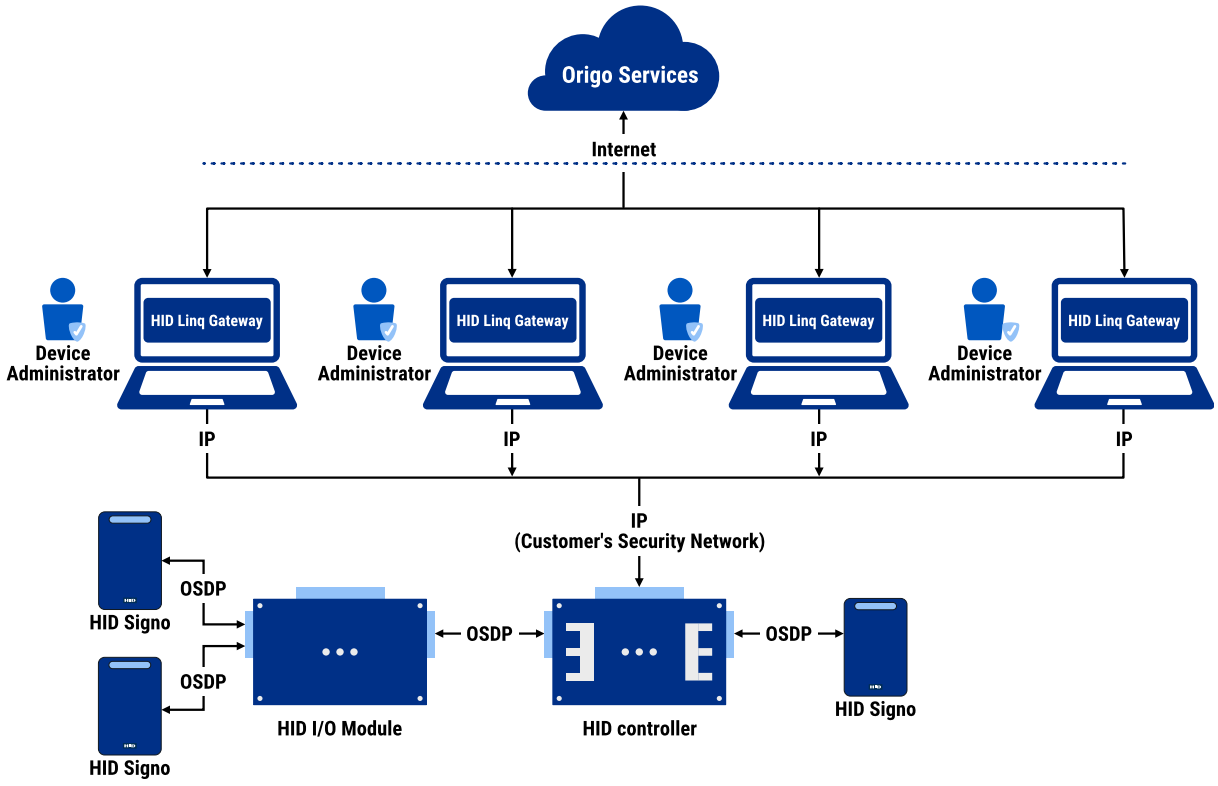
- HID Linq Gateway and the controller must be on the same network. Perform a ping to make sure the PC can see the Mercury panel. HID Linq Gateway can discover and communicate with a HID controller in the same network that your access control solution is deployed.
- HID Linq Gateway must be able to reach HID Linq On Premise services over the network.
- Select up to a maximum of 8 readers connected per HID controller.
- There is no limit to the recommended number of controllers per PC.
- Each controller is limited to a single gateway.
- Rediscover readers after applying a configuration or a factory configuration reset.

Important:

- If the controller and reader use different power sources, make sure that both are grounded by connecting them together.
- A HID Origo connection is required for configuration updates via controller.

In summary, the following steps need to be taken:

1. Use HID Linq Gateway Manager to discover the controller on your local network.
2. Generate a secure certificate in HID Linq On Premise.
3. Upload the certificate to the controller via the web configuration page.
4. Configure the HID Linq MQTT broker.



7.2 Connect a controller to HID Linq On Premise

This is a single operation per controller to establish a connection. Once completed, any HID Signo readers connected to the controller via OSDP V2 will be available in HID Linq On Premise, allowing remote configuration of operational readers at a customer's site.

Note:
- Reader Technicians with physical access to the controller, and Reader Technicians connected via a common HID Linq Gateway, can configure the readers connected to a controller.
- HID Linq On Premise only supports OSDP V2 connection.
- HID Linq On Premise does not support two readers on the same OSDP bus (multi-drop OSDP connection).

Who can connect a controller to HID Linq On Premise?

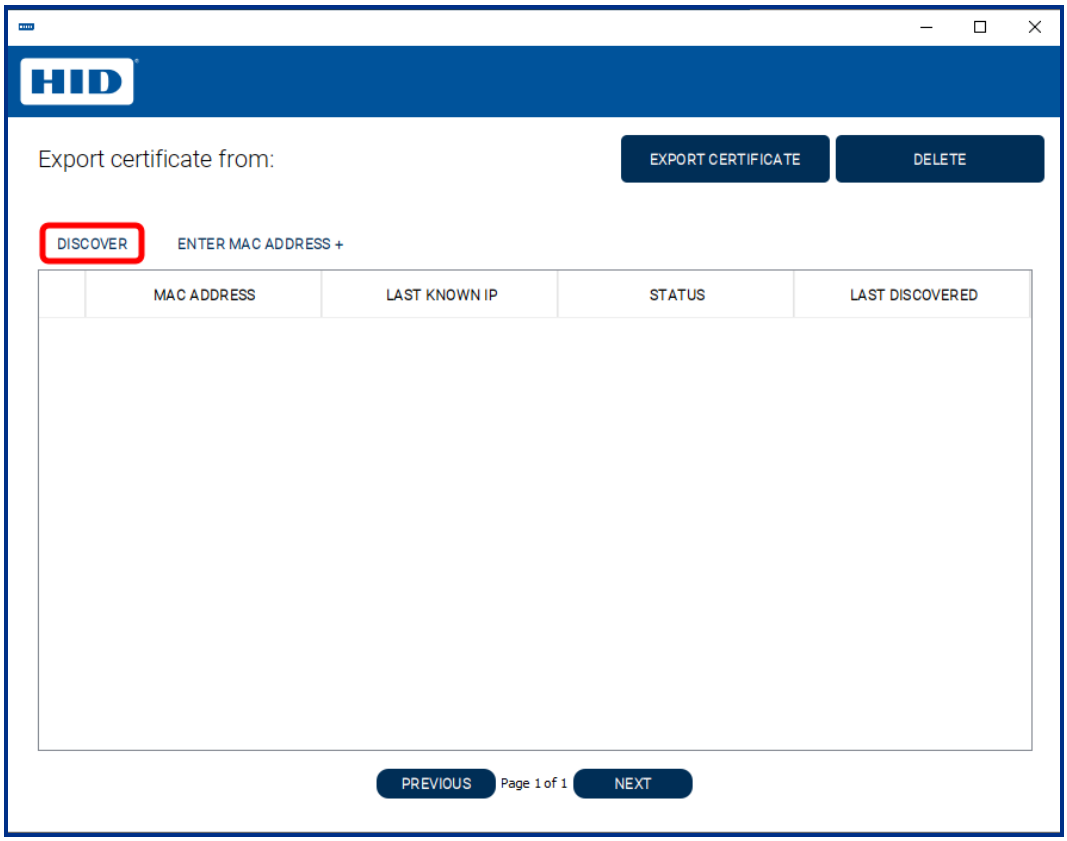
	Reader Manager Portal Administrator	Reader Technician
Permission	Yes	Yes
Multiple reader capability	Yes	Yes

7.2.1 Generate a secure certificate

1. Exit HID Linq Gateway in the Windows server tray.
2. Navigate to **C:\Program Files\HID Global\Linq™ Gateway\1.3.0.6**.
3. Double-click **Configuration.exe** to launch HID Linq Gateway Manager.
4. If HID Linq Gateway is in the **Normal** security profile, enter the master password.
5. Click **Manage HID Mercury panels**. The welcome screen is displayed with a summary of the steps required.
6. Click **BEGIN** to continue.

7. Click **DISCOVER**. HID Linq Gateway Manager will scan the network using mDNS and display any compatible controllers found.

> **Note:** Alternatively, click **ENTER MAC ADDRESS+** and directly enter the MAC address, if known. Click **Add Controller** to confirm.



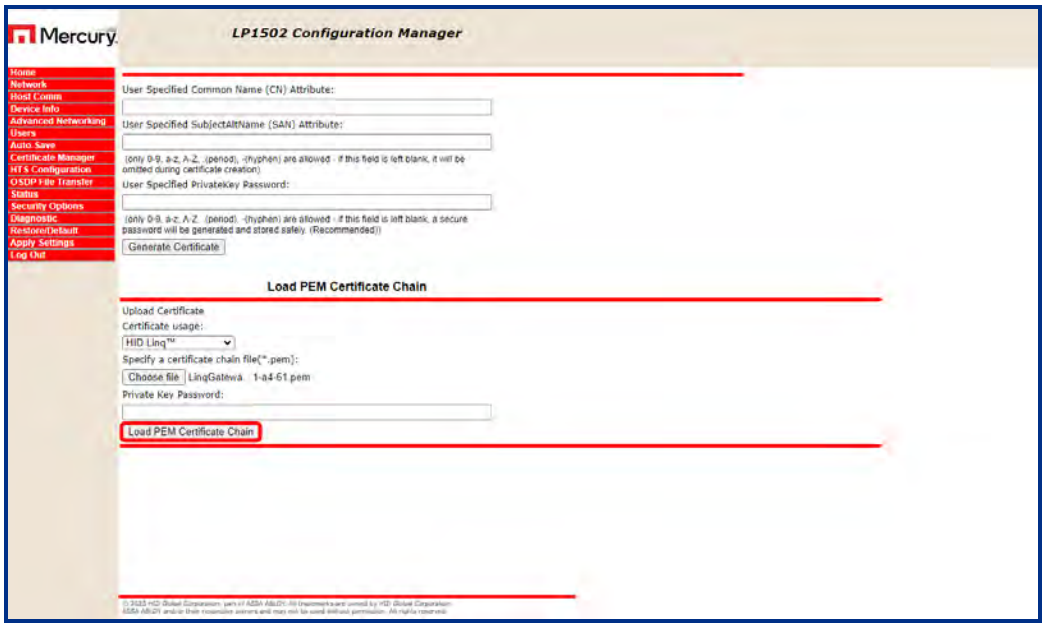
8. Check the box of the required controller and click **EXPORT CERTIFICATE**. This will generate a **.PEM** secure certificate.
9. Click **DOWNLOAD ZIP** to download it to your PC.

> **Note:** Extract the Zip file once it has downloaded.

7.2.2 Upload the secure certificate to the controller

1. Search the IP address of the controller in your web browser.
2. Log in to the panel.

   Note:
   - The default credentials are **admin**/**password**.
   - You may be required to toggle DIP Switch 1. See **7.2.3 Prepare the controller** for more information.
3. Navigate to **Certificate Manager** in the left-hand menu.
4. Under the **Load PEM Certificate Chain** section, click the **Certificate Usage** drop-down menu and select **HID Linq™**.
5. Click **Choose File** and navigate to the location of the **.PEM** secure certificate downloaded in **7.2.1 Generate a secure certificate**.
6. Click **Load PEM Certificate Chain**.



   Note: Once loaded, the **Certificate Information** is displayed.
7. Navigate to **HTS Configuration** in the left-hand menu and add the following HID Linq Gateway information in the **HID Linq™ Configuration** section:

Field	Enter
Connection String	The IP address of the PC running your HID Linq Gateway, and the default port number 8885. For example ssl://193.186.0.123:8885
Username	username
Password	password

8. Click **Configure HID Linq Client** to save. At this point, both HID Linq Gateway and the controller should have a trusted communication channel set up. It should now be possible to discover HID Signo readers connected to the controller via OSDP in HID Linq On Premise.

   Note: Repeat these steps for each connected controller.

7.2.3 Prepare the controller

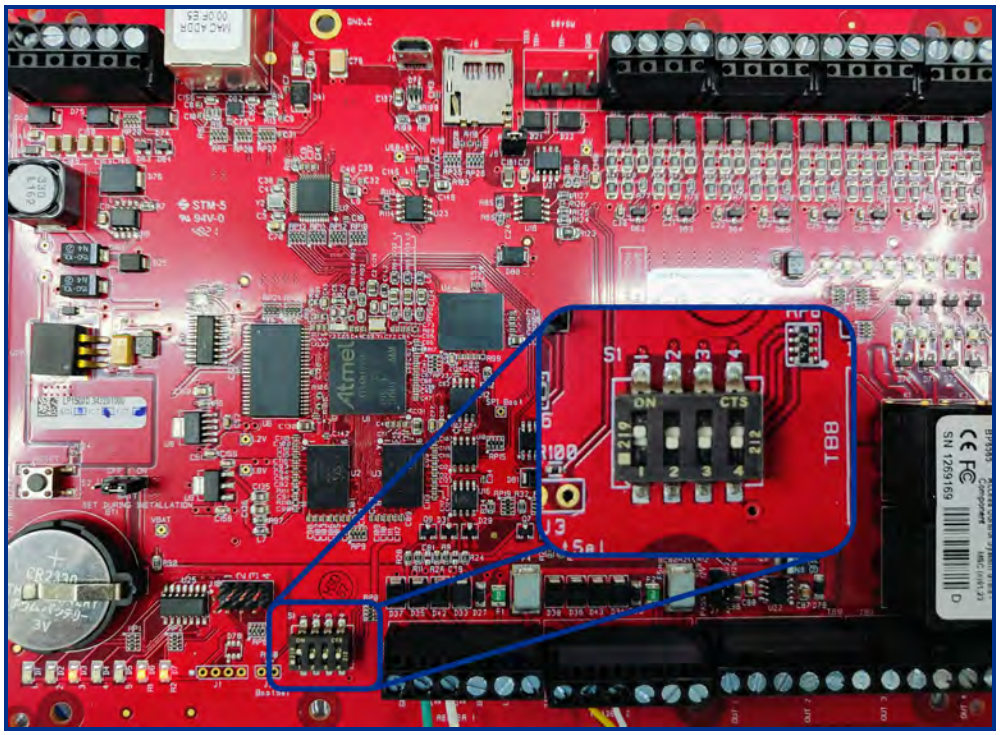
Caution: Firmware upgrade via controllers is not currently supported.

Important:
- When using an LP1502 panel, jumper switch J7 must be set to **PASS** when the input voltage is 12 VDC.
- When using a MR52-S3 SIO board, jumper switch J1 must be set to **Passed Through (PT)** when the input voltage is 12 VDC.
- If the input voltage (VIN) is greater than 20 VDC, switch both J7 and J1 to **12V**. Failure to do so may result in damage to the reader.
- See **B.1 Corresponding HID controller manuals** for the relevant HID Linq On Premise Mercury control panel installation and specification manuals for more information.

1. Open a web browser and navigate to the IP address of the controller.
2. When prompted, log in using your credentials.

   Note:
   The default credentials for Mercury controllers are:
   - Username: **admin**
   - Password: **password**

   If the default credentials do not work, toggle the **S1: DIP Switch 1** to **OFF** and **ON**.
3. To prove that you have physical access to the controller and are not attempting to access the device from a remote location, set the **S1: DIP Switch 1** to the following sequence:
   - **On** - **Off** - **Off** - **Off**

   Note: For alternative controller dip switch locations, see **1.1 HID Controller DIP switches**.
4. The controller is now ready to receive the secure certificate.

Section 08

Reader discovery

8.1 Reader discovery

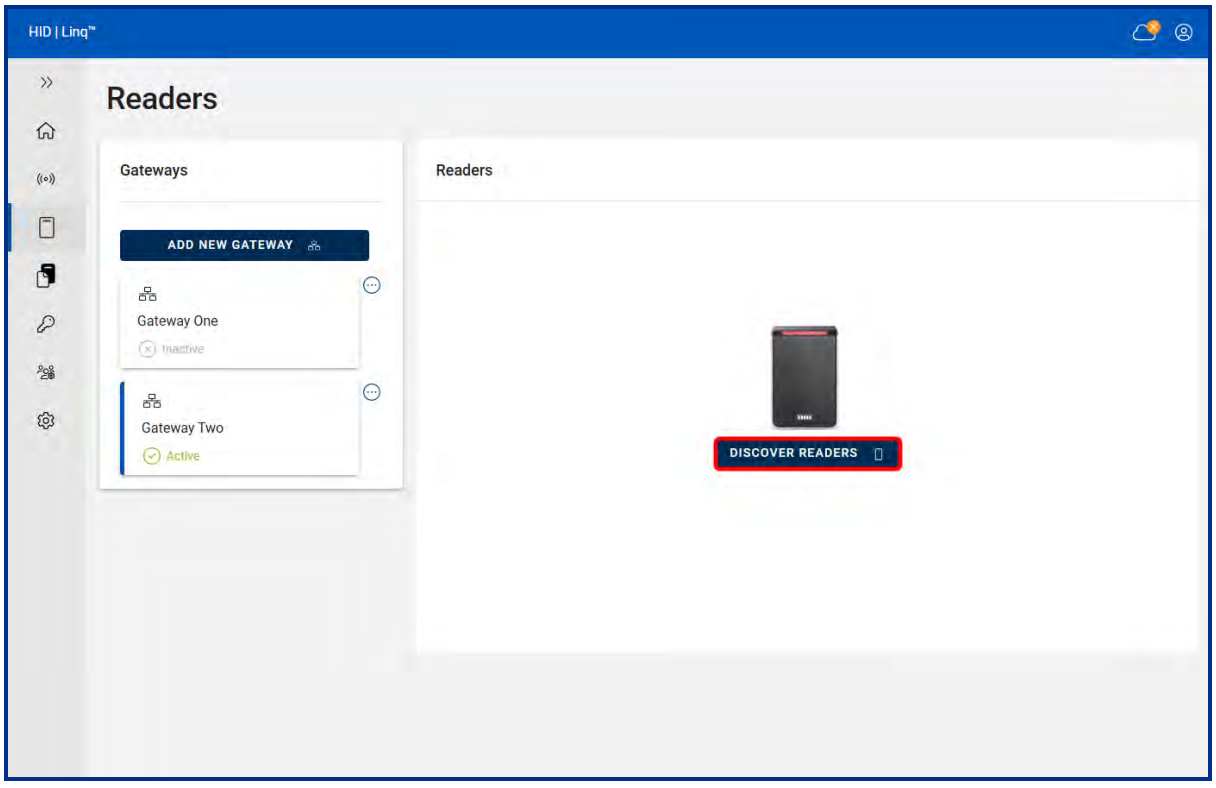
Discover the readers connected to your HID Linq Gateway to manage them.

Who can discover a reader?

	Reader Manager Portal Administrator	Reader Technician
Permission	Yes	Yes
Multiple reader capability	N/A	N/A

Note:
- It is recommended to perform a reader discovery every time a reader is physically connected or disconnected.
- It is recommended to perform a reader discovery after updating the reader firmware or configuration.
- It is recommended to perform a reader discovery after a period of inactivity or if your machine is powered off at any time.

1. Navigate to the **Readers** tab in the left-hand menu.
2. Select the required HID Linq Gateway.
3. Click **DISCOVER READERS**.



Note: The list of readers connected to the required gateway is displayed. Click the ⋯ icon of the required gateway and select **Discover Readers** to refresh the list of readers.

8.2 Locate a connected reader

The locate reader function allows you to physically locate a reader. With multiple readers connected via the HID Signo Provisioning Accessory, or readers installed on the premises, you can individually identify a specific reader before performing a firmware update, applying a Configuration ID, or resetting the reader to its default configuration settings.

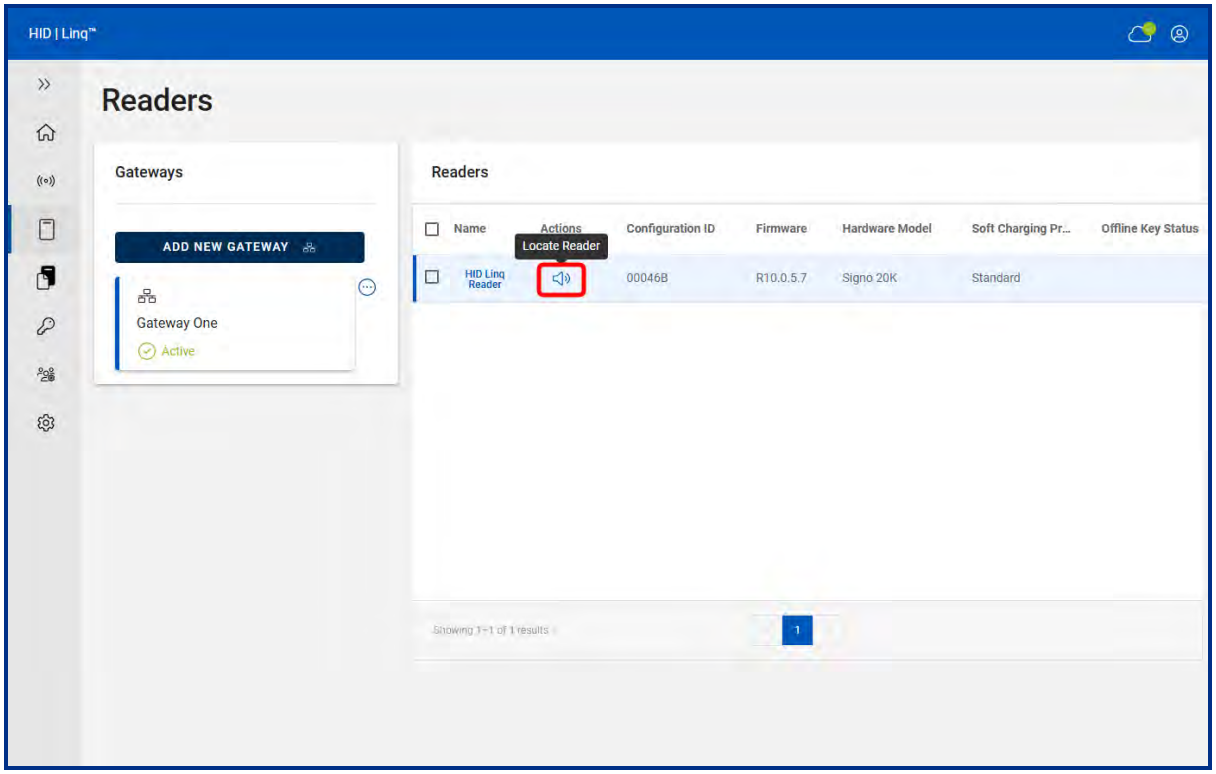
Who can locate a connected reader?

	Reader Manager Portal Administrator	Reader Technician
Permission	Yes	Yes
Multiple reader capability	No	No

There are two ways to locate a connected reader:

Reader list view

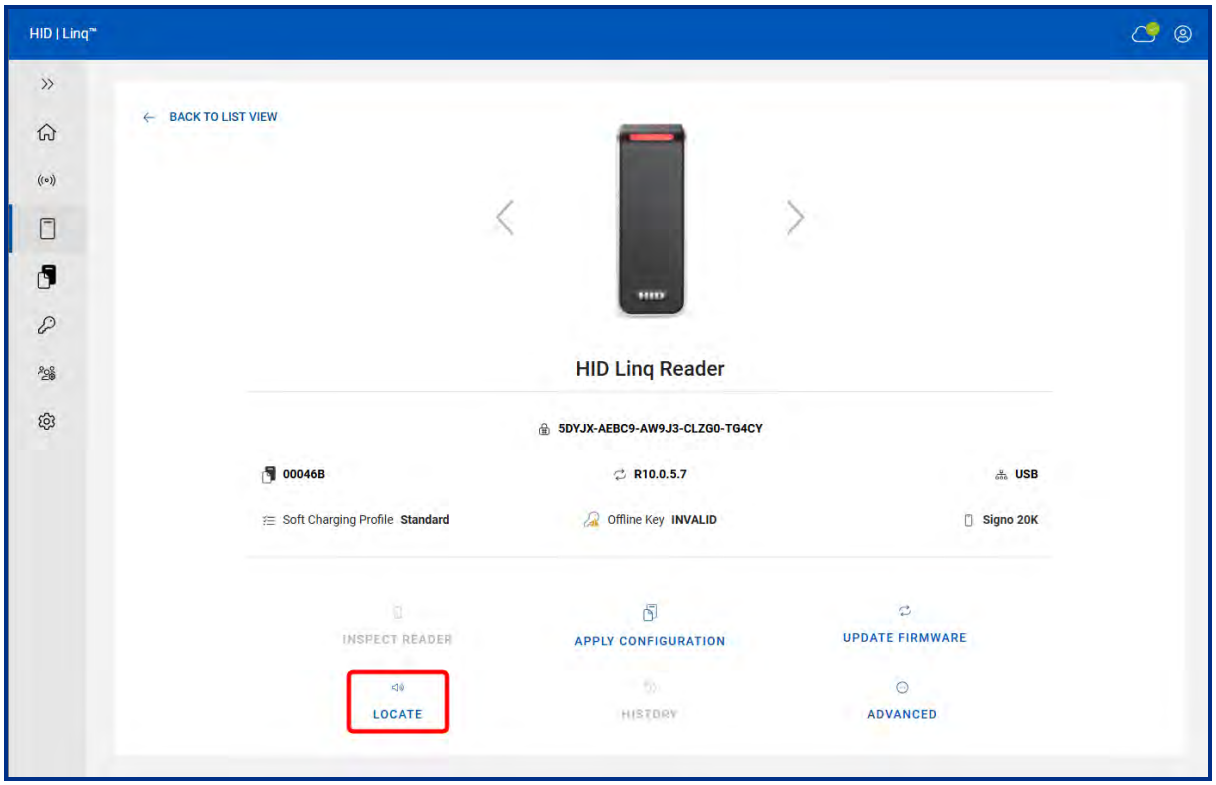
1. Navigate to the **Readers** tab in the left-hand menu.
2. Select the required HID Linq Gateway.
3. Click on the required reader in the reader list.



Note: The reader will emit an audible beep, and the LED will flash green.

Carousel view

1. Navigate to the **Readers** tab in the left-hand menu.
2. Select the required HID Linq Gateway.
3. Click the name of the required reader.
4. Click **LOCATE**.



Note: The reader will emit an audible beep, and the LED will flash green.

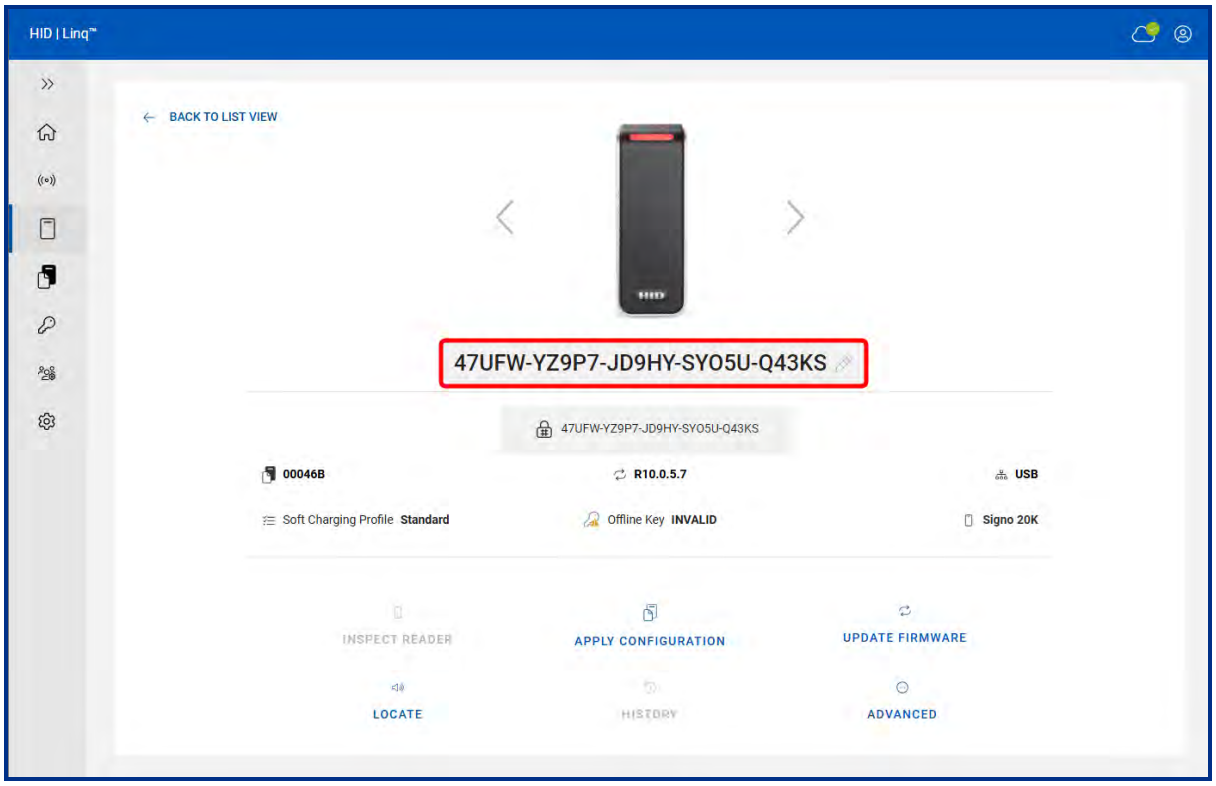
8.3 Reader information

The reader carousel view allows you to view information about the reader:

- Reader name (Default reader UUID)
- Current configuration ID
- Current firmware version
- Connection method
- Soft Charging profile
- Offline Key status
- Reader model

To change the reader name from the default to a user-friendly name:

1. Navigate to the **Readers** tab in the left-hand menu.
2. Select the required reader.
3. Click on the reader name.



4. Enter a friendly name.
5. Click **SAVE**.

Section 9

Keystore

9.1 Keystore

Keystores allow you to use keys online via HID Origo Cloud, or offline via the HID Custom Keystore in HID Linq On Premise.

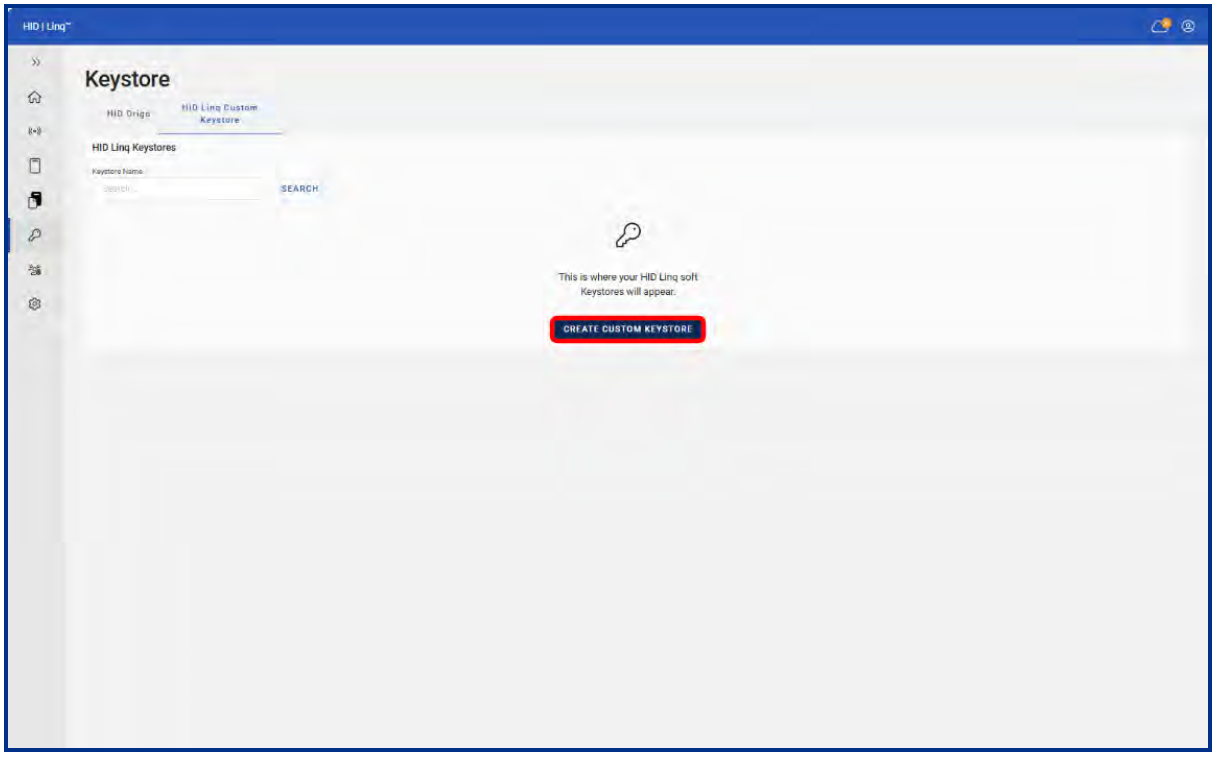
> **Note:**
> - The keystore is only available to System Administrators
> - HID Linq On Premises supports up to 500 keystores, or until only 1 GB of storage remains

HID Custom Keystores allow you to securely store and access keys in the HID Linq On Premise application to perform reader configurations offline. It allows you to store the following:

- OEM SNMP keys to manage HID Signo readers offline
- Custom credential keys for use with:
  - MIFARE/DESFire EV1, EV2 and EV3
  - Seos®
  - iCLASS® and iCLASS SE™

9.2 Create local keystore

1. Navigate to the **Keystore** in the left-hand menu.
2. Click the **HID Linq Custom Keystore** tab.
3. Click **CREATE CUSTOM KEYSTORE**.



4. Enter the keystore name and password and click **PROCEED**.

> **Note:** Passwords must be at least 12 characters.

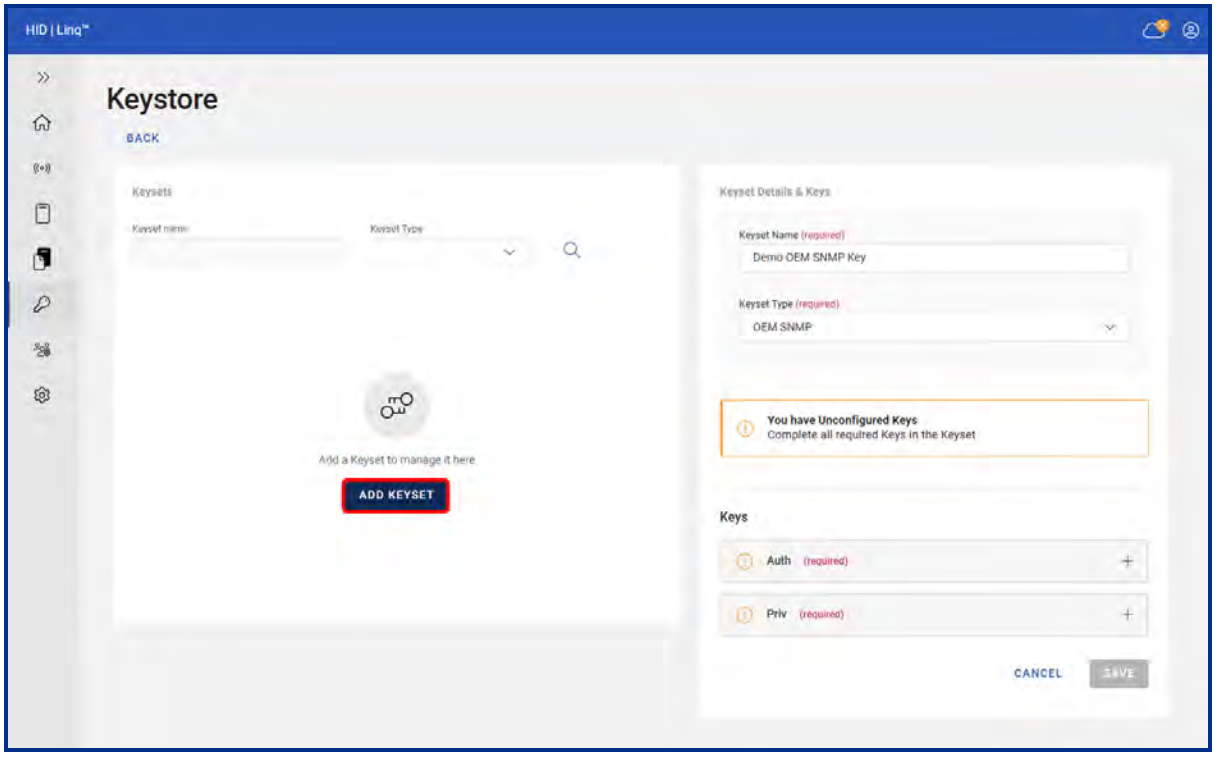
> **Important: Make a note of your password and safely store it. If you forget your password, you will lose access to that keystore.**

5. Click **DONE**.

9.2.1 Add an OEM SNMP key set

> **Important: Once a keyset is added, you can no longer see the key value. To edit the key, you must overwrite the existing key value.**

1. Navigate to the **Keystore** in the left-hand menu.
2. Click the **HID Linq Custom Keystore** tab.
3. Click **Open Keystore** of the required keystore.
4. Click **ADD KEYSET**.

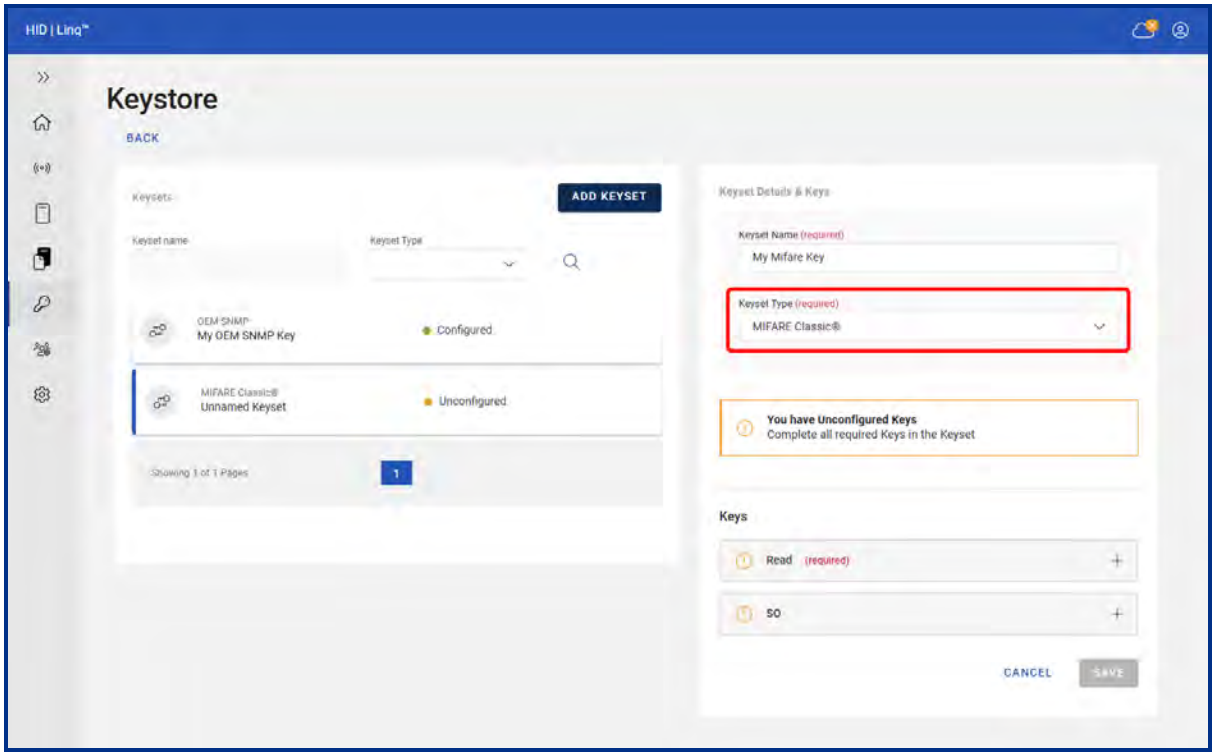


5. Enter the required **Keyset Name**.
6. Select **OEM SNMP** from the **Keyset Type** drop-down list.
7. Enter the required **Auth** key and **Priv** key values.
8. Click **SAVE**.
9. Enter the keystore password and click **SAVE**.

9.2.2 Add a MIFARE key set

Important: Once a keyset is added, you can no longer see the key value. To edit the key, you must overwrite the existing key value.

1. Navigate to the **Keystore** in the left-hand menu.
2. Click the **HID Linq Custom Keystore** tab.
3. Click **Open Keystore** of the required keystore.
4. Click **ADD KEYSET**.
5. Enter the required **Keyset Name**.
6. Select the required **MIFARE** keyset type from the **Keyset Type** drop-down list.



7. Enter the required **Read** key and **SO** values.

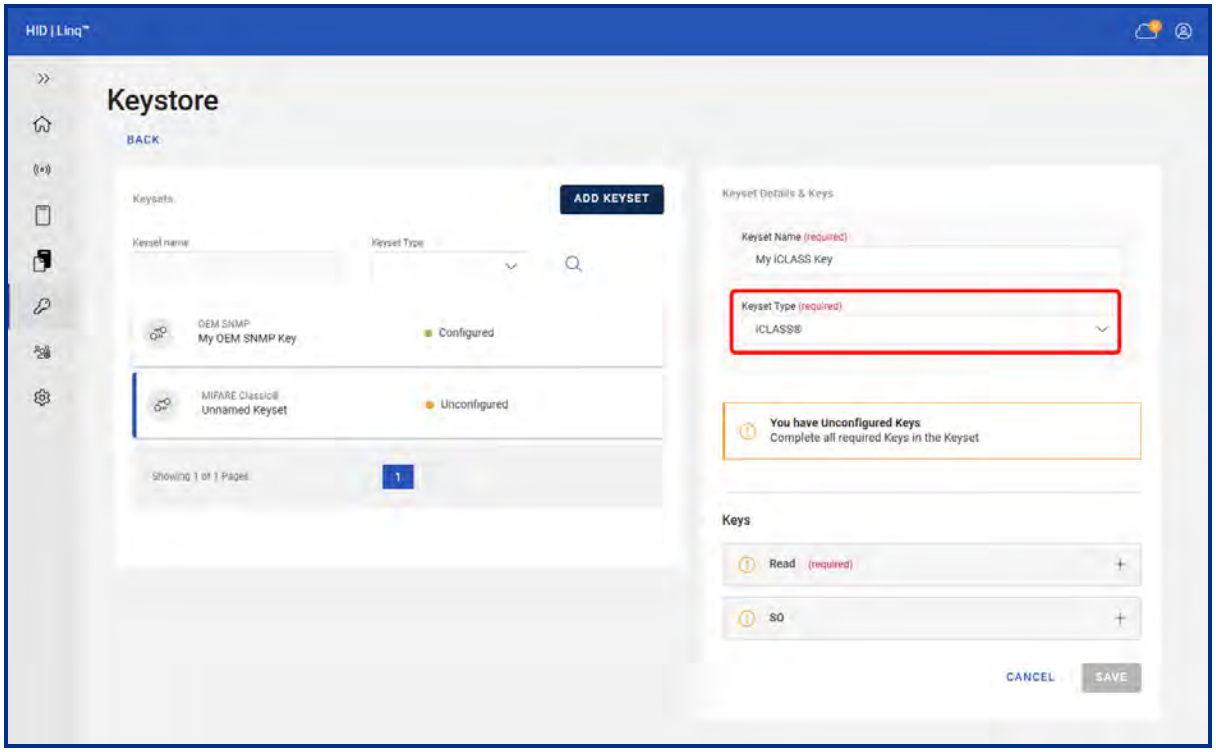
   Note: These key values are set when encrypting a card via CP1000 or third-party software.

8. Click **SAVE**.
9. Enter the keystore password and click **SAVE**.

9.2.3 Add iCLASS or iCLASS SE key set

Important: Once a keyset is added, you can no longer see the key value. To edit the key, you must overwrite the existing key value.

1. Navigate to the **Keystore** in the left-hand menu.
2. Click the **HID Linq Custom Keystore** tab.
3. Click **Open Keystore** of the required keystore.
4. Click **ADD KEYSET**.
5. Enter the required **Keyset Name**.
6. Select the required **iCLASS** or **iCLASS SE** keyset type from the **Keyset Type** drop-down list.



7. Enter the required **Read** key and **SO** values.

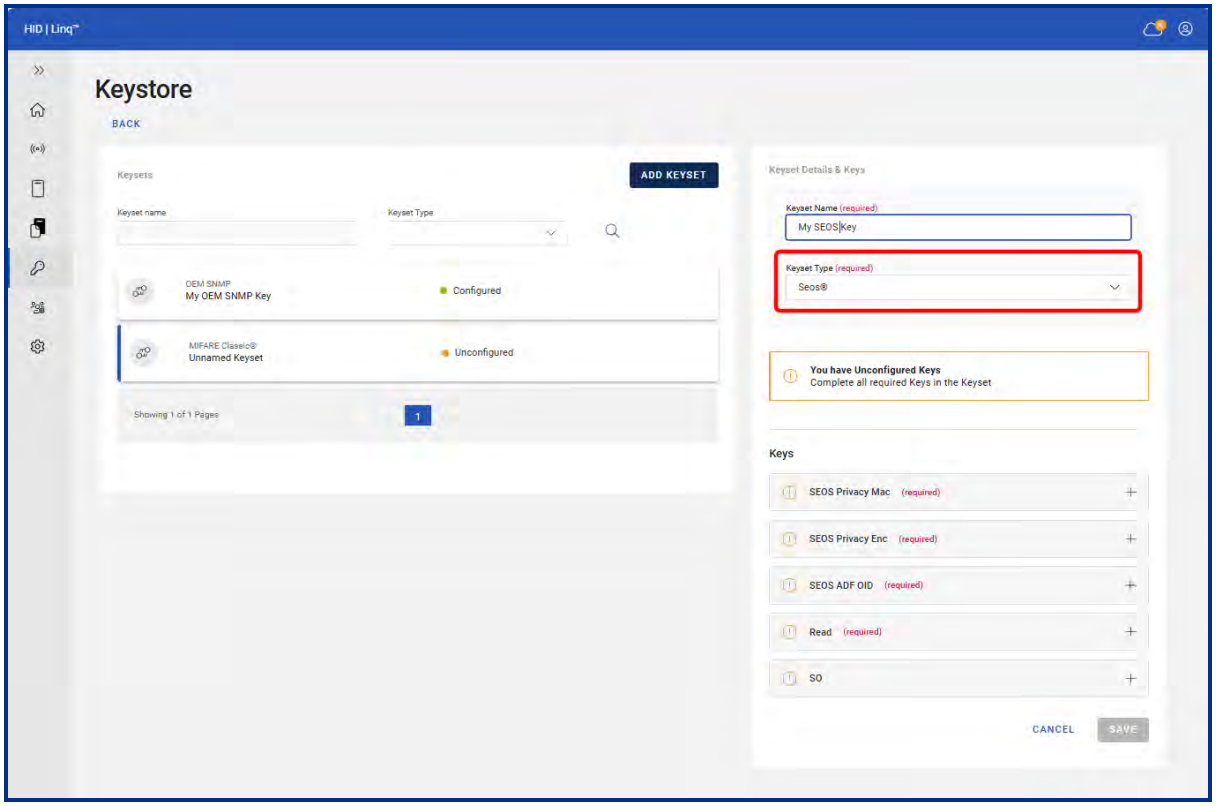
   Note: These key values are set when encrypting a card via CP1000 or third-party software.

8. Click **SAVE**.
9. Enter the keystore password and click **SAVE**.

9.2.4 Add Seos key set

Important: Once a keyset is added, you can no longer see the key value. To edit the key, you must overwrite the existing key value.

1. Navigate to the **Keystore** in the left-hand menu.
2. Click the **HID Linq Custom Keystore** tab.
3. Click **Open Keystore** of the required keystore.
4. Click **ADD KEYSET**.
5. Enter the required **Keyset Name**.
6. Select the required **Seos** keyset type from the **Keyset Type** drop-down list.



7. Enter the required keys for the keyset and the **SO** value.

   Note: These key values are set when encrypting a card via CP1000 or third-party software.

8. Click **SAVE**.
9. Enter the keystore password and click **SAVE**.

Section 10

Reader offline management

10.1 Overview

Enable the offline management of a HID Signo reader for offline mode use. Set your own OEM SNMP Admin key to confirm you are the owner of the reader for offline mode use.

Note: Only Signo readers configured for offline management are supported for offline use. Unprogrammed Signo readers are configured to support offline management from the factory.

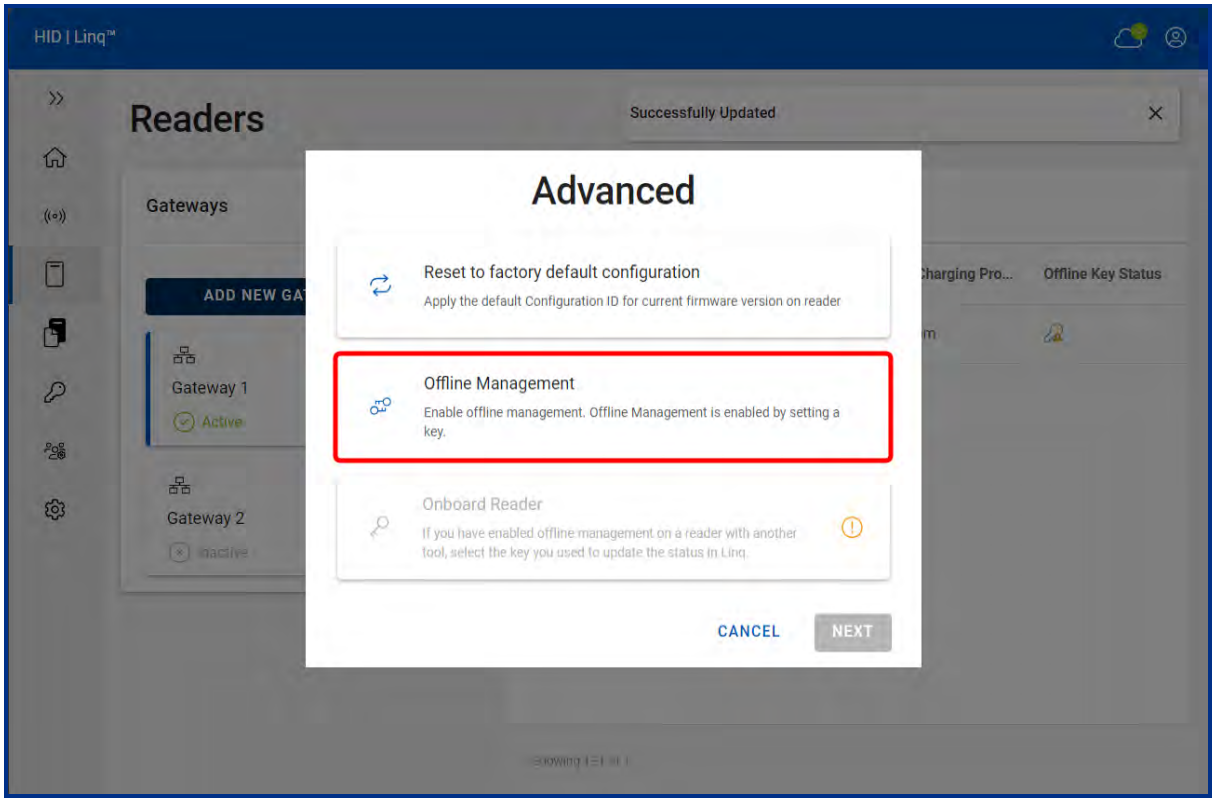
10.2 Set a key

Note:

- Add your OEM SNMP key to the HID Linq Custom Keystore before continuing. See **9.2.1 Add an OEM SNMP key set** for more information.
- The HID Signo reader firmware version must be 10.0.8.5 or newer.

Caution: Make a note of your SNMP and Media keys. These cannot be recovered by HID.

1. Navigate to the **Readers** tab in the left-hand menu.
2. Select the required HID Linq Gateway.
3. Check the box of the required reader(s).
4. Click **ADVANCED**.
5. Click **Offline Management**.



6. Click **NEXT**.
7. Select the required OEM SNMP key and click **APPLY**.

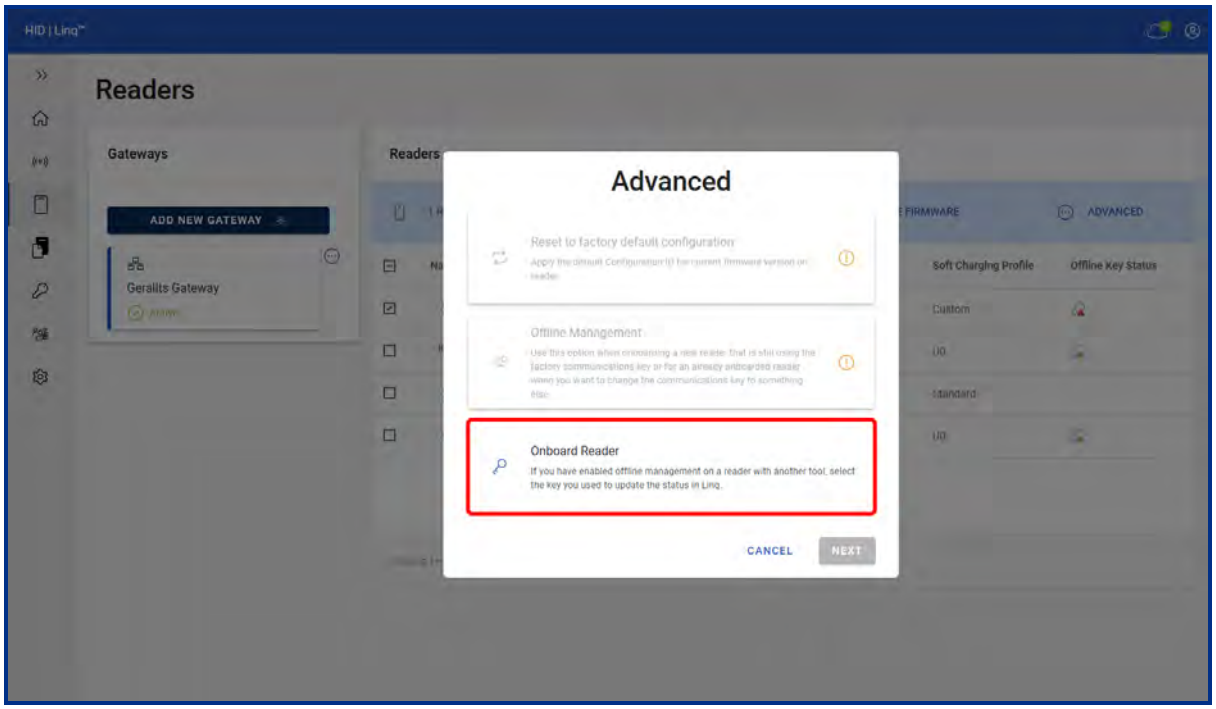
10.3 Roll a key

If the OEM SNMP is unknown or needs changing for business or security reasons:

Note:
- Add your OEM SNMP key to the HID Linq Custom Keystore before continuing. See **9.2.1 Add an OEM SNMP key set** for more information.
- The HID Signo reader firmware version must be 10.0.8.5 or newer.

Caution: Make a note of your SNMP and Media keys. These cannot be recovered by HID.

1. Navigate to the **Readers** tab in the left-hand menu.
2. Select the required HID Linq Gateway.
3. Check the box of the required reader(s).
4. Click **ADVANCED**.
5. Click **Onboard Reader**.



6. Click **NEXT**.
7. Select the required OEM SNMP key and click **APPLY**.

Section 11

Reader configuration

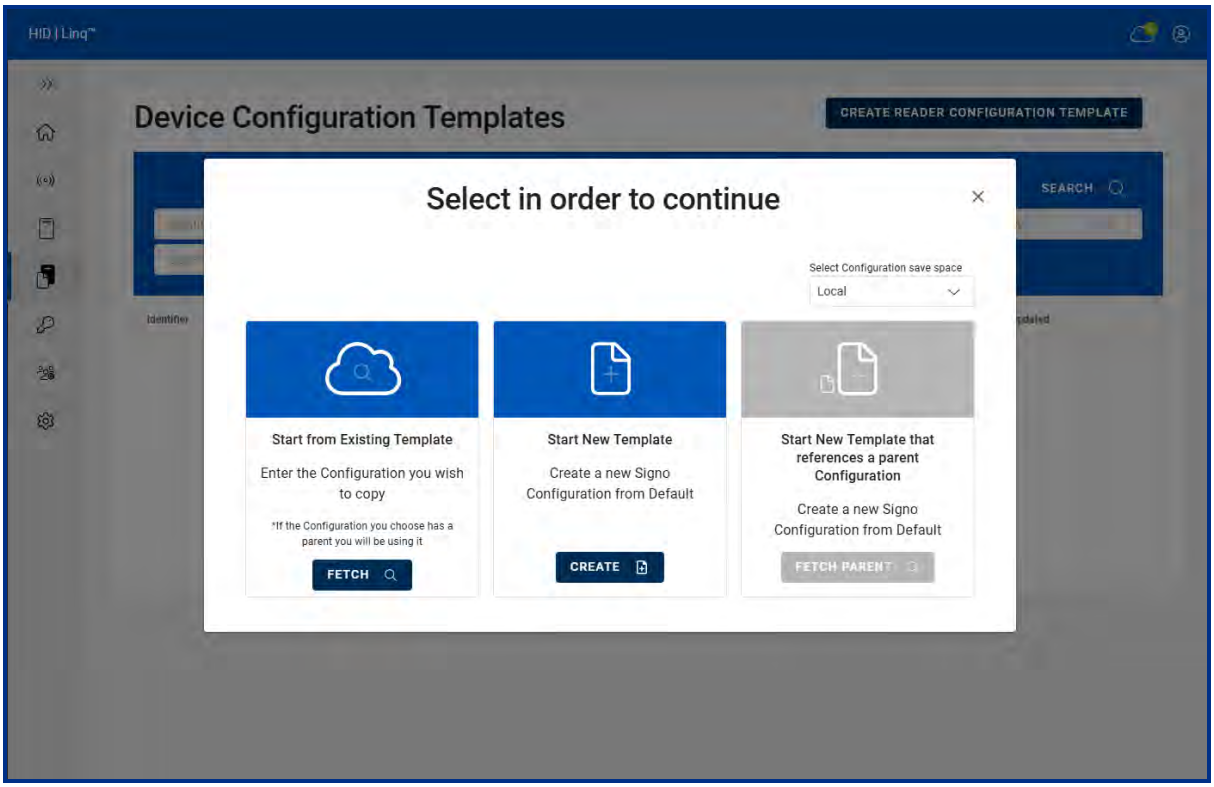
11.1 Create a Configuration ID

Creating a Configuration ID allows you to manage connected readers. Configuration IDs can be saved locally within HID Linq On Premise, or online in HID Origo.

There are three ways to create a Configuration ID:

- **Start from Existing Template**: copies an existing configuration and allows you to change certain parameters
- **Start New Template**: new configuration from the default settings of the reader
- **Start New Template that references a parent Configuration**: references a parent configuration to create a new configuration

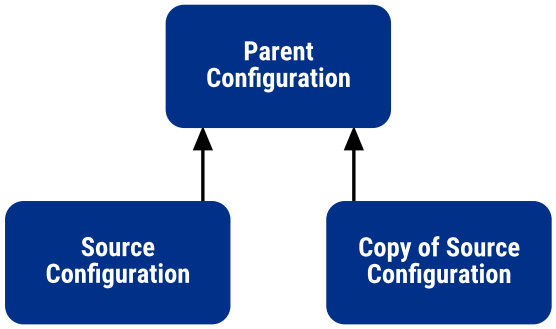
> **Note:** Only available with **Select Configuration save space** drop-down list set to **Origo**.



See **A.1 Configuration ID overview** for more information.

11.1.1 Start from an existing template

This allows you to copy an existing configuration template and make a new one with its properties. You can edit one or more properties without having to create a new template. Any inherited configurations are also copied.



1. Navigate to the **Device Configuration Templates** tab in the left-hand menu.
2. Click **CREATE READER CONFIGURATION TEMPLATE**.
3. Select where to save the configuration from the **Select Configuration save space** drop-down list.

   > **Note:** Configurations saved locally can only be applied to offline readers. See **10.2 Set a key**

4. Click **FETCH**.
5. Enter the required Configuration ID and click **FETCH**.
6. The **11.2 Configuration Editor** page is displayed.

11.1.2 Start New Template

This allows you to create a new Configuration ID template with no parent Configuration ID association.

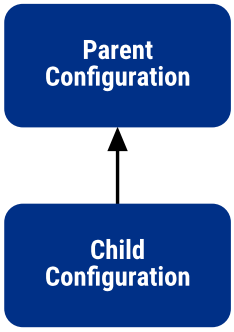
1. Navigate to the **Device Configuration Templates** tab in the left-hand menu.
2. Click **CREATE READER CONFIGURATION TEMPLATE**.
3. Select where to save the configuration from the **Select Configuration save space** drop-down list.

   > **Note:** Configurations saved locally can only be applied to offline readers. See **10.2 Set a key**

4. Click **CREATE**.
5. The **11.2 Configuration Editor** page is displayed.

11.1.3 Start New Template that references a parent Configuration

This allows you to create a new Configuration ID template by referencing a parent template saved in HID Origo. The new configuration ID inherits all properties of the parent configuration.



1. Navigate to the **Device Configuration Templates** tab in the left-hand menu.
2. Click **CREATE READER CONFIGURATION TEMPLATE**.
3. Select **Origo** from the **Select Configuration save space** drop-down list.

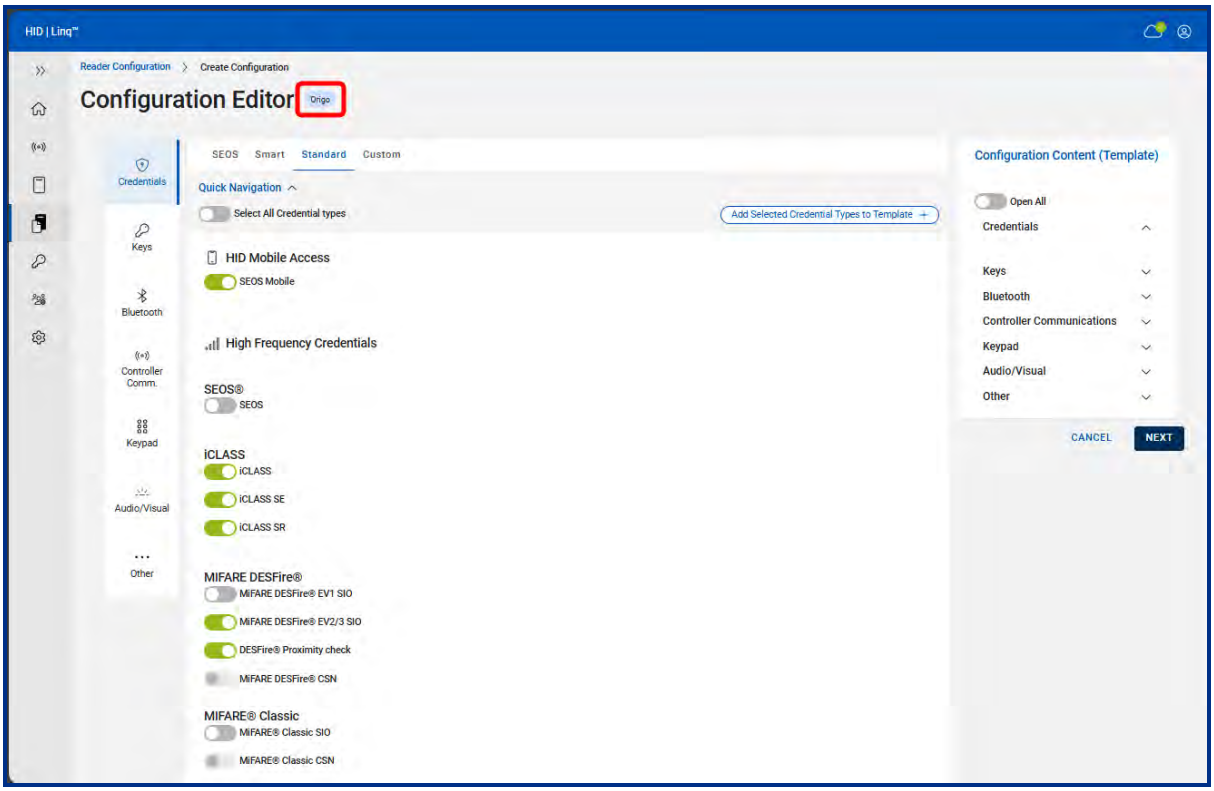
   > **Note: Start New Template that references a parent Configuration** is only available with **Origo** selected in the **Select Configuration save space** drop-down list.

4. Click **FETCH PARENT**.
5. Enter the required Configuration ID and click **FETCH**.
6. The **11.2 Configuration Editor** page is displayed.

11.2 Configuration Editor

The **Configuration Editor** page allows you to change the template properties when creating a new Configuration ID.

A **Local** or **Origo** icon is displayed to show where the configuration is being saved.



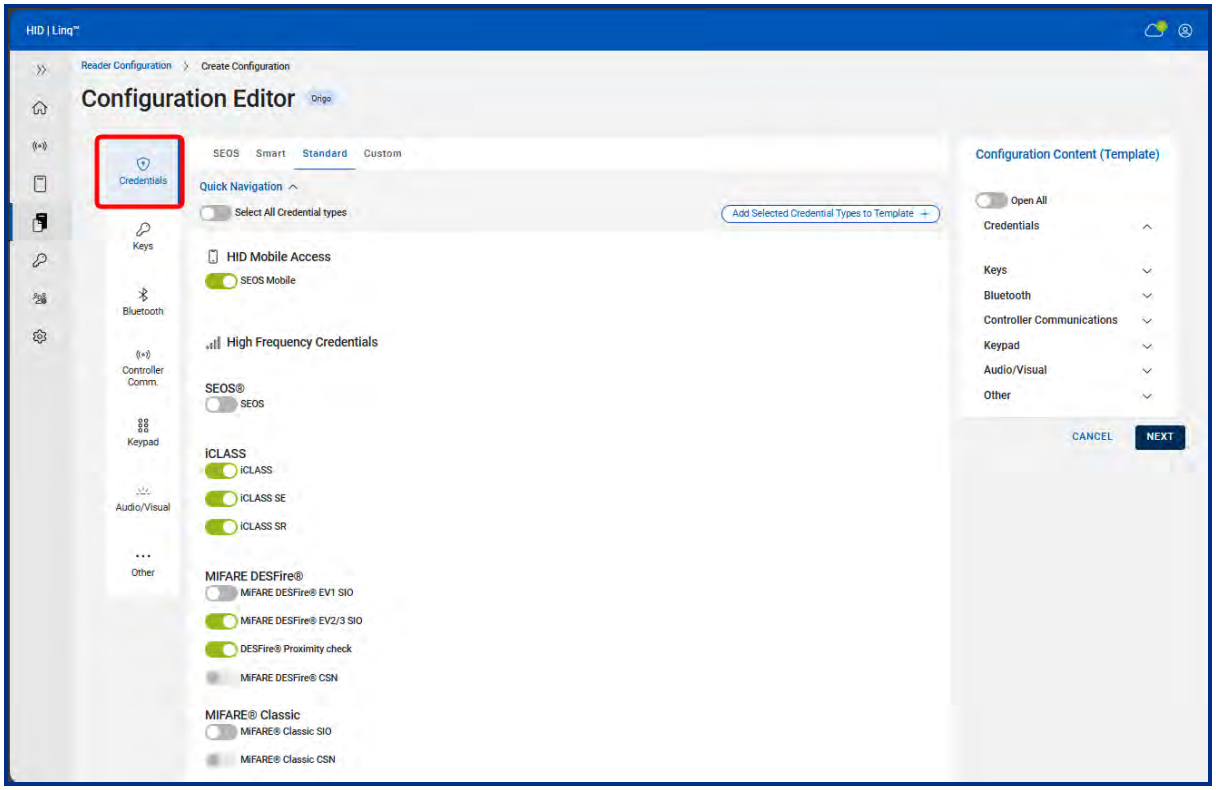
11.2.1 Online credential technology templates

Select the required credential types to enable them on your reader.

Important: All credential technologies are enabled when purchasing an unmodified reader from HID by default. Changing the credential technologies via a configuration overwrites the default settings. Only the credential technologies of the new configuration will be available. The enabled credentials can be changed at any time by applying a configuration to the reader.

Credentials	Soft Charge Profiles			
	SEOS	Smart	Standard	Custom
SEOS Mobile ID's	▪	▪	▪	▪
SEOS	▪	▪	▪	▪
iCLASS SE		▪	▪	▪
iCLASS SR		▪	▪	▪
iCLASS		▪	▪	▪
MIFARE, DESFire, EV1, EV2, EV3 - with SIO		▪	▪	▪
MIFARE Classic with SIO		▪	▪	▪
MIFARE Classic CSN			▪	▪
MIFARE, DESFire, EV1, EV2, EV3 - with Custom Data (Datamapper)				▪
MIFARE Classic with Custom Data				▪
FELICA IDM				▪
DEPAS				▪
125 kHz Proximity			▪	▪
125 kHz Indala Proximity			▪	▪
125 kHz EM4102 Proximity			▪	▪

1. Navigate to the **Credentials** tab.



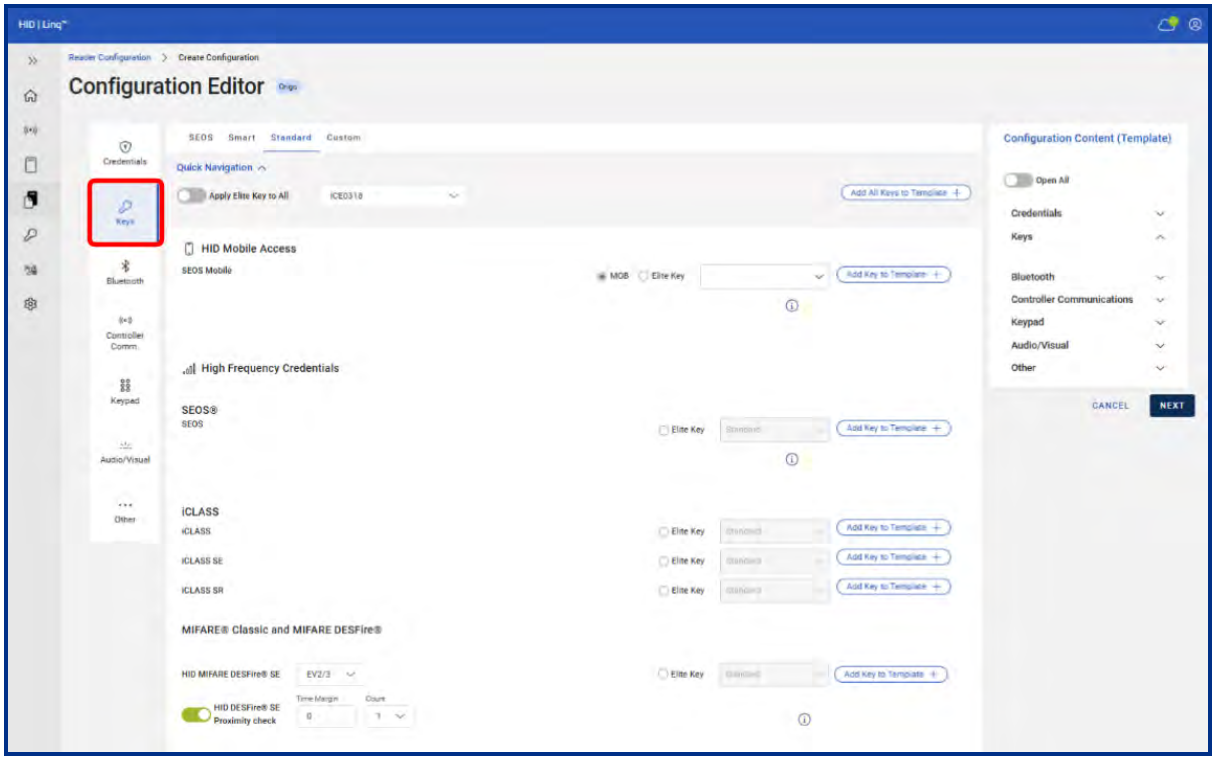
2. Click the required soft charge profile tab.
   - SEOS
   - Smart
   - Standard
   - Custom
3. Click the toggles to enable or disable the required parameters.
4. Click **Add Selected Credential Types to Template** for the required credentials.

> **Note:** Use the **Quick Navigation** toggle to enable or disable all credential types.

11.3 Online key configuration

Select the required HID Origo stored keys to add to the configuration template. See **11.2.1 Online credential technology templates** for the supported online credentials.

1. Navigate to the **Keys** tab.



> **Note:** Click the Information icon to manage your enabled wallet technologies.

2. Click **Add Key to Template** for the required credentials.

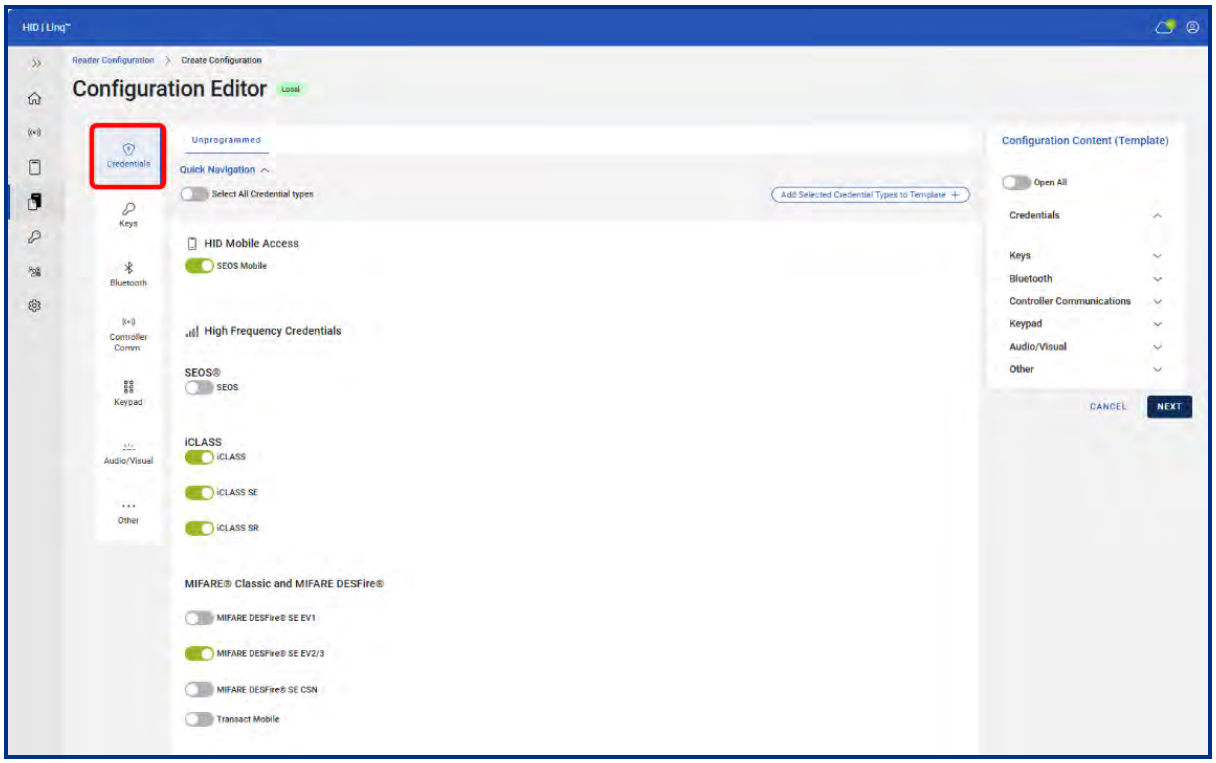
> **Note:** Use the **Quick Navigation** toggle to enable or disable all custom keys.

11.3.1 Offline credential configuration

Select the required credential types to add to the template. See **11.2.1 Online credential technology templates** for the supported credentials.

> **Important: All credential technologies are enabled when purchasing an unmodified reader from HID by default. Changing the credential technologies via a configuration overwrites the default settings. Only the credential technologies of the new configuration will be available. The enabled credentials can be changed at any time by applying a configuration to the reader.**

1. Navigate to the **Credentials** tab.



2. Click the toggles to enable or disable the required parameters.
3. Click **Add Selected Credential Type to Template** for the required credentials.

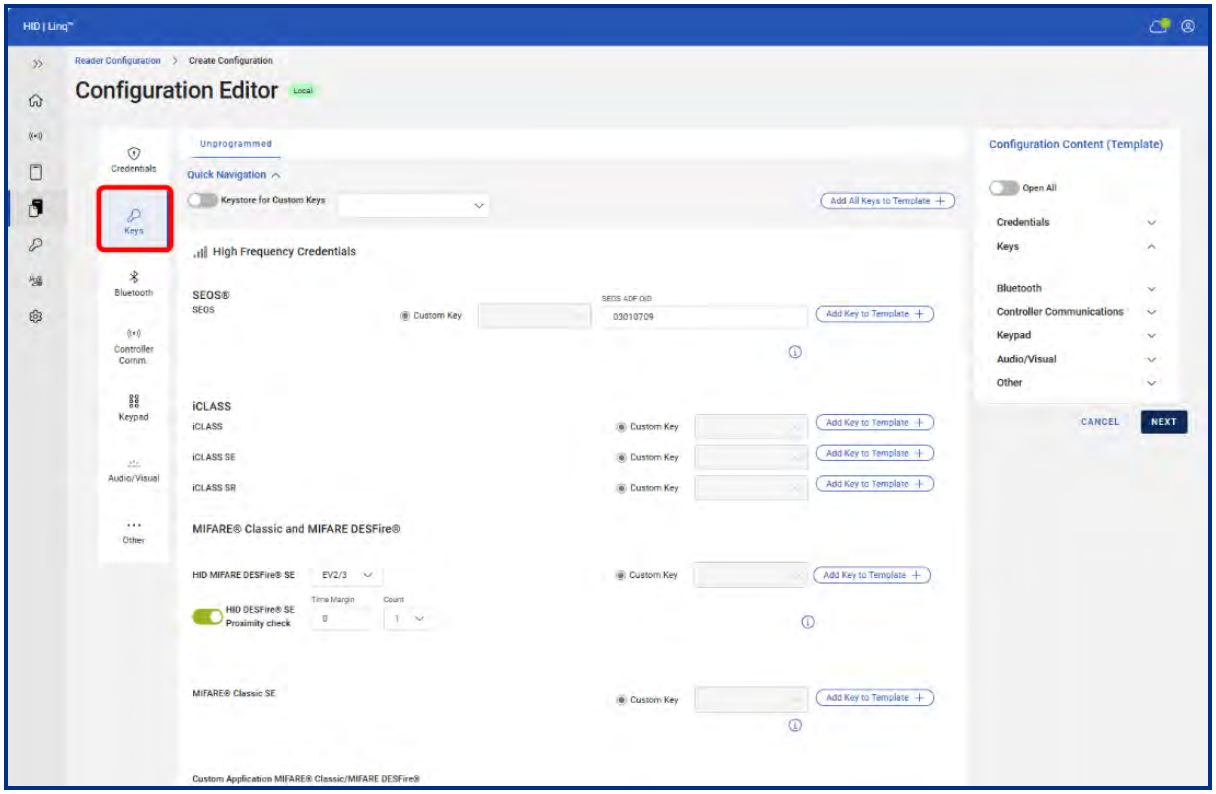
> **Note:** Use the **Quick Navigation** toggle to enable or disable all credential types.

11.4 Offline key configuration

Select the required locally stored keys to add to the configuration template. The following Soft Charge profiles are supported in the offline configuration editor.

Credentials	Soft Charge Profiles
	Unprogrammed
SEOS Mobile ID's	
SEOS	▪
iCLASS SE	▪
iCLASS SR	▪
iCLASS	▪
MIFARE, DESFire, EV1, EV2, EV3 - with SIO	▪
MIFARE Classic with SIO	▪
MIFARE Classic CSN	
MIFARE, DESFire, EV1, EV2, EV3 - with Custom Data (Datamapper)	▪
MIFARE Classic with Custom Data	▪
FELICA IDM	
DEPAS	
125 kHz Proximity	
125 kHz Indala Proximity	
125 kHz EM4102 Proximity	

1. Navigate to the **Keys** tab.

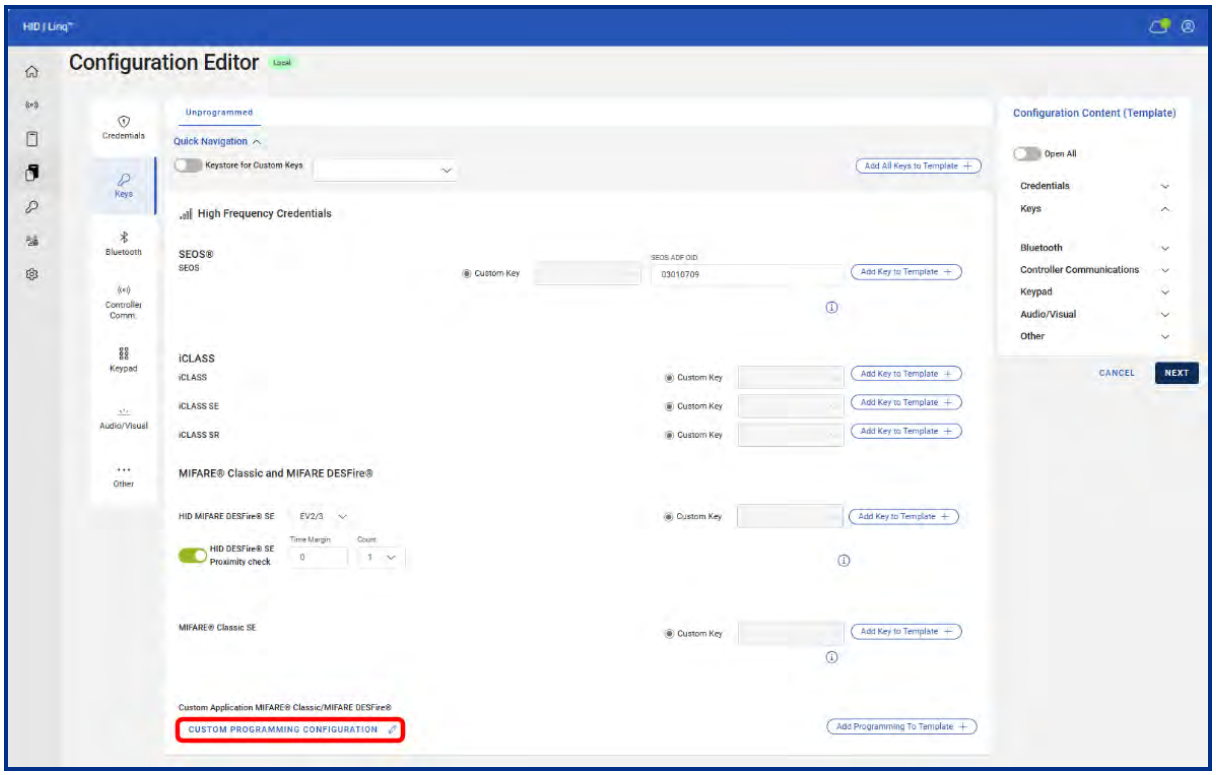


2. Click **Add Key to Template** for the required credentials.

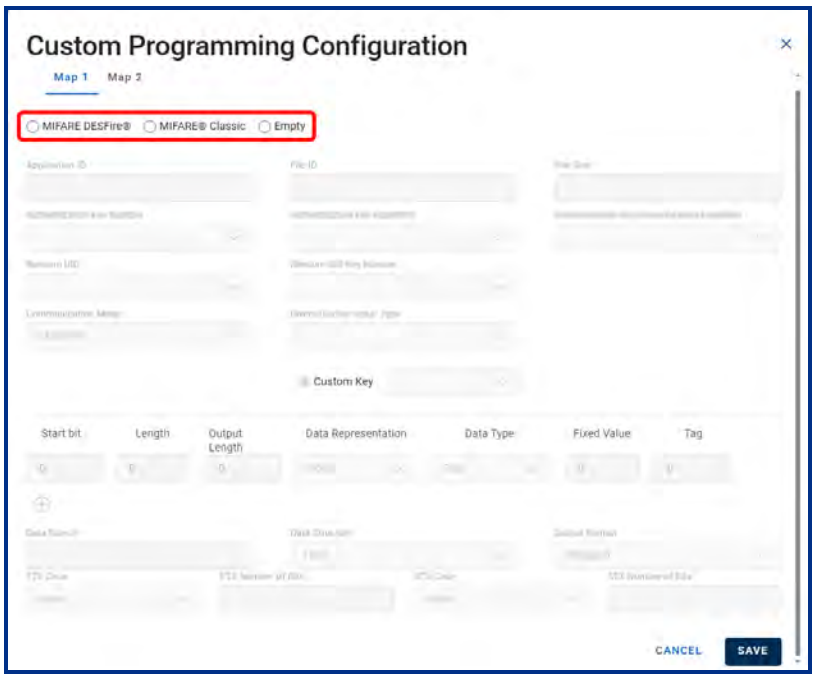
> **Note:**
> - Click **Add All Keys to Template** to add all custom keys to the template.
> - See **11.4 Offline key configuration** for more information on the **Custom Programming** toggle.

Custom Programming Configuration

1. Click the **Custom Programming** toggle to enable or disable custom programming.
2. Click **CUSTOM PROGRAMMING CONFIGURATION**.



3. Select the required credential in the **Custom Programming Configuration** pop-up window.
   - **MIFARE DESFire®**
   - **MIFARE® Classic**
   - **Empty**



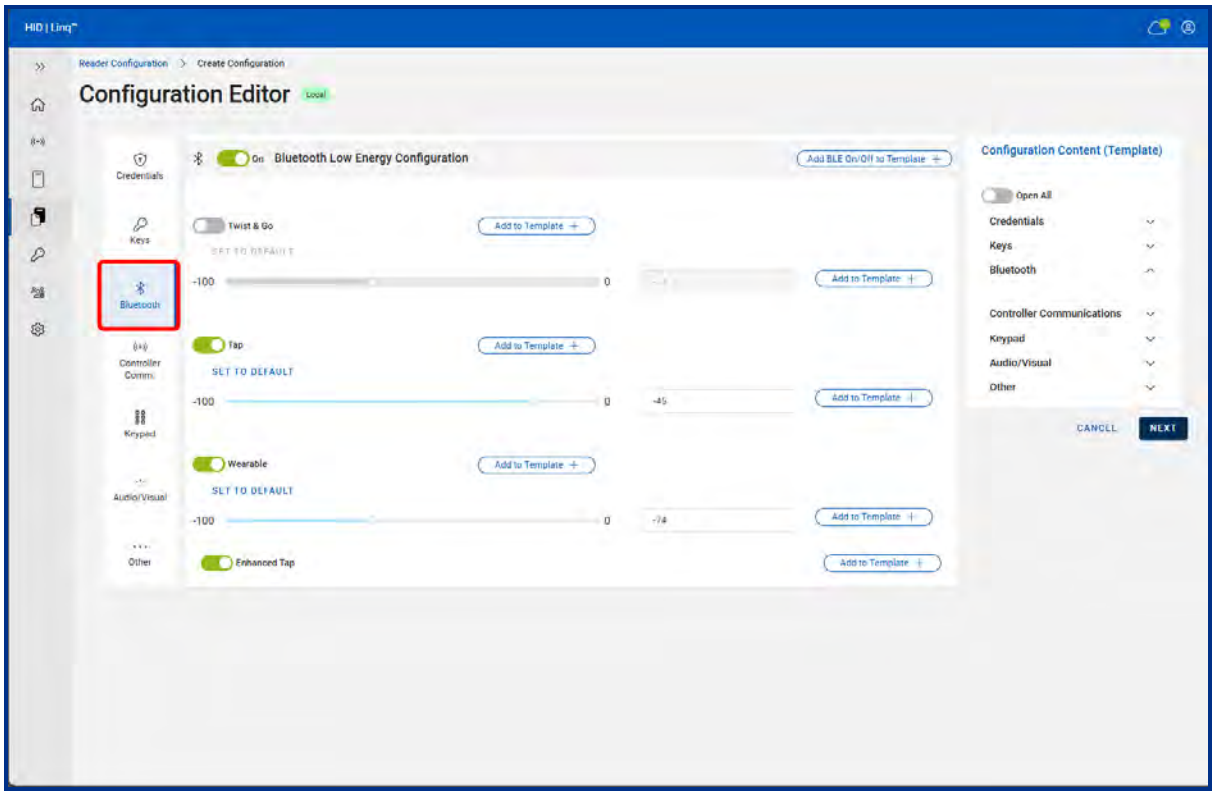
4. Click the toggles to enable or disable the required parameters.

   Note: See **MIFARE Custom Programming Credentials** for more information on the MIFARE DESFire and MIFARE Classic credential configuration parameters.

5. Click **SAVE** to save and close the **Custom Programming Configuration** window.
6. Click **Add Programming To Template** to add the **Custom Programming Configuration** to the template.

11.4.1 Bluetooth Low Energy (BLE) configuration

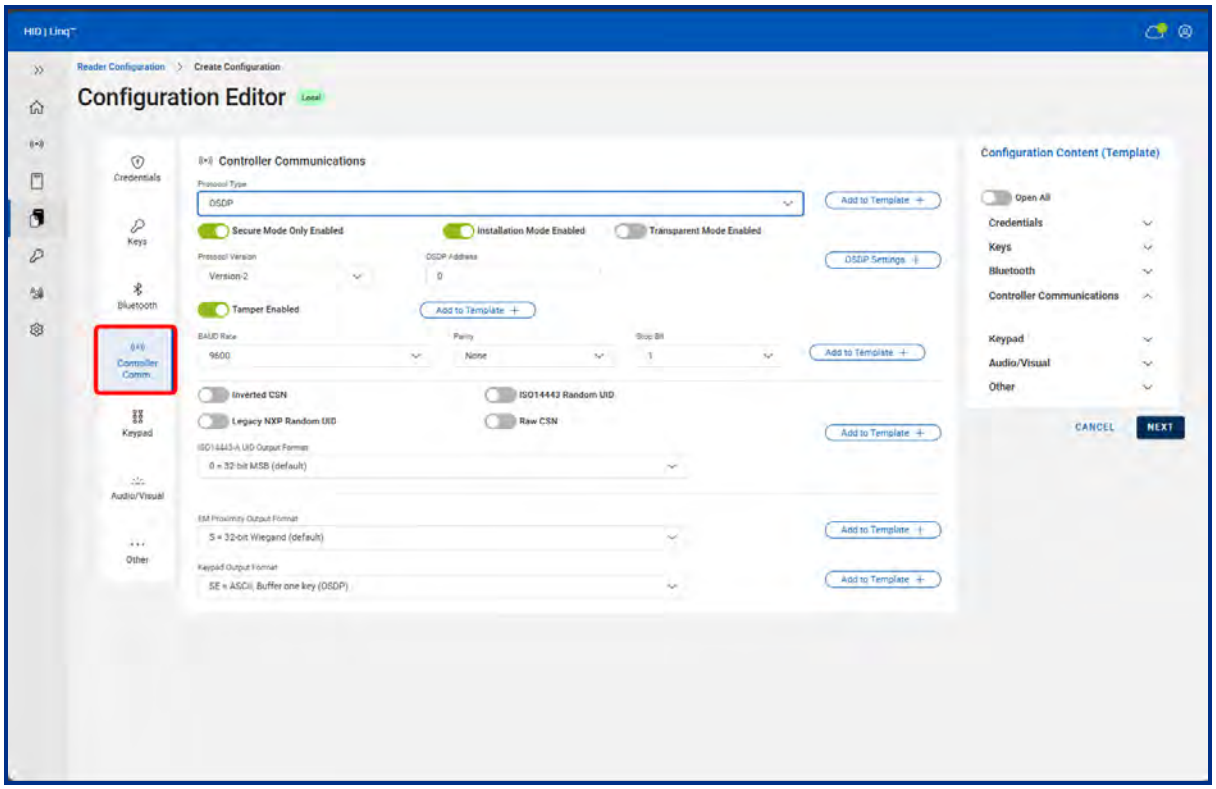
1. Navigate to the **Bluetooth** tab.



2. Click the toggles to enable or disable the required parameters.
3. Click **Add to Template** for the required parameters.

11.4.2 Controller communications

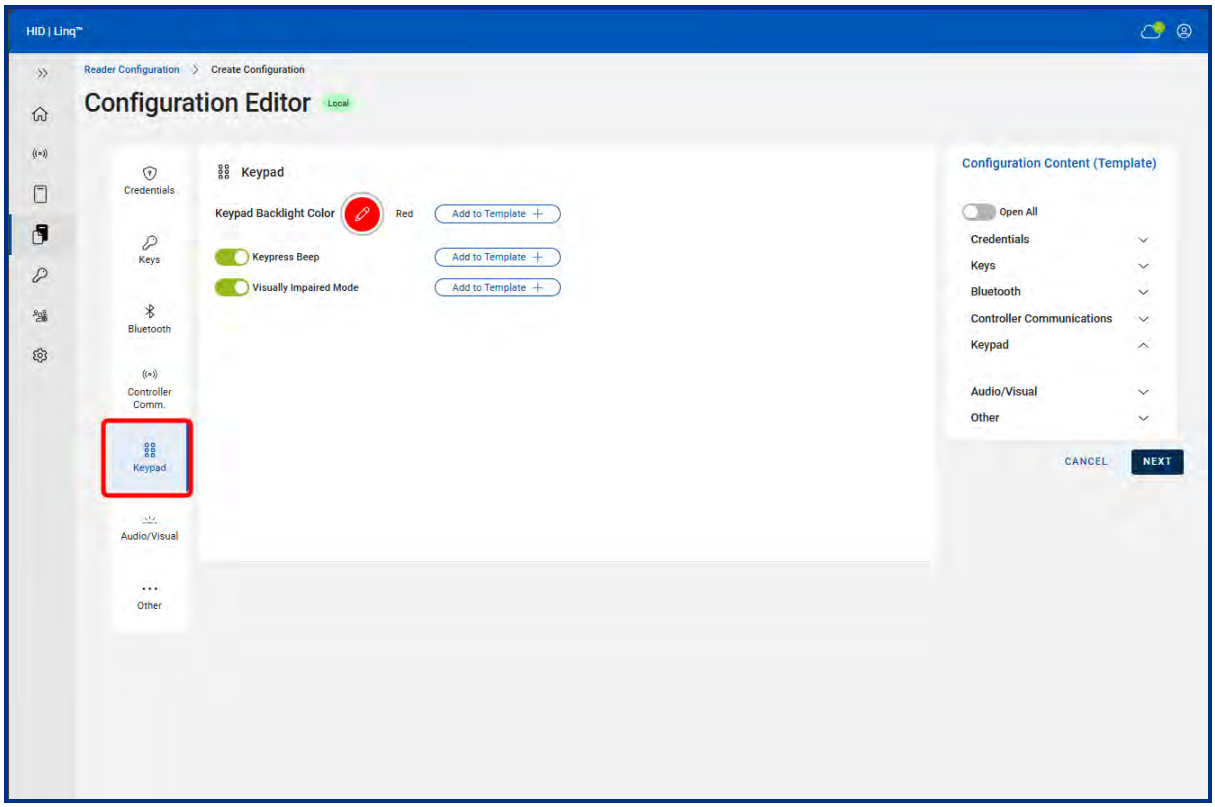
1. Navigate to the **Controller Communications** tab.



2. Select the required **Protocol Type** from the drop-down list.
   - **None**
   - **Wiegand**
   - **OSDP**
   - **WiegandOSDPReady**
   - **ClockAndData**
   - **UART**
   - **PAM**
3. Click the toggles to enable or disable the required protocol type parameters
4. Click **Add to Template** for the required parameters.

11.4.3 Keypad

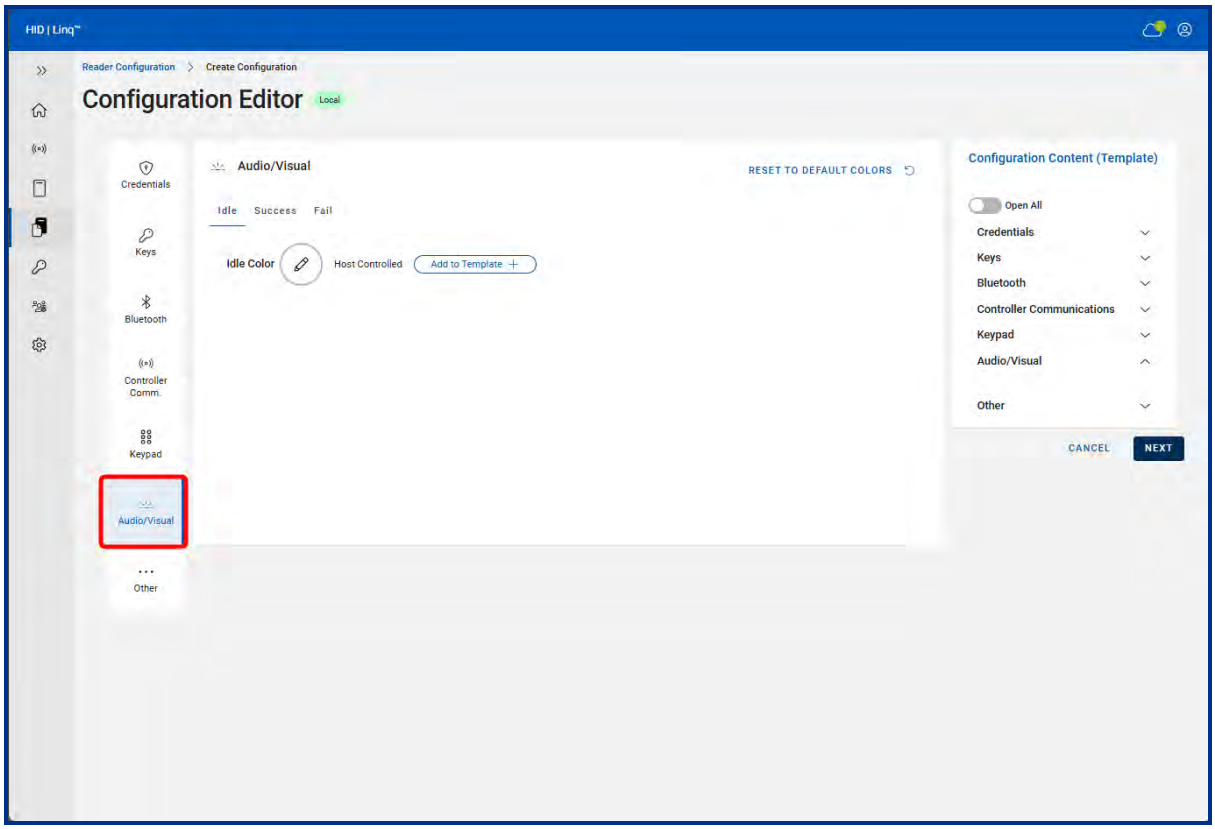
1. Navigate to the **Keypad** tab.



2. Click the toggles to enable or disable the required parameters.
3. Click **Add to Template** for the required parameters.

11.4.4 Audio/Visual

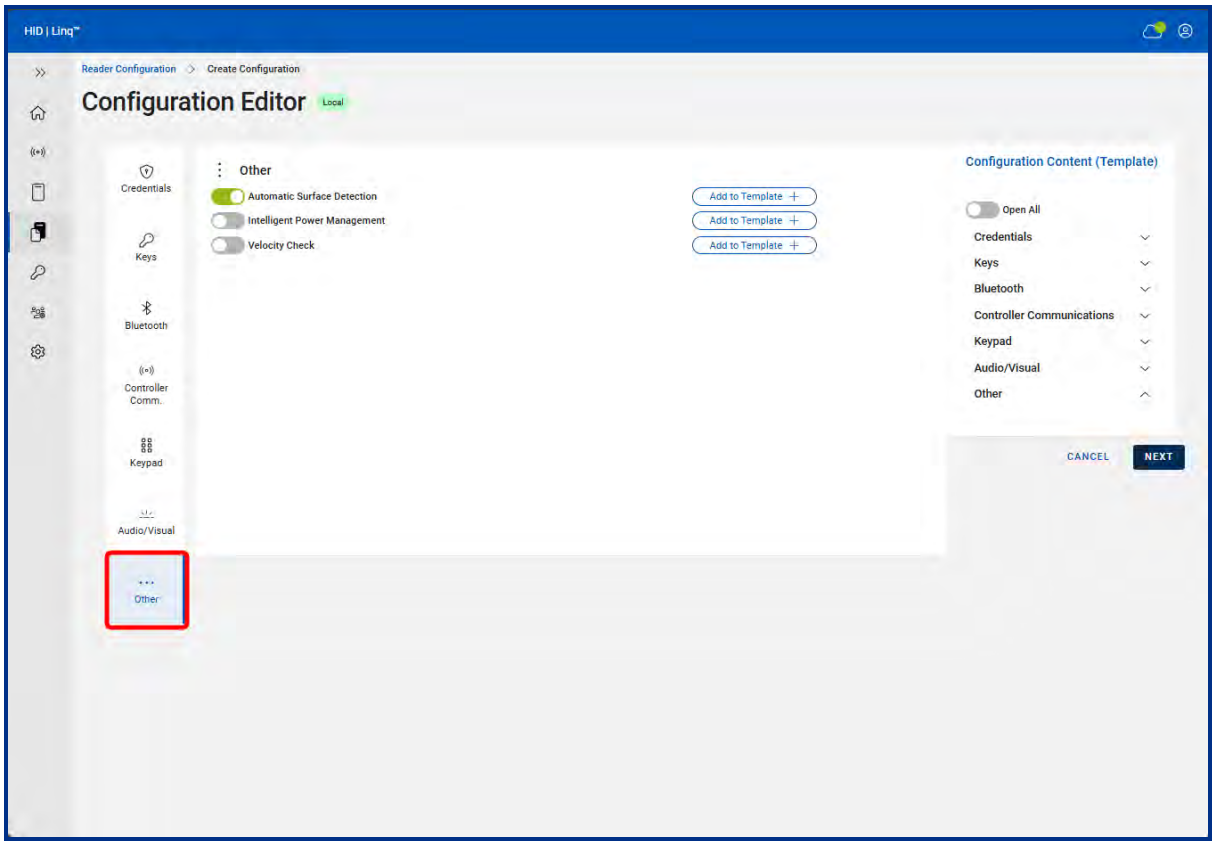
1. Navigate to the **Audio/Visual** tab.



2. Select the required event tab.
   - **Idle**
   - **Success**
   - **Fail**
3. Configure the required parameters.
4. Click **SAVE**.

11.4.5 Other

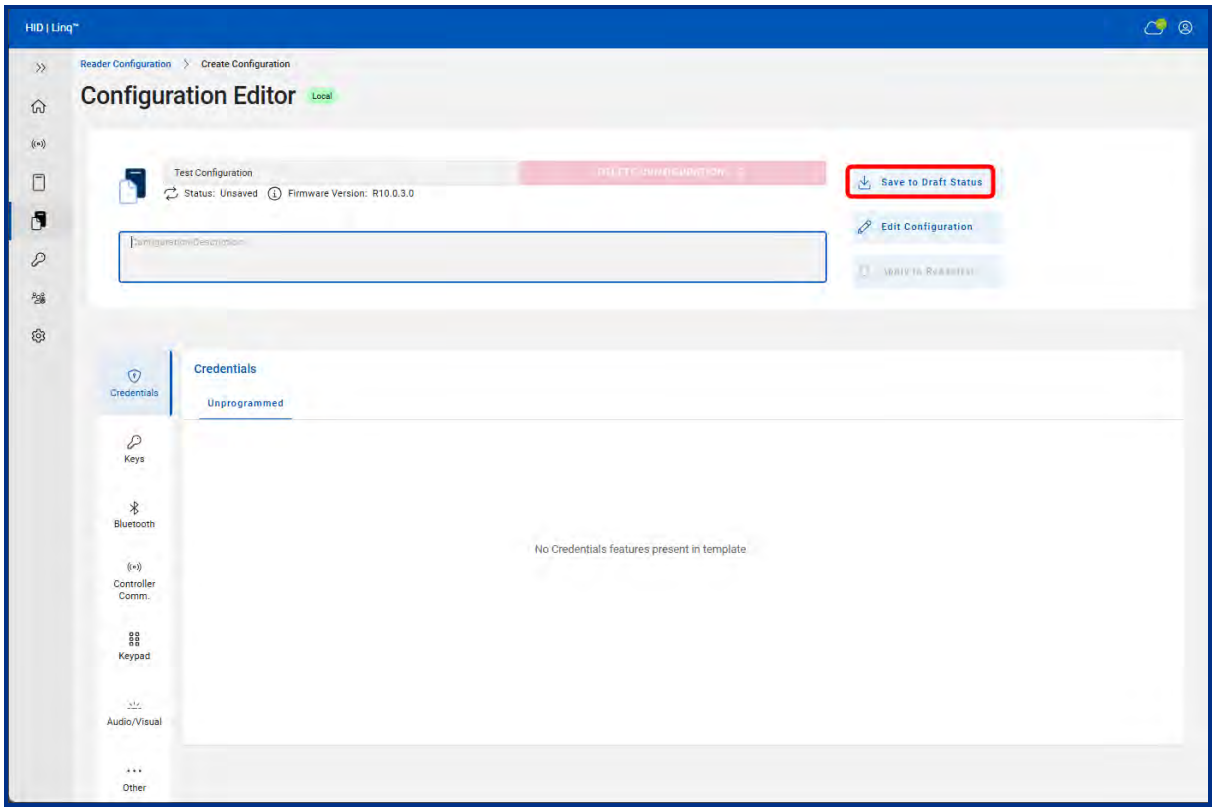
1. Navigate to the **Other** tab.



2. Click the toggles to enable or disable the required parameters.
3. Click **Add to Template** for the required parameters.
4. Click **NEXT** when the required parameters are set.

11.4.6 Save the Configuration ID

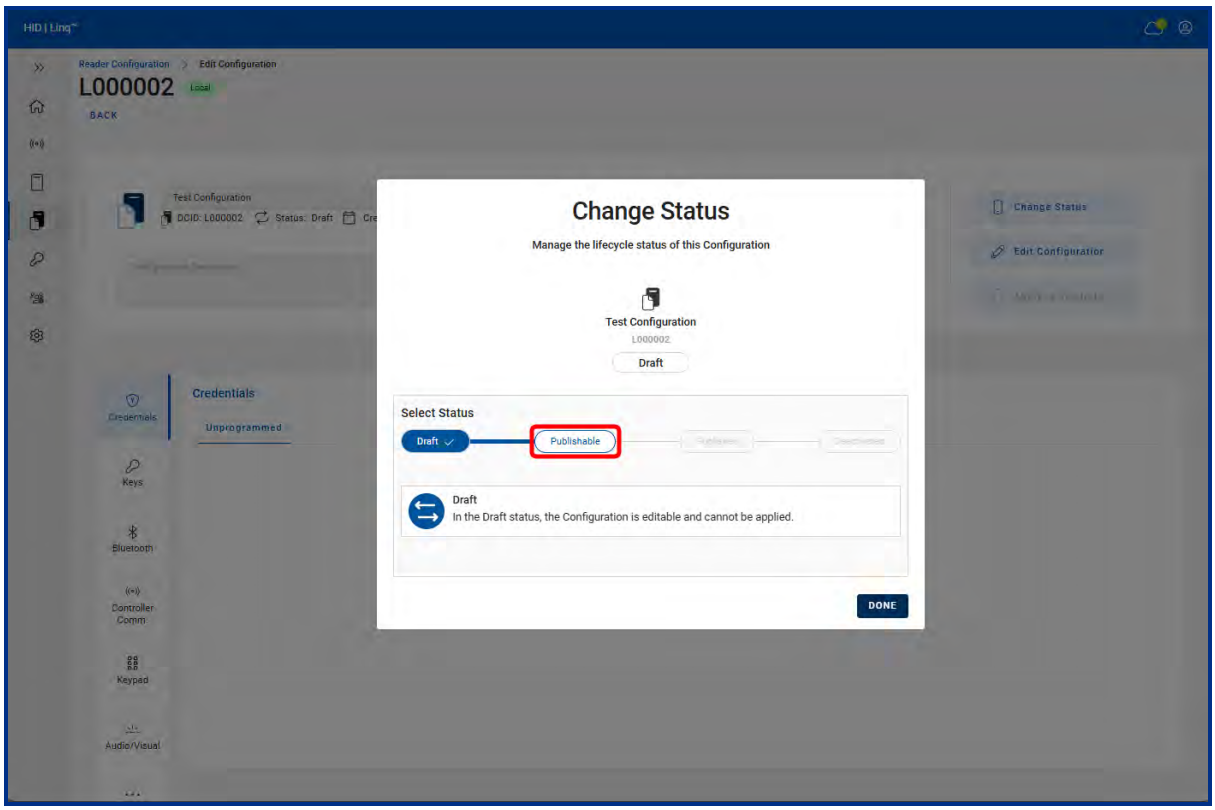
1. Enter a **Configuration Name**.
2. Enter a **Configuration Description**.
3. Click **Save to Draft Status**. The Configuration ID is editable but cannot be applied to a reader.



11.5 Move a Configuration ID to Publishable

Moving the configuration to **Publishable** allows you to apply the template to a reader to test the configuration.

1. Navigate to the **Device Configuration Templates** tab in the left-hand menu.
2. Enter the required Configuration ID and click **SEARCH**.
3. Click the required Configuration ID.
4. Click **Change Status**.
5. Click **Publishable** and click **DONE**.



11.5.1 Move a Configuration ID to Published

Moving the configuration to **Published** allows you to apply the template to readers and makes it public.

Important:

- Test the Configuration ID before moving it to **Published**.
- The Configuration ID cannot be edited or changed back to **Publishable** once it has been **Published**.
- **Published** Configuration IDs cannot be edited because HID keeps a record of configurations applied to a reader. Any changes to a **Published** configuration would invalidate this record.

1. Navigate to the **Device Configuration Templates** tab in the left-hand menu.
2. Enter the required Configuration ID and click **SEARCH**.
3. Click the required Configuration ID.
4. Click **Change Status**.
5. Click **Publishable** and click **DONE**.

11.6 Apply a Configuration ID to a reader

Applying a Configuration ID allows you to manage a reader's visual, audio, and performance characteristics. Configuration IDs can be applied before or after installation of a reader.

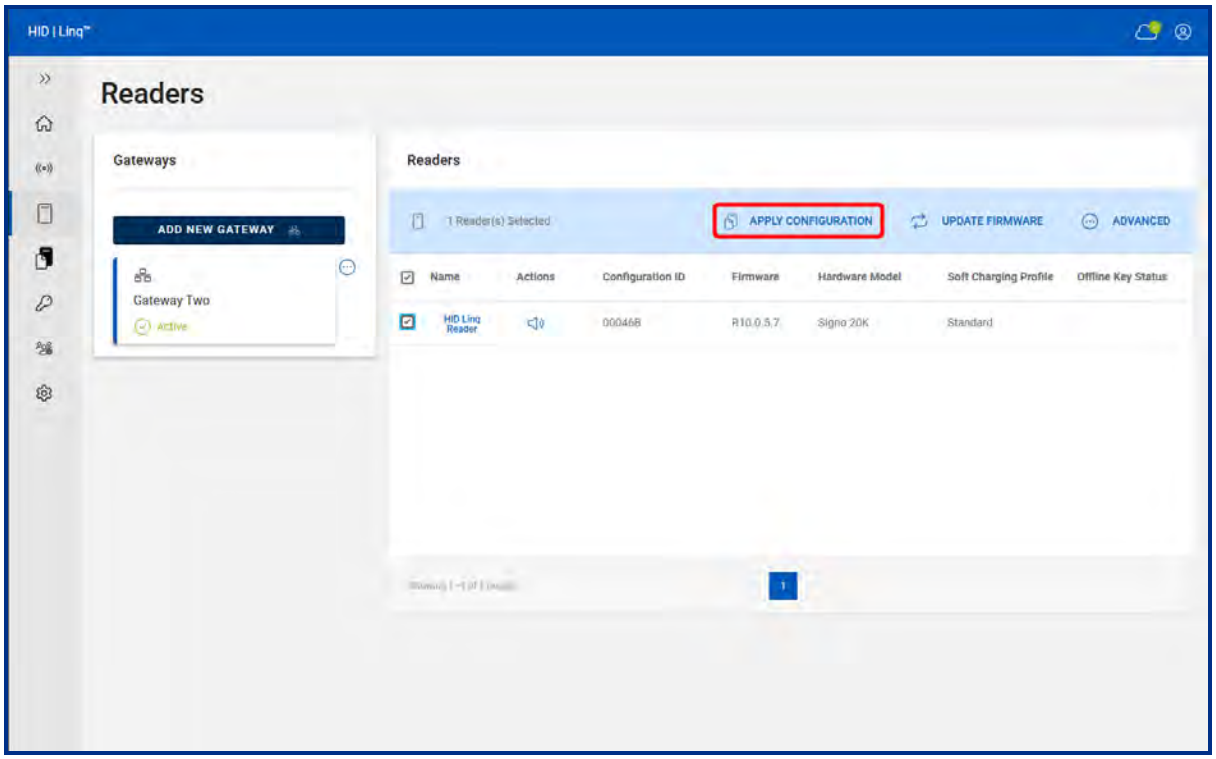
Who can apply a Configuration ID?

	Reader Manager Portal Administrator	Reader Technician
Permission	Yes	Yes
Multiple reader capability	Yes	Yes

Note:
- **System Administrators** and **Device Administrators** can apply a Configuration ID to a reader.
- Readers will not function when applying Configuration IDs. Readers connected to HID controllers should only be updated outside of work hours.
- Searching for a Configuration ID by name is limited to starting characters only.
- Searches are limited to 5000 results.
- Typical search time for a configuration can take up to 15 seconds.

Apply known Configuration IDs directly to a reader via the **Readers** tab. See **11.7 Search for a Configuration ID** to view a Configuration ID before applying it to a reader.

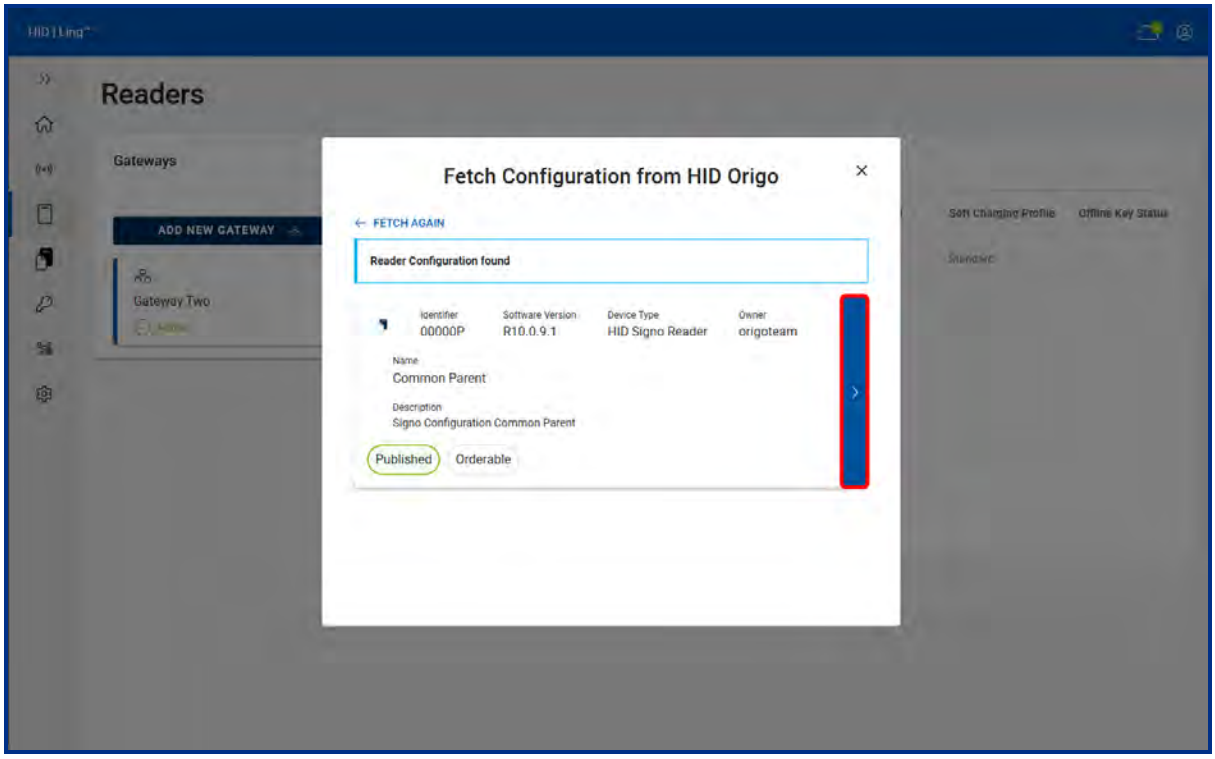
1. Navigate to the **Readers** tab.
2. Check the box of the required connected reader(s).
3. Click **APPLY CONFIGURATION**.



4. Enter the required Configuration ID.

Note: See **1.1 Common Configuration IDs** for a list of commonly used Configuration IDs.

5. Click **FETCH**.
6. Click the arrow to apply the Configuration ID.



7. HID Linq On Premise checks if the Configuration ID is compatible with the reader. Click **CONTINUE** if they are compatible.
8. Click **START APPLYING CONFIGURATION**. Progress is displayed.

   Note: Click **CLOSE THIS WINDOW** to close the window (the process continues in the background). The **Applying Configuration** status bar is displayed on the main page.

9. Click **DONE** to finish.
10. Navigate to the **Readers** tab and click **DISCOVER READERS** to refresh the changes to the reader Configuration ID.

11.7 Search for a Configuration ID

The **Device Configuration Templates** tab allows you to search for a Configuration ID stored locally or in HID Origo by its identifier, name, or status. The search word used must match the first word of the Configuration ID name.

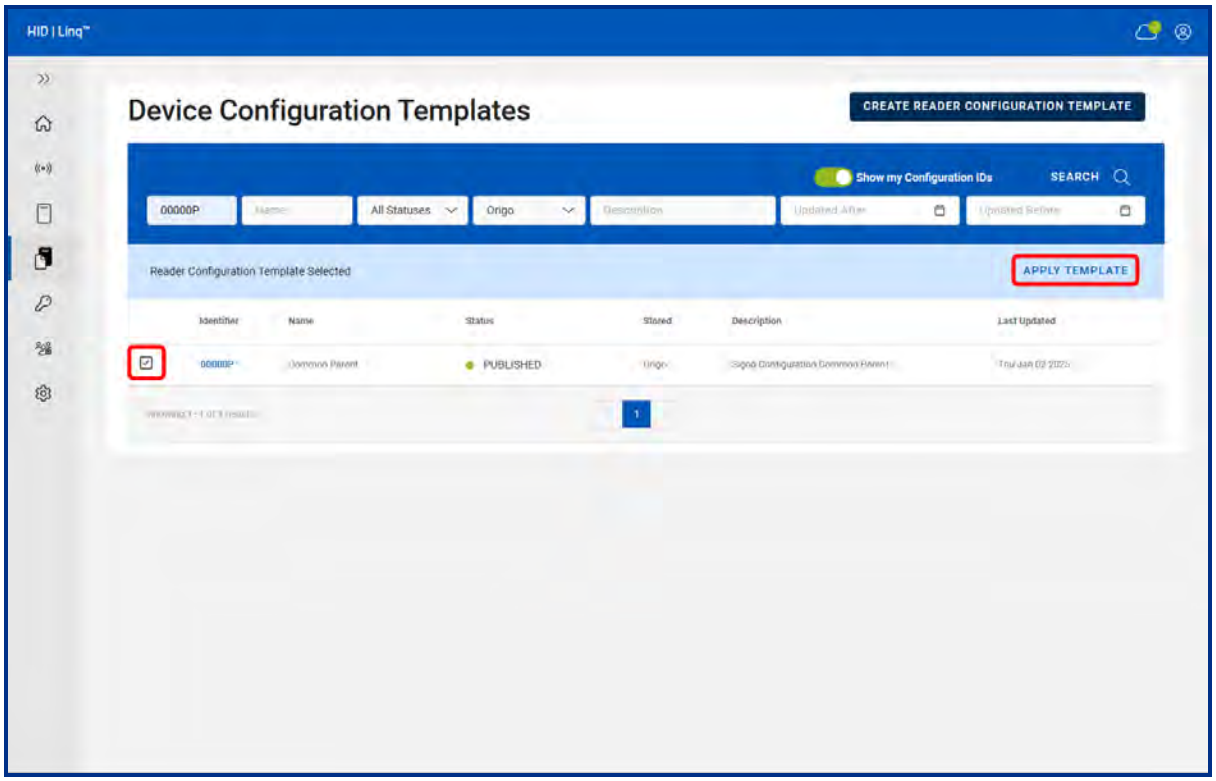
Online reader Configuration IDs are created in HID Origo by an organization, and only members of that organization can access its Configuration IDs.

> **Note:** Configuration IDs owned by the current user are displayed when searching by configuration name or status by default. Disable the **Show my Configuration IDs** toggle to display configurations from the users organization.

11.7.1 Search and apply a Configuration ID

The **Device Configuration Template** tab allows you to search for a Configuration ID and check its status and parameters before applying it to a reader.

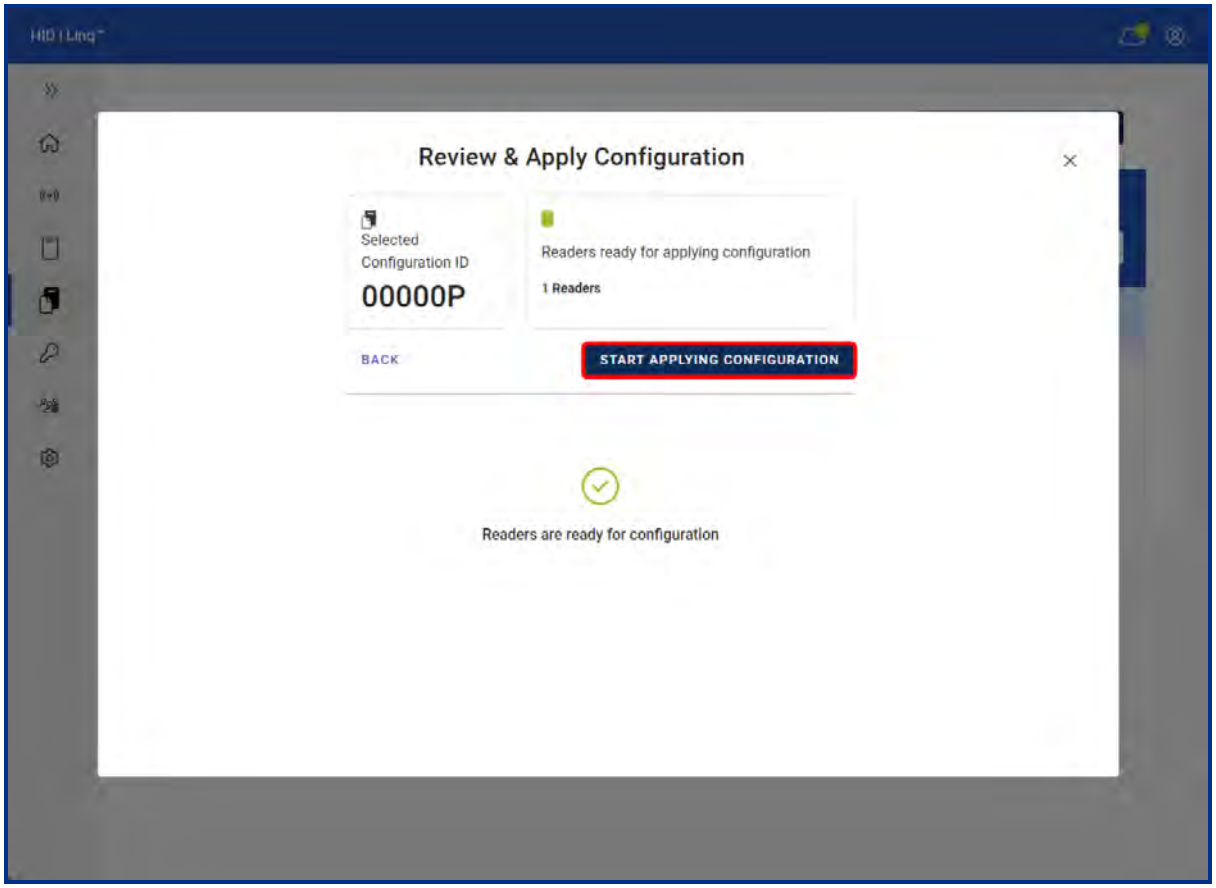
1. Navigate to the **Device Configuration Templates** tab in the left-hand menu.
2. Enter the required search criteria and click **SEARCH**.
3. Check the box of the required Configuration ID and click **APPLY TEMPLATE**.



4. Select the required gateway and click **DISCOVER READERS**.
5. Check the box of the required readers and click **SELECT READERS**.

> **Note:** Use the **Offline Management Status** drop-down list to filter between Online or Offline readers.

6. Click **START APPLYING CONFIGURATION**. Progress is displayed.



> **Note:** Click **CLOSE THIS WINDOW** to close the window (the process will continue in the background). The **Applying Configuration** status bar is displayed on the main page.

7. Click **DONE** to finish.
8. Navigate to the **Readers** tab and click **DISCOVER READERS** to refresh the changes to the reader Configuration ID.

Section 12

Update HID Signo reader firmware

12.1 Update reader firmware

It is recommended to keep your HID Signo reader firmware up to date. When updating the reader firmware, you can re-apply the same firmware version or upgrade to the latest firmware version. Readers connected via a controller are restricted from selection in the firmware update process.

Caution: Firmware upgrade via Mercury controllers is not currently supported.

Note: Readers with firmware version 7.5 or older must first be updated to 9.1 before they can be updated to the latest firmware.

Who can update reader firmware?

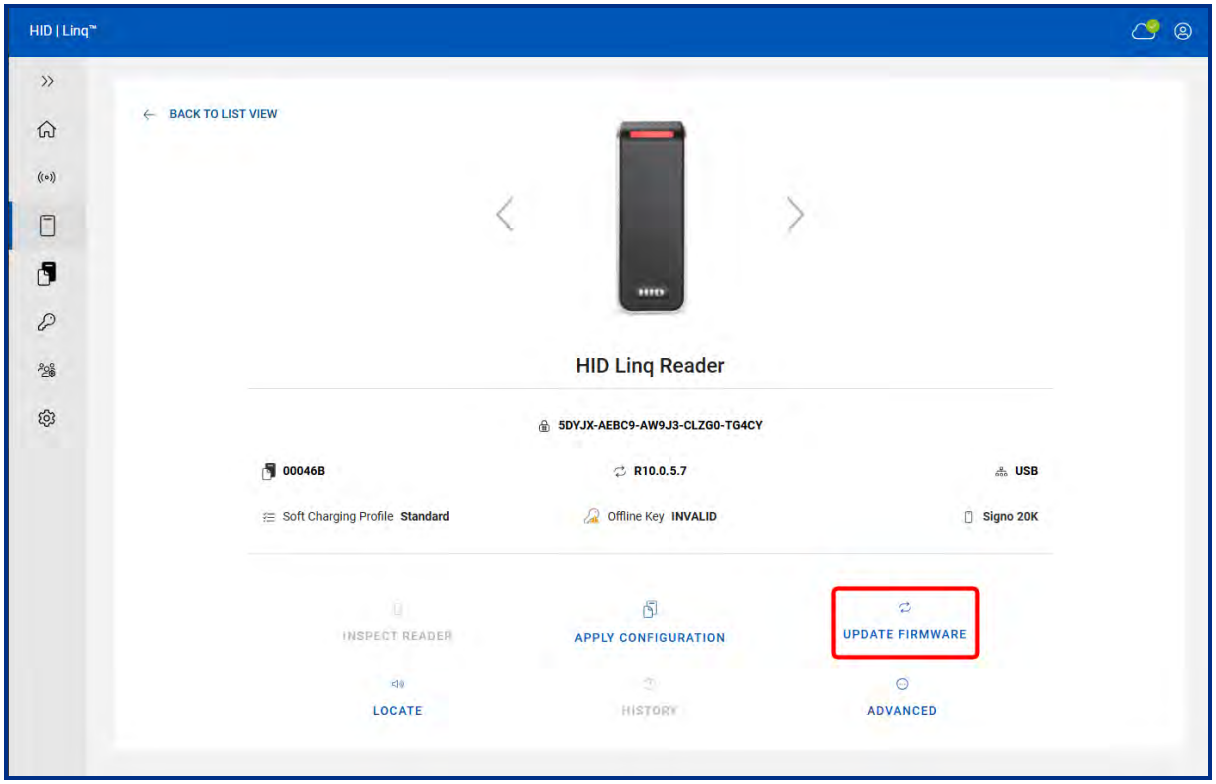
	Reader Manager Portal Administrator	Reader Technician
Permission	Yes	Yes
Multiple reader capability	Yes	Yes

Important:
- Readers will not function during firmware updates.

Note:
- An active connection to HID Linq On Premise is required to update reader firmware.
- The maximum recommended number of readers per hub is four.
- Do not disconnect the reader or remove the power supply until after the firmware update is complete. While a firmware update can be retried, it is possible that an interrupted firmware update may render the reader unusable and may void the warranty. If you encounter issues, contact HID Technical Support for assistance.
- A reader connected via USB takes approximately 8-12 minutes to complete.
- When updating multiple readers in parallel, the time to update each reader is the same.
- It is not possible to downgrade reader firmware.

1. Navigate to the **Readers** tab in the left-hand menu.
2. Select the required HID Linq Gateway.
3. Select the required connected reader.

4. Click **UPDATE FIRMWARE**.



5. Select the latest firmware version from the **Available Firmware Versions** list.

> **Note:** Only the latest firmware can be re-applied to a reader that already has the latest firmware version.

6. Click **UPDATE FIRMWARE** and confirm **UPDATE FIRMWARE** in the pop-up window.

> **Important: Do not disconnect or power off the reader during the firmware update process.**

> **Note:** Close the window (the process will continue in the background). The **Firmware Update** status bar is displayed on the main page.

7. Navigate to the **Readers** tab and click **DISCOVER READERS** to refresh the changes to the reader Configuration ID.

Firmware update	Result
Success	Firmware update was successful. Re-discover the readers to see the changes to the readers.
Fail	Firmware update failed. Attempt the update again or contact HID Technical Support if the firmware update continues to fail.
Partial update	After a partial update, the reader is still discoverable. Repeat the update process. Reader operations are disabled until a successful firmware update is complete. Contact HID Technical Support if the firmware continues to partially update.

> **Note:** If the reader is damaged, it will not be discoverable. Contact HID Technical Support.

12.2 Update multiple reader firmware

Caution: Firmware upgrade via Mercury controllers is not currently supported.

When updating the reader firmware, you can upgrade to the latest firmware version. Upgrading your HID Signo reader firmware keeps them up to date with the latest features and security updates from HID. It is best practice to keep your HID Signo reader firmware up to date.

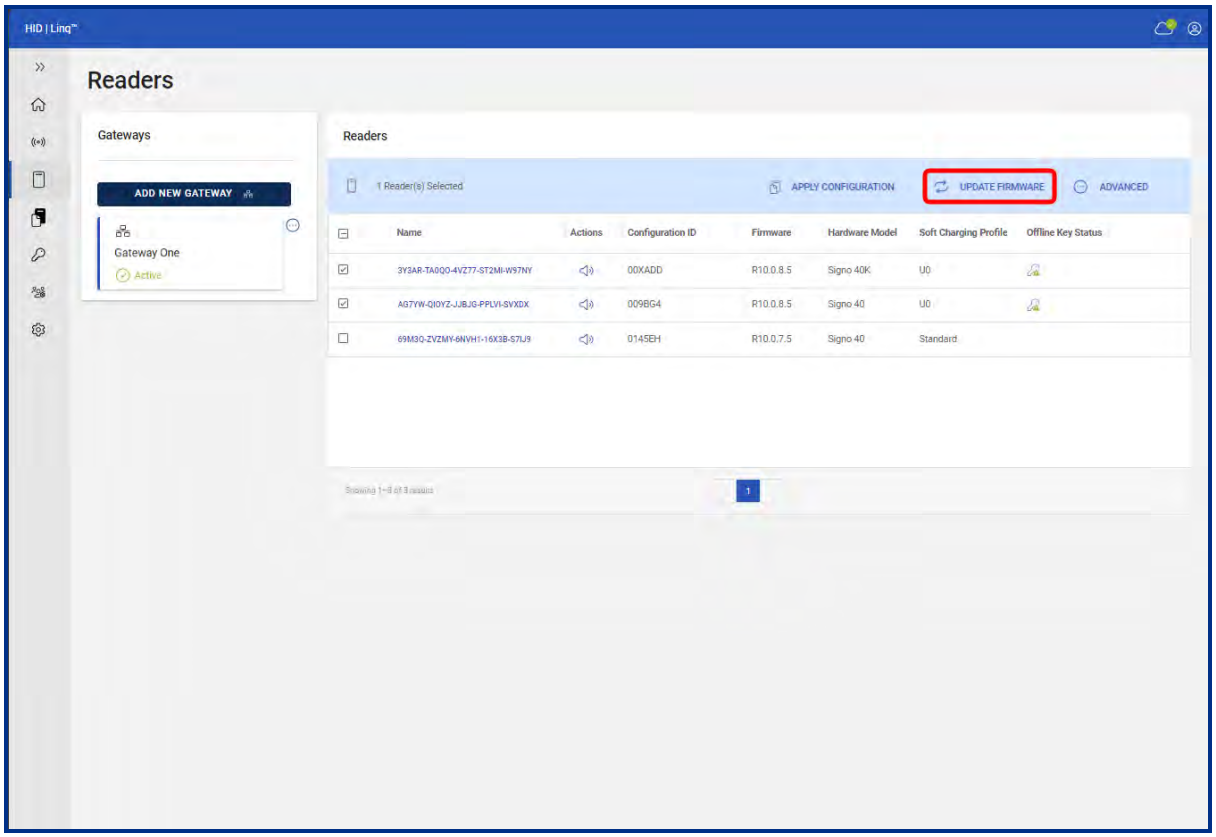
Important:
- Readers will not function during firmware updates.

Note:
- An active connection to HID Linq On Premise is required to update reader firmware.
- Do not disconnect the reader or remove the power supply until after the firmware update is complete. While a firmware update can be retried, it is possible that an interrupted firmware update may render the reader unusable and may void the warranty. If you encounter issues reach out to HID Technical Support for further assistance.
- A reader connected via USB takes approximately 8 minutes to complete.
- When updating multiple readers in parallel, the time to update each reader is the same.
- It is not possible to downgrade reader firmware.
- Multiple readers are updated in a group. The group is displayed in the progress bar. Update multiple groups of readers at the same time. See **12.2.1 Reader grouping** for more information.

1. Navigate to the **Readers** tab in the left-hand menu.
2. Select the required HID Linq Gateway.
3. Check the box of the required connected readers.

   Note:
   - Update up to four readers connected via USB, at any one time.
   - All selected readers must have the same current firmware version.
   - All selected readers can only be updated to the latest firmware version.
   - If any reader in the list cannot be updated to the desired version, HID Linq On Premise will display a notification and not attempt the update for that individual reader.
   - Once the update process is complete, the status of each reader is refreshed to show the version of the firmware installed.

4. Click **UPDATE FIRMWARE**.



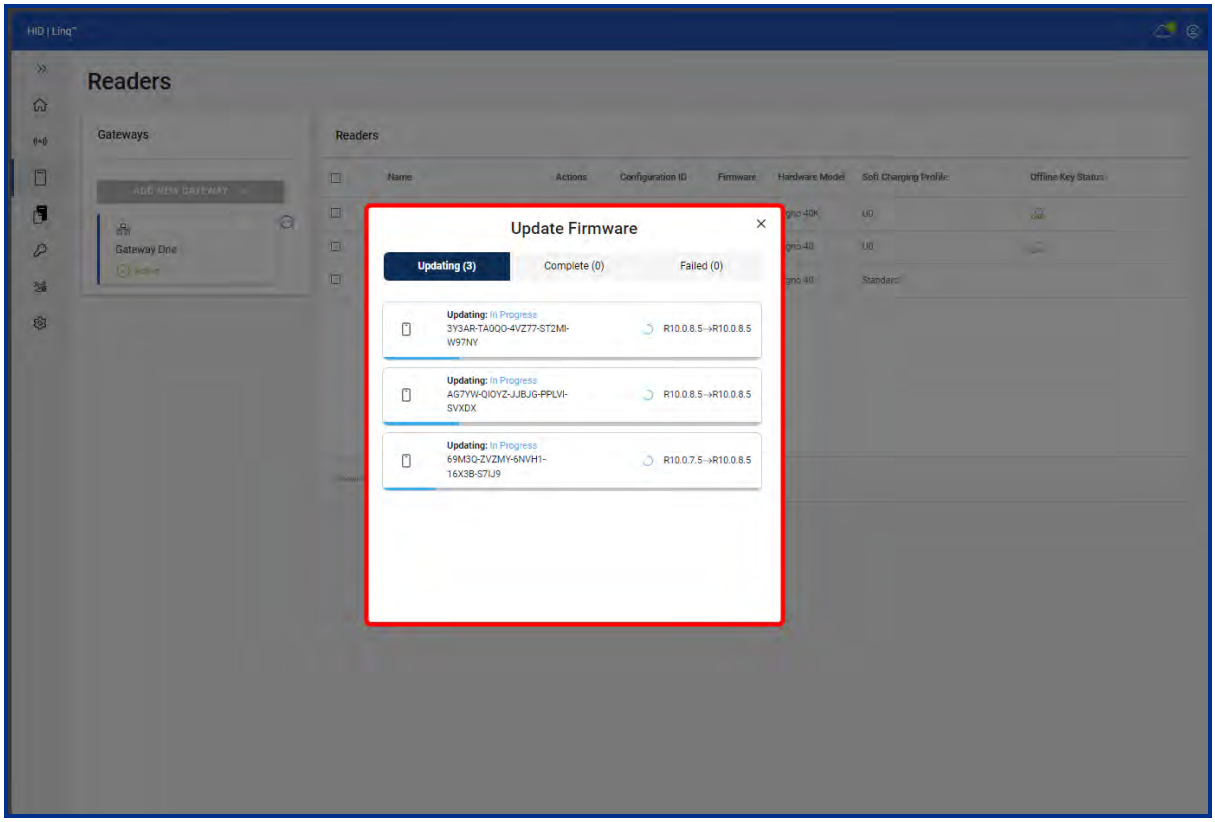
5. Select the latest firmware version from the **Available Firmware Versions** list.

> **Note:** Only the latest firmware can be re-applied to a reader that already has the latest firmware version.

6. Click **UPDATE FIRMWARE** and confirm **YES, UPDATE FIRMWARE VERSION** in the pop-up window.

> **Important: Do not disconnect or power off the reader during the firmware update process.**

7. Close the pop-up window (the process continues in the background). The **Firmware Update** status bar is displayed on the main page.



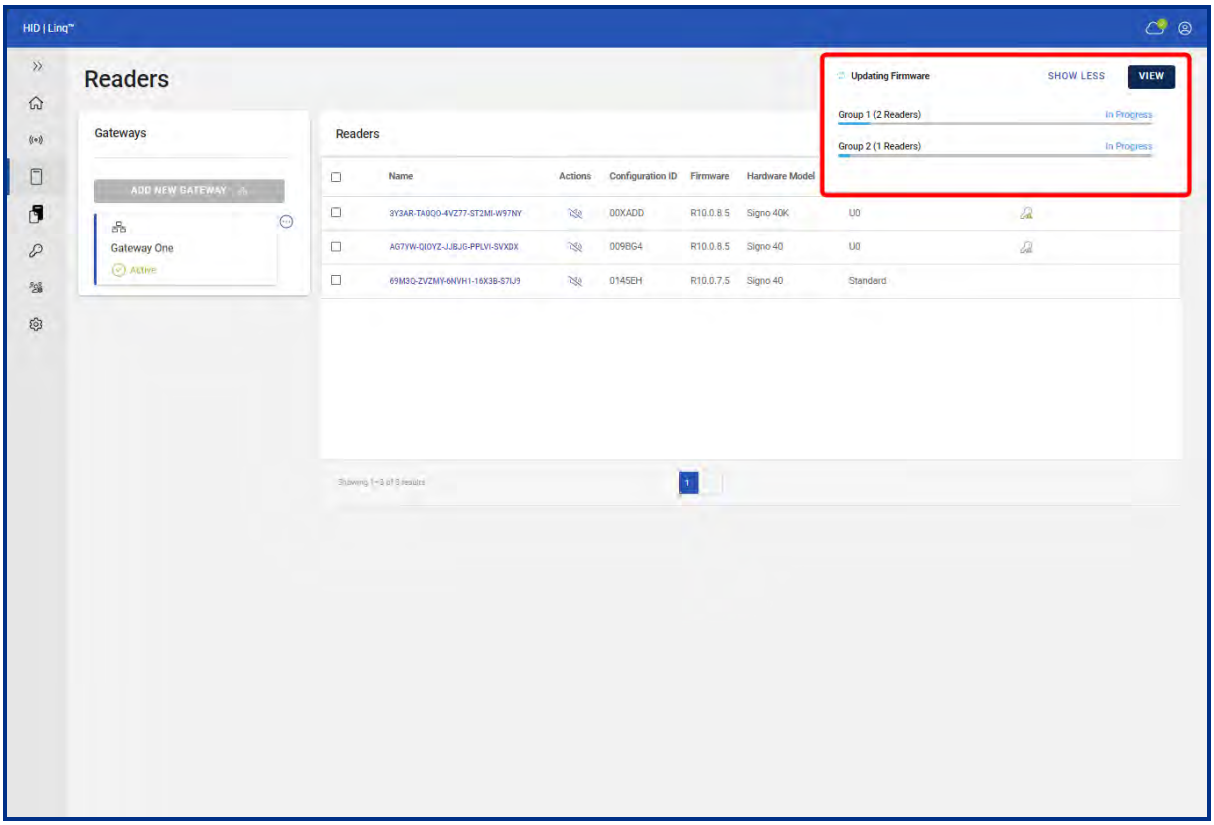
8. Once complete, navigate to the **Readers** tab and click **DISCOVER READERS** to refresh the changes to the reader Configuration ID.

Firmware update	Result
Success	Firmware update was successful. Re-discover the readers to see the changes to the readers.
Fail	Firmware update failed. Attempt the update again or contact HID Technical Support if the firmware update continues to fail.
Partial update	After a partial update, the reader is still discoverable. Repeat the update process. Reader operations are disabled until a successful firmware update is complete. Contact HID Technical Support if the firmware continues to partially update.

Note: If the reader is damaged, it will not be discoverable. Contact HID Technical Support.

12.2.1 Reader grouping

HID Linq On Premise groups one or more readers during a firmware update.

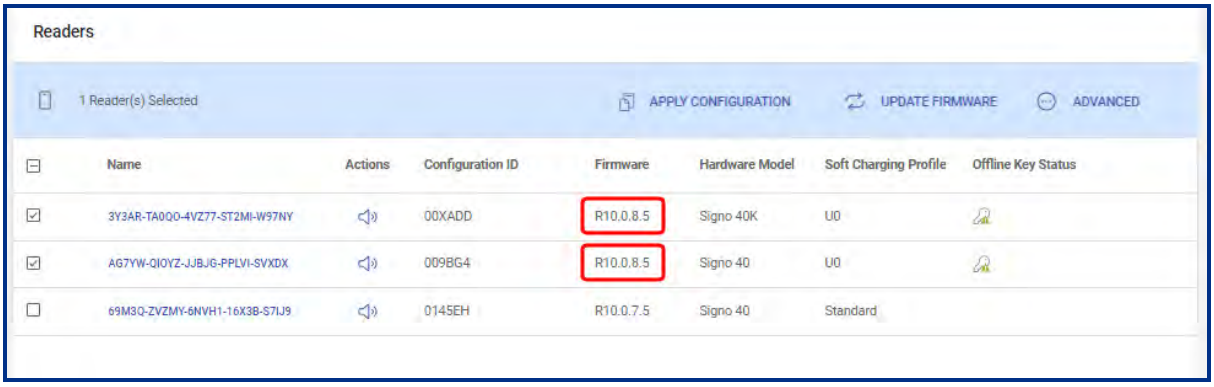


For example:

Reader	Current Firmware version	Target Firmware Version
A,B,C	R10.0.7.5	R10.0.10.4 (Upgrade)
D,E,F	R10.0.4.2	
G,H,I	R10.0.3.1	

Readers **D**, **E** and **F** are at the same firmware version. You can only select them together to update them simultaneously. This would result in them being grouped as **Group 1**.

Readers **G**, **H** and **I** are at the same firmware version. You can only select them together to update them simultaneously. This would result in them being grouped as **Group 2**.



Note:

- All selected readers must have the same current firmware version.
- All selected readers can only update to the latest firmware version.

Section 13

Reset a reader to the default configuration

13.1 To reset a reader to default configuration

Note: If a reader is configured with an Elite key, that key will be removed from the reader. The key reference can be modified, and the reader can be configured with a different Elite key.

Who can reset a reader to default configuration?

	Reader Manager Portal Administrator	Reader Technician
Permission	Yes	Yes
Multiple reader capability	No	No

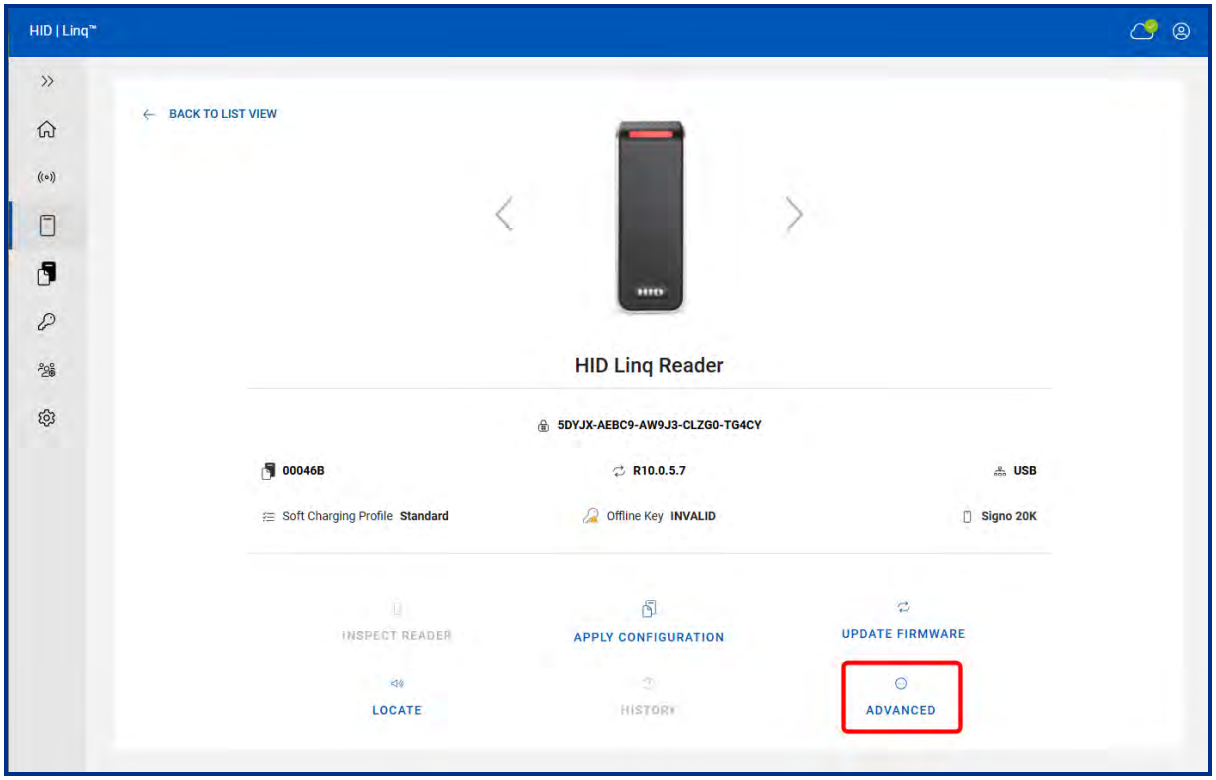
A reader configuration reset could be useful to:

- Push a new configuration
- Put the reader back to Standard from Elite profile
- Troubleshoot

Note:
- The credential profile of a reader is set before shipping and cannot change. The Configuration ID selected by HID Linq On Premise matches the default configuration for the credential profile of the reader.
- Resetting the device to its default configuration does not affect the reader firmware version.
- The reader must have the latest firmware version to enable this feature.
- Reset one reader at a time.
- If the operation fails, please contact HID Technical Support.
- Some reader profiles are not supported for this operation. See **Reset Reader** for more information.

1. Navigate to the **Readers** tab in the left-hand menu.
2. Select the required HID Linq Gateway.

3. Select the required connected reader and click **ADVANCED**.



4. Click **Reset to factory default configuration** and click **NEXT**.
5. Click **START APPLYING CONFIGURATION**.
6. Click **CLOSE**.
7. Navigate to the **Readers** tab and click **DISCOVER READERS** to refresh the changes to the reader Configuration ID.

13.1.1 Supported reader profiles

The reset operation is only supported for the following profiles:

- Standard
- Custom

See **1.1 Error and warning messages** for more information.

Appendix A

Configuration IDs

A.1 Configuration ID overview

Users with access to Origo services have access to a library of reader Configuration IDs. Each reader Configuration ID has a unique six character identifier.

Reader Configuration IDs support an inheritance capability. When creating a new reader Configuration ID, this allows a parent Configuration ID to be referenced that specifies a set of starting values, (which can be a small set or a complete listing of all available attributes such as the factory defaults) so that the subset of configuration values in the new Configuration ID, can be changed to what is needed.

When a Configuration ID in its own definition, or through inheritance, specifies the complete reader configuration, it is referred to as a Full Configuration ID. When a Configuration ID specifies a subset of values, it is referred to as a Delta Configuration ID:

- **Delta Configuration ID:** changes just the required attributes, leaving everything else at its current value. Past configurations values can be maintained or modified where needed.
- **Full Configuration ID:** sets the value of every attribute regardless of their previous values.

Note: When an Elite Key is used to protect the reader (referred to as the SNMP Key) and the Configuration ID being applied contains a main key reference to the standard key, the Elite Key value in the reader does not change. This maintains the security of the reader and only permits those with rights to that Elite key to configure the device. The main key of the reader can be changed from one Elite Key to another Elite Key when the user has rights to both keys.

A.1.1 Reader Configuration ID status

Status Transition flow	Description
Draft	The reader Configuration ID is in a fully editable state.
Publishable	The reader Configuration ID is in a test state.
Published	The reader Configuration ID is locked. It can be used to configure any connected readers.
Deactivated	The reader Configuration ID is archived and no longer usable.

A.2 Common Configuration IDs

The below Configuration IDs are universal and can be uploaded to a HID Signo reader.

A.2.1 Full Configuration IDs

Note: Full Configuration IDs contain all reader configuration settings and keys.

Configuration ID	Description
00039R	Default configuration of a Seos® profile reader. This Configuration ID can be applied to any HID Signo reader.
00000P	Default configuration of a Standard profile reader. This Configuration ID can be applied to a Standard or Custom profile reader
0005PU	Default configuration of a Custom profile reader. This Configuration ID can only be applied to a Custom profile reader.
00039T	Default configuration of a Smart profile reader. This configuration can only be applied to a Smart profile reader.

A.2.2 Delta Configuration IDs

Note: Delta Configuration IDs contain one specific reader configuration setting, or a limited number of reader configuration settings.

Configuration ID	Description
00416J	Turn off Bluetooth Low Energy (LE). Mobile credentials will not work.
00416P	Turn on Bluetooth Low Energy.
007T4R	Set the LED to blue. For HID Signo 20K and 40K readers, this Configuration ID will also set the keypad backlight to blue.
00G9L2	Set the LED to red. For HID Signo 20K and 40K readers, this Configuration ID will also set the keypad backlight to red.
007UP7	Disables I'm Alive.
007UPC	I'm Alive (with a default of 60 seconds).
0095W6	Disables anti-passback.
009HUP	Enables anti-passback (with a setting of 1 second).
00BX6X	Enables anti-passback (with a setting of 10 seconds).

Appendix **B**

Mercury Controller installation manuals

B.1 Corresponding HID controller manuals

Mercury controllers	Installation manual
LP1501	*HID® Mercury™ LP1501 Controller Installation and Specifications* (PLT-05243)
LP1502	*HID® Mercury™ LP1502 Controller Installation and Specifications* (PLT-05244)
LP2500	*HID® Mercury™ LP2500 Controller Installation and Specifications* (PLT-05245)
LP4502	*HID® Mercury™ LP4502 Controller Installation and Specifications* (PLT-05246)
MP1501	*HID® Mercury™ MP1501 Controller Installation and Specifications* (PLT-07669)
MP1502	*HID® Mercury™ MP1502 Controller Installation and Specifications* (PLT-07611)
MP2500	*HID® Mercury™ MP2500 Controller Installation and Specifications* (PLT-07667)
MP4502	*HID® Mercury™ MP4502 Controller Installation and Specifications* (PLT-07612)

Aero controllers	Installation manual
X1100	*HID® Aero X1100 Installation Guide* (PLT-04233)
X1100A	

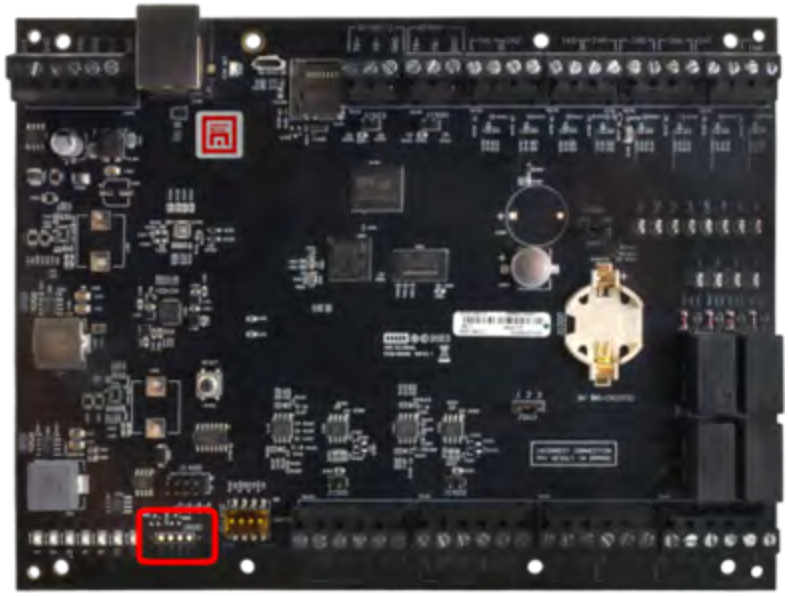
B.2 HID Controller DIP switches

To prove that you have physical access to the controller and are not attempting to access the device from a remote location, set the **S1: DIP Switch 1** to the following sequence:

On - **Off** - **Off** - **Off**

HID Aero controller

HID Mercury MP series controller



Appendix C

HID Linq Gateway secure deployment

C.1 Installation

Download from official sources

Only download HID Linq Gateway from official HID sources.

> **Important: Do not download HID Linq Gateway from a third-party as it may be compromised.**

Check digital signature

To check the authenticity of the download file:

1. Navigate to your **Downloads** folder.
2. Right-click the file and select **Properties**.
3. Navigate to the **Digital Signatures** tab.
4. Make sure there is a valid **HID Corporation Ltd** signature.

Update Windows

Make sure that your Windows operating system is up to date before downloading HID Linq Gateway, to help avoid potential vulnerabilities that could be exploited by malicious software.

Antivirus scan

Use a reputable antivirus software to make sure that your system is free from any malware or threats before downloading HID Linq Gateway.

System restore point

Create a system restore point, so that you have a stable system state to refer to if there are any problems during the installation of HID Linq Gateway.

Installation process

For the installation process, see **5.3 Install HID Linq Gateway**.

User account control

Windows may give User Account Control (UAC) warnings during the installation process. Only verify and proceed if you initiated the installation process.

Firewall settings

HID Linq Gateway may require network access for certain features. Check that your Windows firewall settings allow HID Linq Gateway to communicate securely over the network.

> **Note:** You may be required to **Allow an app through the firewall** in the Windows **Firewall & network protection** tab.

URL	Description
https://*.*.hidglobal.com/*	
https://a3p6nbw5omi6ja-ats.iot.us-east-1.amazonaws.com	Used by HID Origo Services API

Ports

If the following services are blocked, HID Linq Gateway will not work as expected.

Port	Description	Configurable
8885	Listens for connections from Mercury Panels	No

Port 8885 is listed above in the context of secure deployment of HID Linq Gateway.

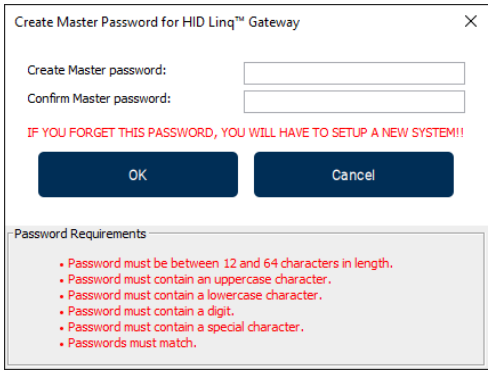
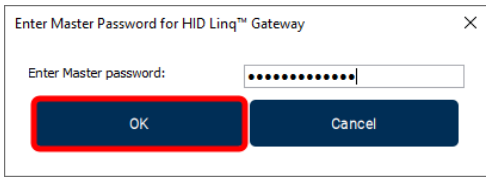
C.2 Running HID Linq Gateway

> **Note:** HID Linq Gateway and the Mercury panel must be on the same network. Perform a ping to make sure the PC can see the Mercury panel.

Gateway.exe	• Allows HID Linq On Premise to communicate with readers connected via USB to the local PC. • Allows HID Linq On Premise to communicate with readers connected via OSDP to specific Mercury panels.
Configuration.exe	• Allows configuration of HID Linq Gateway security profiles. • Facilitates the onboarding of Mercury panels.

C.3 Passwords

Important: If you forget your master password, you must uninstall HID Linq Gateway, delete the downloads and Zip file, and repeat the download process again. The password cannot be reset.

Description	Image
You will be prompted to Create a Master password: • The first time the software is started. • Switching from the relaxed security profile to the normal security profile.	
The Master password only applies to the normal security profile. You will be prompted to enter it when: • Starting the application. • Reconnecting to Linq On Premise after a network issue. • Switching from the relaxed security profile to the normal security profile. • While downloading a Mercury certificate.	

C.4 Security profiles

There are two security profiles available for HID Linq On Premise. See the following to select your required security profile.

Security profile	Description
Normal	• Data is secured using a master password. The password is not stored so the software relies on the user to provide it, for access to the necessary data. • The software must run using the same operating system account. No other user of the computer can use the software. • Service that allows browsers to detect that HID Linq On Premise is running through a WebSocket. • Application that helps facilitate communication between HID Linq On Premise and readers.
Relaxed	• Data is secured using a master password. The master password is cache encrypted on the PC. Any user of the computer can run the software without entering the master password. • Any operating system user can run HID Linq On Premise. • Service that allows browsers to detect that HID Linq On Premise is running through a WebSocket. • Application that helps facilitate communication between HID Linq On Premise and readers.

C.5 Updates and maintenance

- Keep HID Linq Gateway updated to ensure optimal performance and security.
- Perform regular maintenance tasks like scanning for malware, updating software, and backing up important data to maintain the security and integrity of your system.

C.6 User support

Contact the **Technical Support** team for further assistance if required.

Appendix D

Logs

D.1 Logs

When contacting HID Technical Support, you will need access to the HID Linq On Premise logs. Navigate to **C:\ProgramData\HID Global\HID Linq™ Gateway\logs**.

Appendix E

MIFARE Custom Programming Credentials

E.1 MIFARE DESFire credential values

Parameter	Value
Application ID	Six digit hex string
File ID	Two digit hex string
File Size	Bytes
Authentication Key Number	• KeyA_Key0 • KeyB_Key1 • Key2 • Key3 • Key4 • Key5 • Key6 • Key7 • Key8 • Key9 • KeyA • KeyB • KeyC • KeyD • FullAccess • NoAccess
Authentication Key Algorithm	• None • DES • AES
Authentication Key Diversification Algorithm	• None • AES_3DES • AV2-AES_AES_3DES • SDES
Random UID	• None • DES • AES
Communication Mode	• Plain • MAC • ENCRYPT • UNKNOWN
Custom Key	Keyset name from HID Ling Custom Keystore
DESFire functionality	
Proximity Check	Enable / Disable
Key (Proximity Check enabled)	Keyset name from HID Linq Custom Keystore
Time Margin (Proximity Check enabled)	Integer
Count (Proximity Check enabled)	Integer

Parameter	Value
EV2 Secure Messaging	Enable / Disable
Data Structure	
Start bit	Integer
Length	Integer
Output Length	Integer
Data Representation	• None • ByteReversed
Data Type	• Raw • BinHex • Int32 • BCDNibble • BCDByte • ASCIIDecimal • ABATrack2String • HKBU
Fixed Value	Integer
Tag	Integer
Data Search	Integer
Data Structure	• Field • IE • GM
Output Format	• None • Wiegand • ABATrack2 • ASCIIDecimal
ETX Code	• None • Fixed0 • Fixed1 • EvenParity • OddParity
ETX Number of Bits	Integer
STX Code	• None • Fixed0 • Fixed1 • EvenParity • OddParity
STX Number of Bits	Integer
Diversification	

Parameter	Value
Diversification Input: Type	• NXP AN10922 (UID+AID+SYSID) • NXP AN10957 (UID+Padding) • 1+UID+PADDING • 88+UID+88+Padding
Diversification Input System ID	Hex string of paired hex digits

E.2 MIFARE Classic credential values

Parameter	Value
Application ID	Four digit hex string
File ID	Two digit hex string
File Size	Bytes
Authentication Key Number	• KeyA_Key0 • KeyB_Key1
Authentication Key Algorithm	• None • MIFARE
Custom Key	Keyset name from HID Ling Custom Keystore
Data Structure	
Start bit	Integer
Length	Integer
Output Length	Integer
Data Representation	• None • ByteReversed
Data Type	• Raw • BinHex • Int32 • BCDNibble • BCDByte • ASCIIDecimal • ABATrack2String • HKBU
Fixed Value	Integer
Tag	Integer
Data Search	Integer
Data Structure	• Field • IE • GM
Output Format	• None • Wiegand • ABATrack2 • ASCIIDecimal
ETX Code	• None • Fixed0 • Fixed1 • EvenParity • OddParity

Parameter	Value
ETX Number of Bits	Integer
STX Code	• None • Fixed0 • Fixed1 • EvenParity • OddParity
STX Number of Bits	Integer
Diversification	
Diversification Input: Type	• NXP AN10922 (UID+AID+SYSID) • NXP AN10957 (UID+Padding) • 1+UID+PADDING • 88+UID+88+Padding
Diversification Input System ID	Hex string of paired hex digits

Appendix F

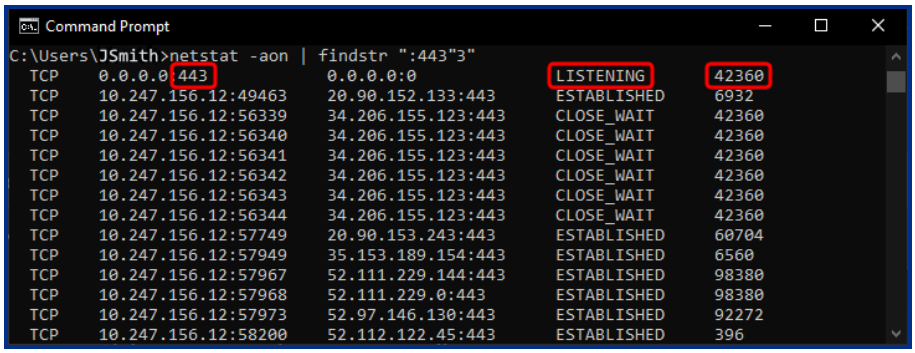
Troubleshooting

F.1 Port conflict troubleshooting

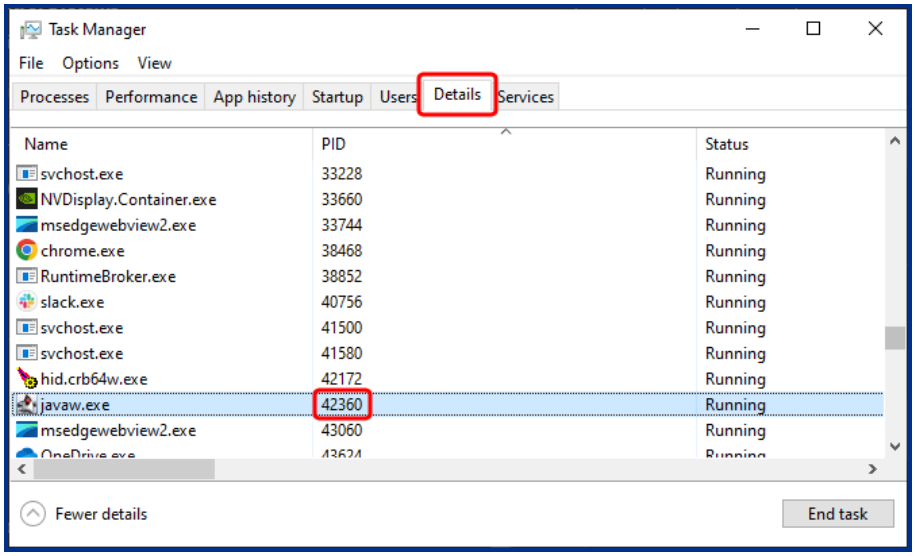
HID Linq On Premise uses port 443 by default. If an existing application is using port 443, the HID Linq On Premise web browser will not open.

To locate the application using port 443:

1. Open the Command Prompt.
2. Enter `netstat -aon | findstr ":443"` and press **Enter**.
3. Make a note of the PID of the application using port 443.



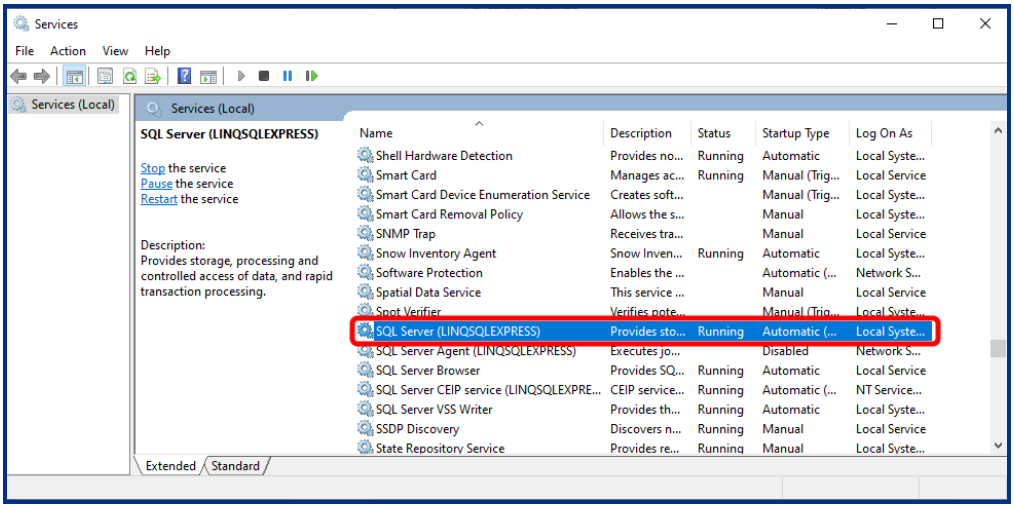
4. Open Windows Task Manager and select navigate to the **Details** tab.
5. Use the PID noted in step 3 to locate the application. Close the application and restart HID Linq On Premise.



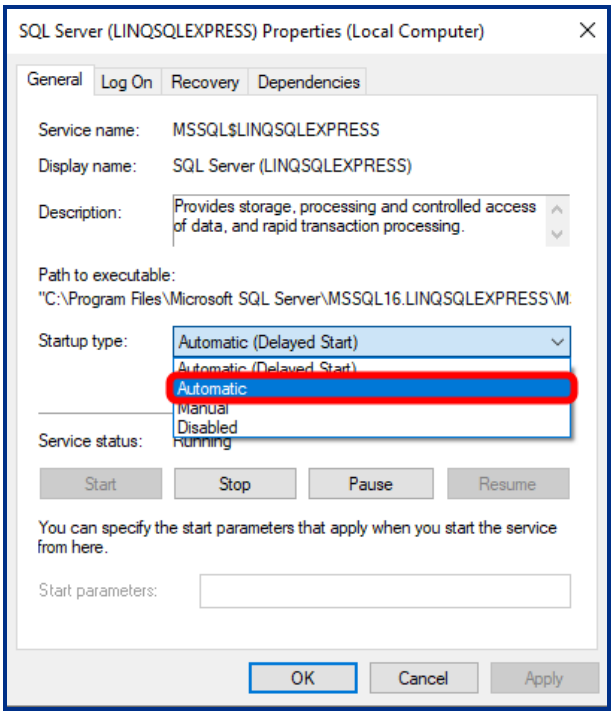
F.2 SQL Server troubleshooting

The HID Linq On Premise server auto start fails when it cannot connect to the database. To fix this issue, the SQL Server **Startup type** can be changed.

1. Open the Windows Services window.
2. Right-click **SQL Server (LINQSQLEXPRESS)** and select **Properties**.



3. Select **Automatic** from the **Startup type** drop-down list.



4. Click **Apply** and click **OK**.

F.3 Enter Database password for HID Linq On Premise

If an old version of SQL Server or SSMS has been installed prior to HID Linq On Premise, the HID Linq Database password might be rejected.

Troubleshoot the automatic installation of SQL Server 2022 Express by navigating to **C:\Program Files\Microsoft SQL Server\160\Setup Bootstrap\Log**. Open the **Summary.txt** file and check the latest installation date.

To uninstall all older versions of SQL and related tools before reinstalling HID Linq On Premise:

> **Important: Only complete the following steps if it is the initial installation. Deleting files for an existing setup will destroy customer data.**

- Uninstall all SQL Server related services from Windows
- Uninstall HID Linq On Premise
- Delete **C:\Program Files\HID Global\Linq Device Manager**
- Delete **C:\ProgramData\HID Global\Linq Device Manager**

F.4 Mercury panel does not connect to the HID Linq Gateway

If the time on the Mercury panel is incorrect, a certificate error is given in the logs. See **Logs** for more information on logs.

To check for the bad certificate:

1. Navigate to **C:\ProgramData\HID Global\HID Linq™ Gateway\logs**.
2. Search **bad_certificate** in the HID Linq Gateway logs.

   > **Note:** Return example: [WARN] UTC:2025-Jan-27 17:42:38.685 - Could not accept connection from tcp://192.168.0.251:57416: javax.net.ssl.SSLHandshakeException: Received fatal alert: **bad_certificate** (Received fatal alert: **bad_certificate**)
3. Check the time on the Mercury panel is correct.
4. Check the jumpers of the Mercury panel Real Time Clock (RTC) are in the ON position.

F.5 Readers unavailable troubleshooting

Readers are grayed out when HID Linq On Premise cannot retrieve the reader information from HID Origo. There are several reasons a reader is grayed out:

The user performing a reader discovery does not have a HID Reader Technician account configured

HID Linq On Premise cannot reach HID Origo to query the reader information from the digital twin. See **4.1 HID Origo account** for information on connecting a HID Origo account to HID Linq On Premise.

The computer IP Address has changed since HID Linq On Premise install

The websocket server only accepts connections where the origin header is included in the allowed server SAN (default) list. See **4.10.1 Manually perform a system recovery** to import the recovery key. This regenerates the CA certificate and webserver certificate.

> **Note:** Any certificate connections need to be set up again. For example HID Linq Gateway, HID Linq™ Mobile or any future server connected devices.

No internet connection

Check your internet connection.

Revision history

Date	Description	Revision
July 2025	Updated to support HID Linq On Premise software version v1.3.0.	A.1
March 2025	Initial release.	A.0

hidglobal.com

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

PLT-08128, Rev. A.1

Part of ASSA ABLOY