



HID[®] Reader Manager[™] Solution

User Guide (Android)

PLT-03858, A.9
July 2021

Powering
Trusted Identities

Copyright

© 2018 - 2021 HID Global Corporation/ASSA ABLOY AB. All rights reserved.

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

Trademarks

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

Contacts

HID Global Technical Support: www.hidglobal.com/support.

| Americas and Corporate | Asia Pacific |
|---|--|
| 611 Center Ridge Drive Austin, TX 78753 USA Phone: +1 866 607 7339 | 19/F 625 King's Road North Point, Island East Hong Kong Phone: +852 3160 9833 |
| Europe, Middle East, and Africa (EMEA) | Brazil |
| 3 Cae Gwyrdd Green Meadow Springs Cardiff CF15 7AB United Kingdom Phone: +44 (0) 1440 711 822 | Condomínio Business Center Av. Ermano Marchetti, 1435 Galpão A2 - CEP 05038-001 Lapa - São Paulo / SP Brazil Phone: +55 11 5514-7100 |

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

What's new

| Date | Description | Revision |
|-----------|--|----------|
| July 2021 | <ul style="list-style-type: none"> ■ Section 1.1 and B.1. Updated sections to state HID Reader Manager support for HID Signo Express readers. ■ Section 2.4.1 (Credential details). Updated section to state the credential profiles that are available for HID Signo Express readers. ■ Section 2.4.1 (ISO14443A UID Output Format settings). Updated section for the ability to enable/disable the Raw Data option and the 64-Bit LSB format option. ■ Section 2.4.4 Reader Inspection report. Updated section and screenshots for the ability to identify the Reader Model for Signo readers. | A.9 |

A complete list of revisions is available in [Revision history](#).

| | |
|---|-----------|
| Introduction | 5 |
| 1.1 Document purpose | 6 |
| 1.2 Intended audience | 6 |
| 1.3 HID Reader Manager solution overview | 7 |
| 1.3.1 Key authorization | 8 |
| 1.4 Reader and Mobile device compatibility | 8 |
| 1.4.1 Readers | 8 |
| 1.4.2 Mobile devices | 8 |
| HID Reader Manager App | 9 |
| 2.1 Overview | 10 |
| 2.2 Mobile application setup overview | 10 |
| 2.2.1 Prerequisites | 10 |
| 2.2.2 HID Reader Manager setup overview | 10 |
| 2.2.3 Download and install the Reader Manager app | 11 |
| 2.2.4 Register a new account within the app | 12 |
| 2.2.5 Log into the HID Reader Manager app | 14 |
| 2.2.6 Activate the HID Reader Manager app | 15 |
| 2.2.7 Display authorized keys | 16 |
| 2.2.8 HID Reader Manager app settings | 17 |
| 2.3 Reader configuration | 20 |
| 2.3.1 Test configuration changes | 20 |
| 2.4 Basic app functionality | 21 |
| 2.4.1 Create a new template | 21 |
| 2.4.2 Manage templates | 32 |
| 2.4.3 Connect to a reader | 36 |
| 2.4.4 Reader inspection report | 38 |
| 2.4.5 Firmware upgrade | 39 |
| 2.4.6 View detailed reader configuration | 40 |
| 2.4.7 Apply configuration changes | 43 |
| 2.4.8 Change reader name | 44 |
| HID Reader Manager Service | 45 |
| 3.1 Overview | 46 |
| 3.2 Mobile Access setup | 46 |
| 3.2.1 Reader Manager service | 46 |
| 3.3 Access the Reader Manager service | 47 |
| 3.4 Enroll a Reader Technician | 49 |
| 3.4.1 Edit Reader Technician information | 52 |
| 3.4.2 Delete an enrolled Reader Technician | 54 |

| | |
|---|-----------|
| 3.5 Issue authorization keys | 56 |
| 3.5.1 Edit authorization key information | 59 |
| 3.5.2 Revoke (delete) an authorization key | 60 |
| 3.6 Configure HID Reader Manager service settings | 63 |
| 3.6.1 Export Reader Technician record settings | 64 |
| 3.6.2 Invitation Email settings | 64 |
| 3.6.3 Configure Delete Threshold | 65 |
| 3.7 Add additional Reader Manager Admin | 66 |
| 3.8 Edit existing Admin Services and Roles | 69 |
| Troubleshooting | 71 |
| 4.1 Reader Manager App messages | 72 |
| 4.1.1 Error and warning messages | 72 |
| 4.1.2 Information messages | 74 |
| 4.1.3 Validation messages | 74 |
| 4.2 Contact HID Technical Support | 75 |
| Reader upgrade | 76 |
| A.1 Supported firmware versions for upgrade | 77 |
| A.1.1 HID SE readers | 77 |
| A.1.2 HID SE Express readers | 78 |
| A.1.3 HID Signo reader | 79 |
| A.2 iCLASS SE reader upgrade | 80 |
| A.2.1 iCLASS SE Bluetooth & OSDP upgrade kits | 80 |
| A.2.2 iCLASS SE/multiCLASS SE Bluetooth & OSDP upgrade kit instructions | 81 |
| A.2.3 Configure reader in HID Reader Manager | 83 |
| Identify HID reader models | 86 |
| B.1 Physically inspect reader | 87 |
| B.2 Check the product labeling | 88 |
| B.2.1 HID Signo readers | 88 |
| B.2.2 iCLASS SE readers | 89 |
| B.2.3 Mobile-Capable readers | 89 |
| B.2.4 Mobile-Enabled and Mobile-Ready readers | 89 |
| B.3 Check the reader firmware version with Reader Manager | 90 |
| Glossary | 91 |
| C.1 Glossary | 92 |

Section **01**

Introduction

1.1 Document purpose

This document provides an overview of the HID® Reader Manager™ solution and provides information and procedures for Reader Manager Administrators and Technicians to:

- Download and install the HID Reader Manager mobile app.
- Register and authenticate the HID Reader Manager app on a mobile device.
- Enroll Reader Technicians and issue Authorization Keys through the HID Reader Manager service.
- Inspect and change reader configurations for:
 - HID® Signo™ readers (including HID® Signo™ Express readers)
 - The iCLASS SE® Express R10 reader
 - Supported iCLASS SE®/multiCLASS SE® readers
- Update reader firmware for HID® Signo™ readers, the iCLASS SE® Express R10 reader, and supported iCLASS SE®/multiCLASS SE® readers.
- Upgrade supported Mobile-Capable iCLASS SE/multiCLASS SE readers with Bluetooth Low Energy (BLE) modules.

1.2 Intended audience

This document is intended for personnel performing the following roles:

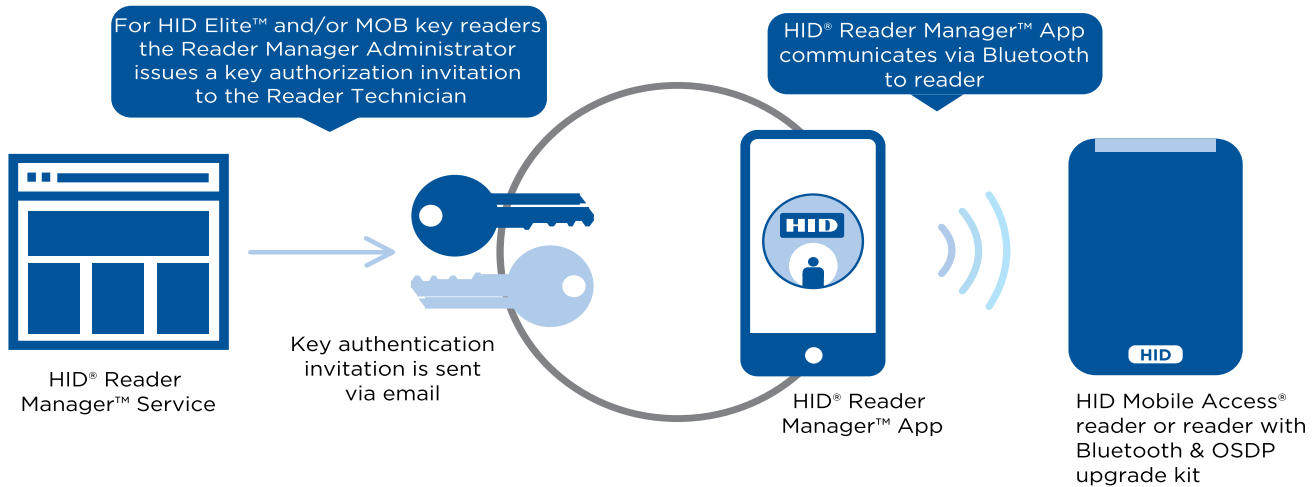
- **Reader Manager Administrator:** the Reader Manager Administrator performs the following tasks:
 - HID Reader Manager service account management.
 - Enrolling Reader Technicians and issuing invitation codes.
 - Issuing and revoking authorization keys.
- **Reader Manager Technician:** the Reader Manager Technician performs the following tasks:
 - Carrying out compatibility checks for the reader and HID Reader Manager app.
 - Self-registration within the HID Reader Manager app.
 - Linking the Reader Manager app to the Reader Manager service via an issued invitation code.
 - Performing reader configuration changes and firmware upgrades.
 - Reader configuration update testing.

1.3 HID Reader Manager solution overview

The HID Reader Manager solution streamlines management of BLE capable readers in the field. Administrators can easily adjust certain configuration settings (for example audio/visual settings, BLE read range settings), upgrade firmware, inspect connected reader status and extend functionality on HID Signo readers, the iCLASS SE Express R10 reader, and supported iCLASS SE/multiCLASS SE readers. The main components of the HID Reader Manager solution are:

- **HID Reader Manager Application:** Mobile app which connects, via Bluetooth, to a reader for configuration changes, firmware upgrades and reader inspections by Reader Technicians.
- **HID Reader Manager Service:** A service accessed via the HID® Origo™ Management Portal which facilitates Reader Technicians to use the HID Reader Manager App with readers that have HID Elite™ and/or MOB keys. The service is used by HID Elite and/or MOB key Reader Manager Administrators to issue Key Authorization to only authorized Reader Technicians.

Note: The HID Reader Manager App can be used to configure Standard Key readers, however the Reader Manager service is not required for Standard Key readers as these do not use HID Elite and/or MOB keys.
- **iCLASS SE/multiCLASS SE Bluetooth and OSDP Upgrade Kit:** Plug-in module and adhesive reflector back plate kit, to be used with the HID Reader Manager App to upgrade readers to support Bluetooth and/or Open Supervised Device Protocol (OSDP). For more information, refer to the [Reader upgrade](#) section.



1.3.1 Key authorization

HID Reader Manager uses key authorization to:

- Securely connect and control access by the mobile app to HID Signo readers, the iCLASS SE Express R10 reader, and iCLASS SE/multiCLASS SE readers using either of two keyset types:
 - Mobile (MOB####): Issued for HID Mobile Access credentials only.
 - HID Elite (ICE####): Issued for HID Elite physical and/or HID Mobile Access credentials.
- Securely pair the readers and credentials to ensure only matching secure pairs will communicate with each other.

Each key is specific to the individual customer and are issued when enrolling into either the HID Mobile Access or HID Elite credential programs.

Important: Access to authorization keys must be carefully controlled to ensure only authorized personnel have configuration access to readers and to prevent keys being used and loaded onto unauthorized readers.

1.4 Reader and Mobile device compatibility

1.4.1 Readers

The HID Reader Manager solution is only compatible with HID Signo readers, the iCLASS SE Express R10 reader, and iCLASS SE/multiCLASS SE Rev E readers (with Bluetooth & OSDP module installed). While most firmware versions of iCLASS SE and multiCLASS SE Rev E readers are compatible you will need to verify this, even if the reader is “Mobile-ready” or “Mobile-enabled”.

For details on supported firmware versions, refer to the [Reader upgrade](#) section.

1.4.2 Mobile devices

The HID Reader Manager application is compatible and available for Android and iOS mobile devices. As more versions are added with new releases you will need to check for version compatibility at:

<https://www.hidglobal.com/reader-manager-system-requirements>

Section **02**

HID Reader Manager App

2.1 Overview

This section provides the required steps and procedures to be performed by the Reader Technician in order to install, register, and activate the HID® Reader Manager™ app on a mobile device. The section also provides information on the functionality of HID Reader Manager app.

2.2 Mobile application setup overview

2.2.1 Prerequisites

Note: The following prerequisites only apply to HID Elite™ or Mobile (MOB) key users:

- A Mobile Access account is established for the organization through the HID Global onboarding process. See [3.2 Mobile Access setup](#).
- The Reader Manager service instance is available for the Organization. See [3.2.1 Reader Manager service](#).
- A Reader Manager Administrator has been setup and enabled for the Organization's Reader Manager service instance.

2.2.2 HID Reader Manager setup overview

The HID Reader Manager app setup process consists of the following steps:

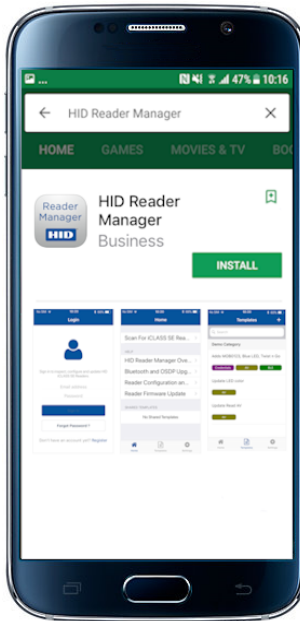
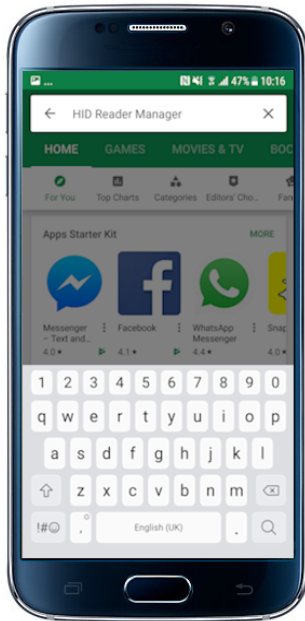
1. The Reader Technician downloads and installs the HID Reader Manager app onto a mobile device. See [2.2.3 Download and install the Reader Manager app](#).
2. The Reader Technician performs registration with the HID Reader Manager app. See [2.2.4 Register a new account within the app](#).

The following additional setup steps are required for HID Elite or Mobile (MOB) key users:

1. The Reader Manager Administrator enrolls the Reader Technician using the Reader Manager service and issues an invitation code and key authorization. See the [HID Reader Manager Service](#) section.
2. The Reader Technician activates the issued invitation code in the HID Reader Manager app. See [2.2.6 Activate the HID Reader Manager app](#).
3. The Reader Technician verifies key authorization has been received in the HID Reader Manager app. See the [HID Reader Manager Service](#) section.

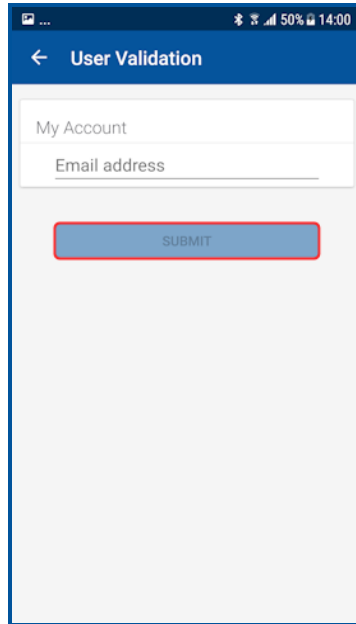
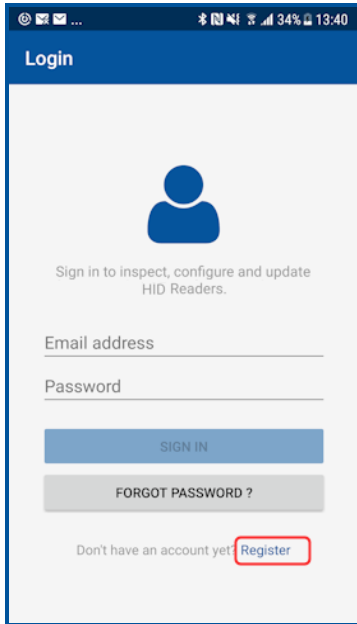
2.2.3 Download and install the Reader Manager app

1. Ensure your Android mobile device is connected to the Internet, either via mobile data network or Wi-Fi.
2. On your mobile device go to the Google Play (for Android devices).
3. Search for **HID Reader Manager**.
4. Download and install the app on your mobile device.

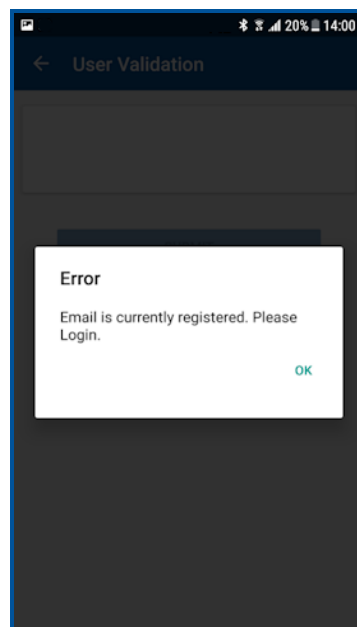
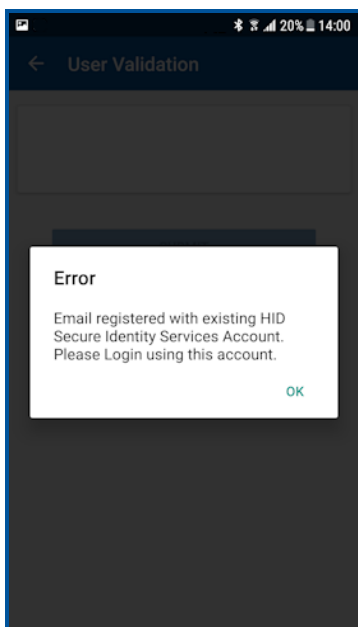


2.2.4 Register a new account within the app

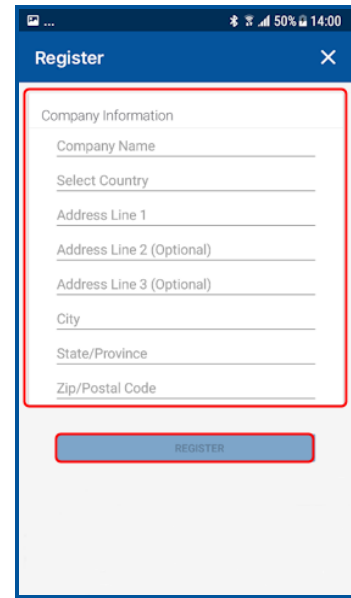
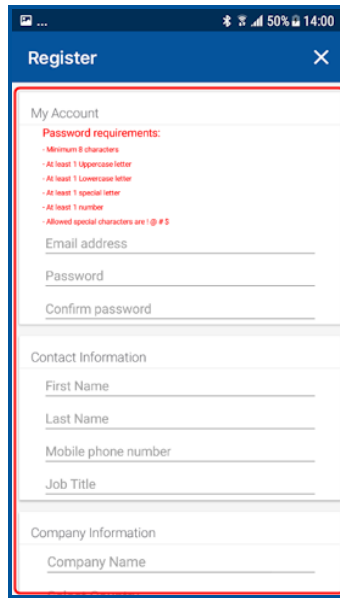
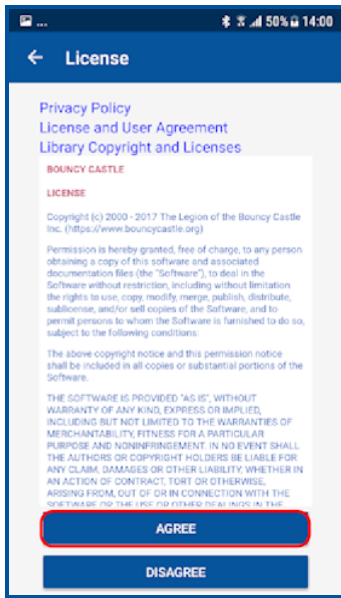
1. Open the HID Reader Manager app on your mobile device.
2. On the **Login** screen, tap the **Register** link.
3. On the **User Validation** screen, enter your email address and tap **SUBMIT**.



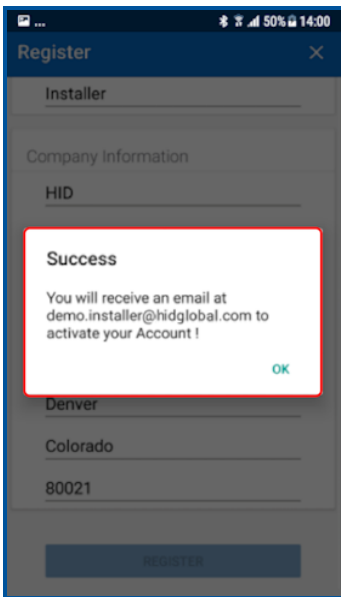
Note: If the entered email address is associated with an existing HID Origo™ Management Portal account (for example, an Org Admin or Reader Manager Admin) or the email address is already registered then the following messages are displayed. Tap **OK** to return the **Login** screen and use your existing roles' credential to log into Reader Manager. See [2.2.5 Log into the HID Reader Manager app](#).



- On the **License** screen, read the privacy policies and license agreements and tap **AGREE**.
Note: Tapping **DISAGREE** will return you to the **User Validation** screen.
- Enter your registration details (optional fields are indicated) and tap **REGISTER**.



- After receiving a **Success** prompt, tap **OK**.



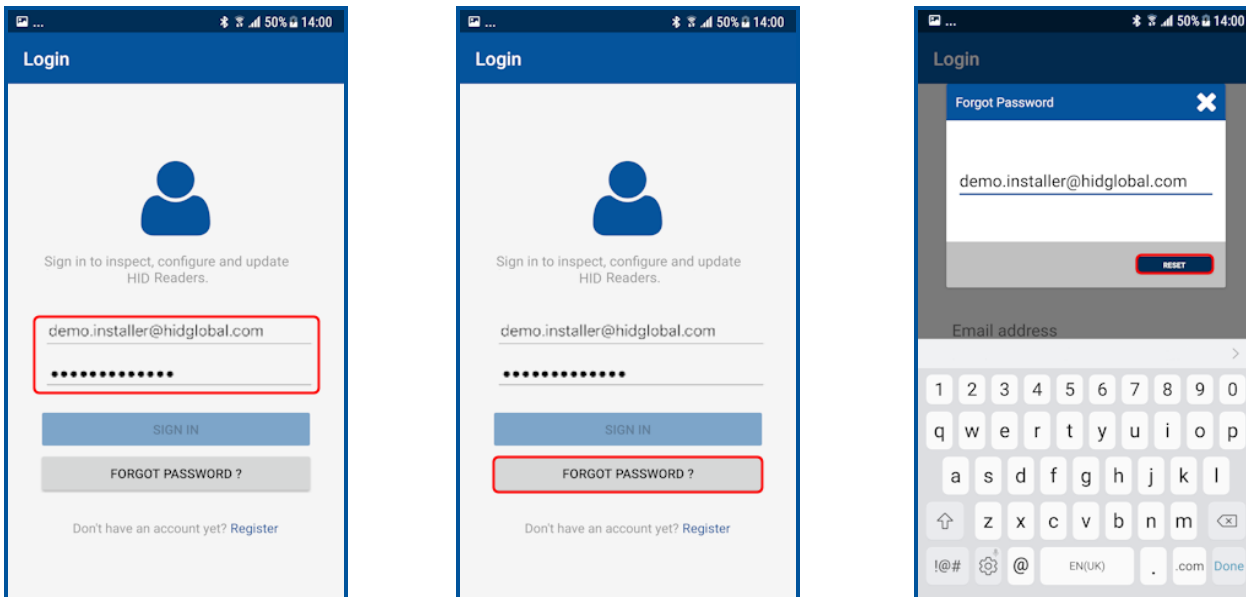
- Check your registered email account for a HID Reader Manager email containing an activation link. If you do not receive the HID Reader Manager email within a few minutes of registration, check your Spam or Junk Email folder in case the email was delivered there instead of your Inbox.
- Open the HID Reader Manager email and click on the activation link included in the email.
Note: The activation link has an expiry date which is indicated in the email. If the activation link has expired please contact HID Technical Support.
- A successful activation message will appear in a new browser. You can now log into the HID Reader Manager app using the registered email address and password.

2.2.5 Log into the HID Reader Manager app

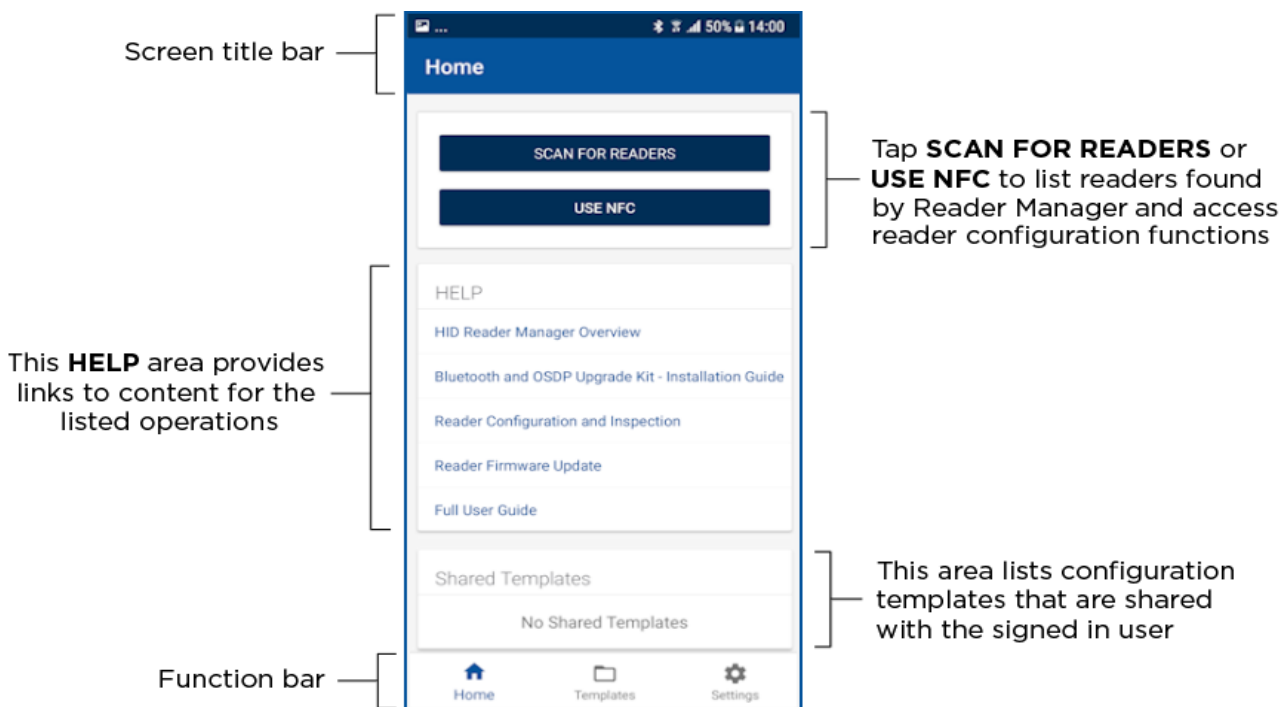
When the account registration process has been completed you can log into the HID Reader Manager app using the email address and password details provided during registration.

If you have forgotten your login password, tap **FORGOT PASSWORD?**. Enter your email address and tap **RESET**. Your password will be reset through the management portal therefore check your registered mail account for a password reset notification email.

Note: If the login credentials are associated with an Org Admin or Reader Manager Admin then the password will need to be reset in the HID Origo Management Portal.



Home screen layout



2.2.6 Activate the HID Reader Manager app

Note: This section does not apply to Standard Key readers as these do not use HID Elite and/or MOB Keys.

Prior to activating the HID Reader Manager app, the Reader Manager Administrator must enroll the Reader Technician within the HID Reader Manager service. See [3.4 Enroll a Reader Technician](#).

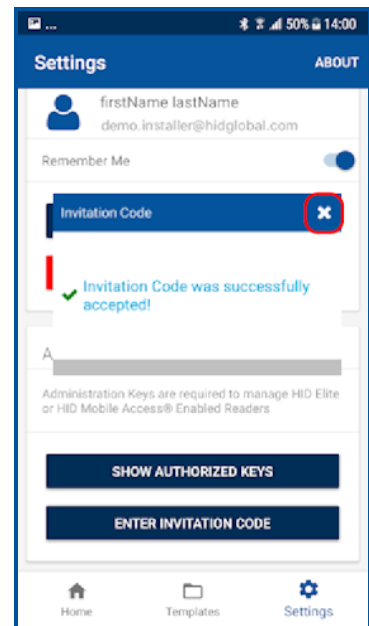
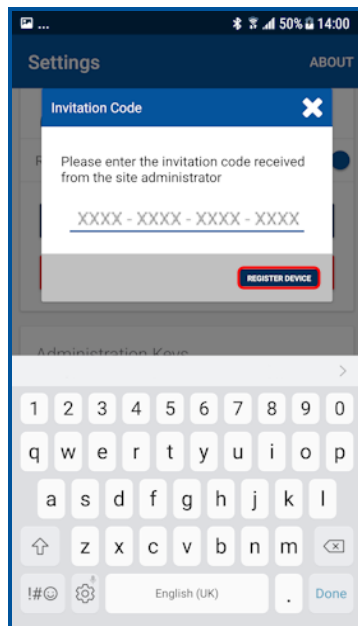
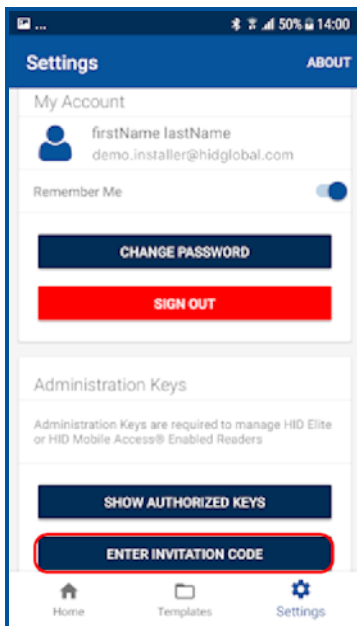
Once the Reader Manager Administrator has enrolled a Technician within the HID Reader Manager service an invitation email will be sent to the Technician's registered email address containing an invitation code.

To activate an invitation code in the HID Reader Manager app:

1. Log into the HID Reader Manager app using your registered email and password.
2. On the **Home** screen, tap the **Settings** icon.
3. Open the invitation email on the device and tap the invitation link. The invitation code will be automatically entered in the Reader Manager App. Alternatively, manually enter the invitation code by tapping **ENTER INVITATION CODE** on the **Settings** screen.
4. Tap **REGISTER DEVICE**.

Note: The invitation code is a one time use code.

An **Invitation code was successfully accepted!** message will display if the code was valid and entered correctly. Tap **X** to close.

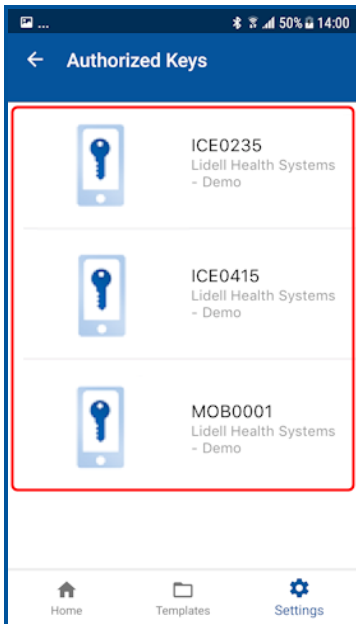
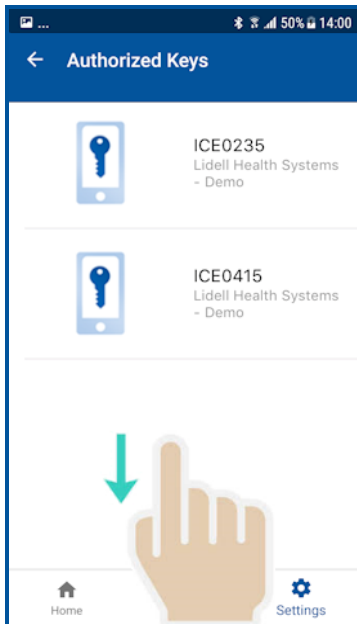
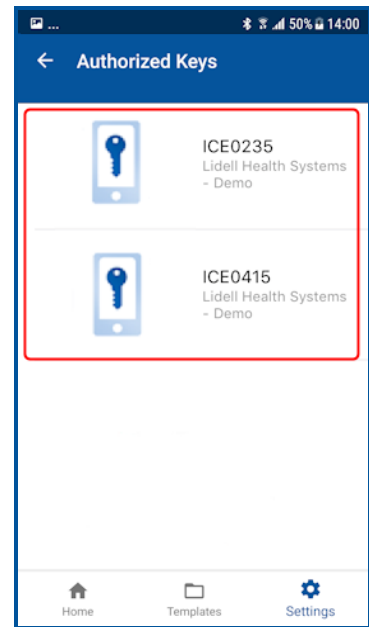
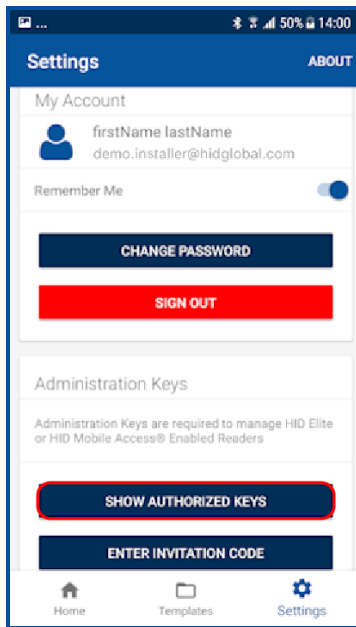
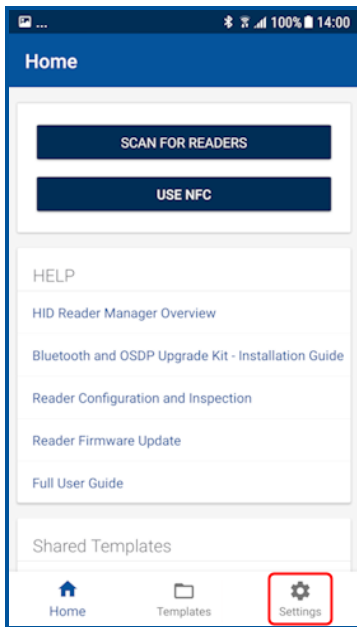


2.2.7 Display authorized keys

Note: This section does not apply to Standard Key readers as these do not use HID Elite and/or MOB Keys. Authorized keys issued via the Reader Manager service can be viewed in the Reader Manager app:

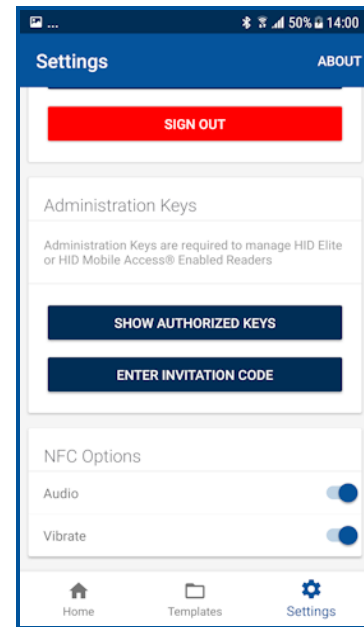
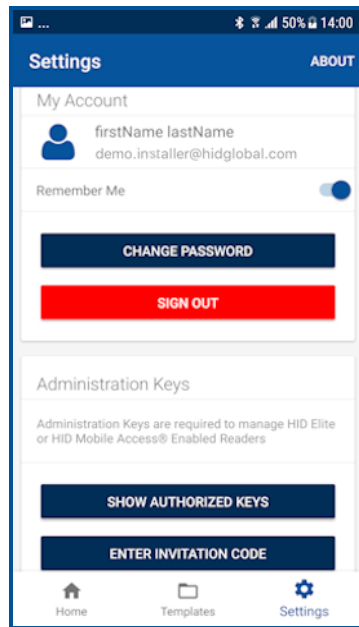
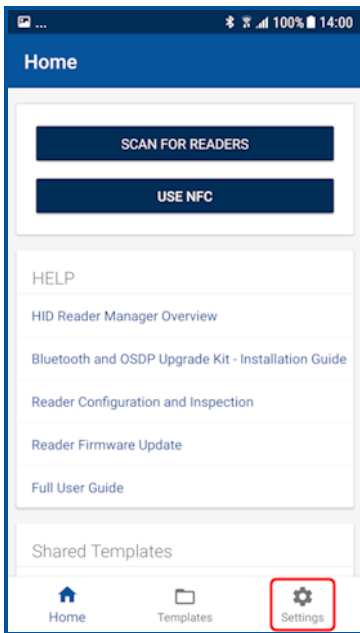
1. On the **Home** screen, tap the **Settings** icon .
2. Tap **SHOW AUTHORIZED KEYS** to display authorized keys.

Note: Authorized keys are added the app memory and will only be visible after a screen refresh. If an authorized key is not displayed swipe down to refresh the screen.



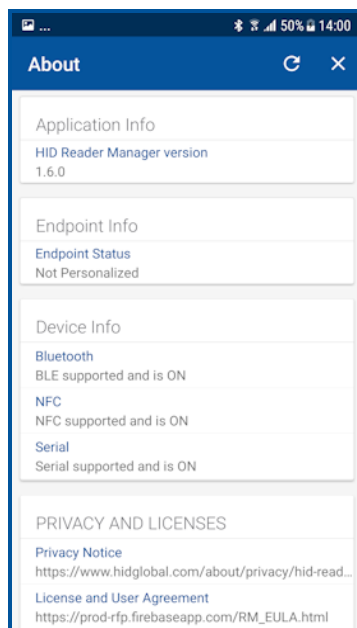
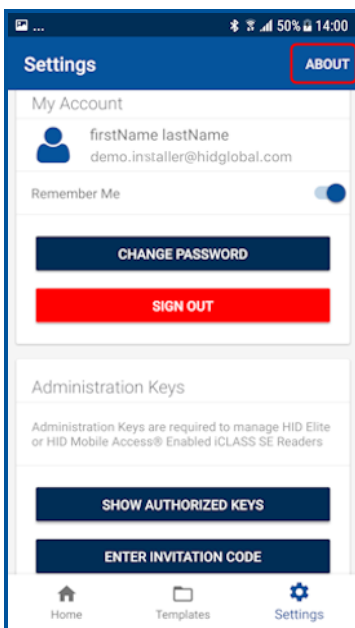
2.2.8 HID Reader Manager app settings

On the **Home** screen, tap the **Settings** icon to access HID Reader Manager app settings.



About HID Reader Manager

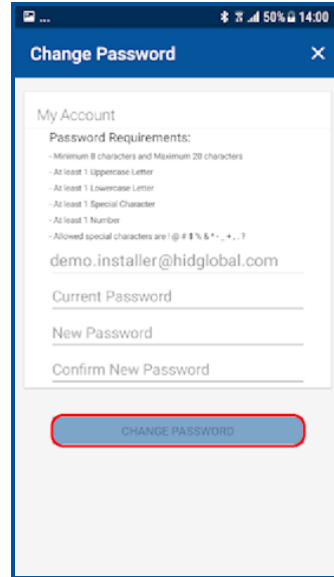
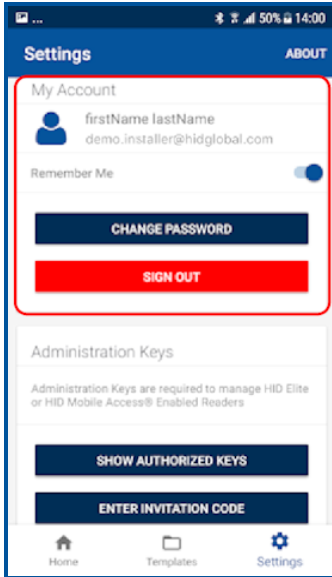
On the **Settings** screen, tap **About** to display Application, Endpoint, and Device information as well as Privacy and License agreements.



My Account

The **My Account** area displays user account information and provides the following options:

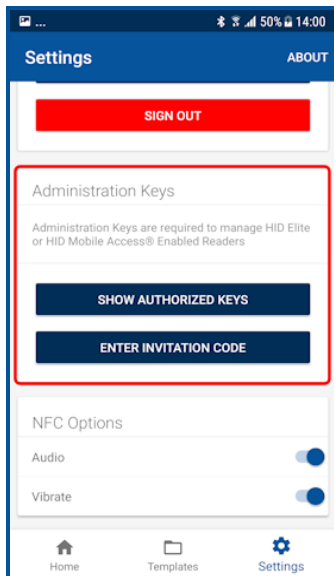
- **Remember Me:** enable this option to enable the system to remember your account information.
- **CHANGE PASSWORD:** tap to access the **Change Password** screen. Enter a new app login password (refer to the on screen password requirements) and tap **CHANGE PASSWORD**.
Note: If the login credentials are associated with an Org Admin or Reader Manager Admin then the password will need to be reset in the HID Origo Management Portal.
- **SIGN OUT:** tap to exit the app.



Administration Keys

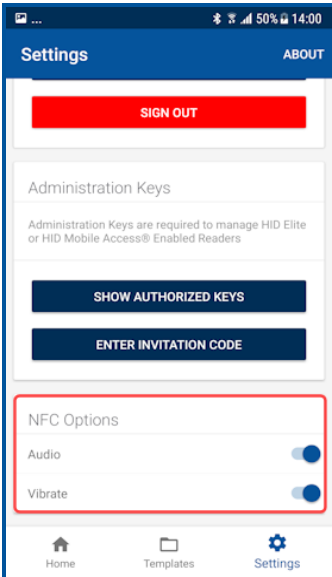
In the **Administration Keys** area the following functions are available:

- **SHOW AUTHORIZED KEYS:** displays a list of the issued authorized keys.
- **ENTER INVITATION CODE:** allows you to enter and activate the issued invitation code in the app.



NFC Options

In the **NFC Options** area the **Audio** and **Vibrate** indicators can be enabled/disabled for NFC interactions.



2.3 Reader configuration

The HID Reader Manager solution is only compatible with iCLASS SE®/multiCLASS SE® Rev E readers (with Bluetooth & OSDP module installed), the iCLASS SE® Express R10 reader, and HID® Signo™ readers.

The process to apply configuration changes to a reader consists of the following steps:

1. The Reader Technician checks the reader firmware version and, if necessary, performs a reader firmware upgrade. See [2.4.5 Firmware upgrade](#).
2. The Reader Technician creates a configuration template to simplify programming the reader. See [2.4.1 Create a new template](#).
3. The Reader Technician applies the created configuration template to the reader. See [2.4.7 Apply configuration changes](#).

2.3.1 Test configuration changes

It is important to fully test any configuration changes performed with the HID Reader Manager app to ensure complete working functionality:

- If you have upgraded to Mobile Access, test mobile credentials with the Mobile Access app to confirm communication with the reader and BLE operations perform as configured.
- If you have loaded any mobile keys, ensure that all credentials work at the reader.

2.4 Basic app functionality

2.4.1 Create a new template

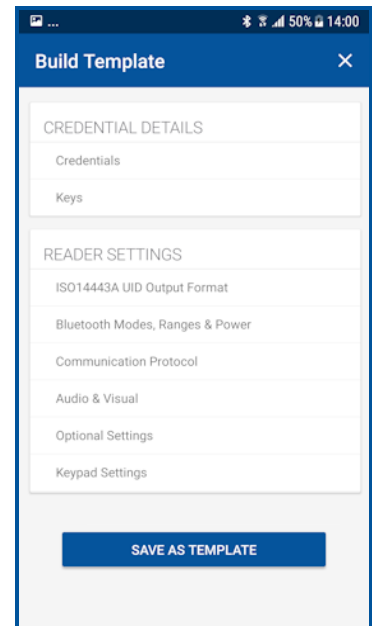
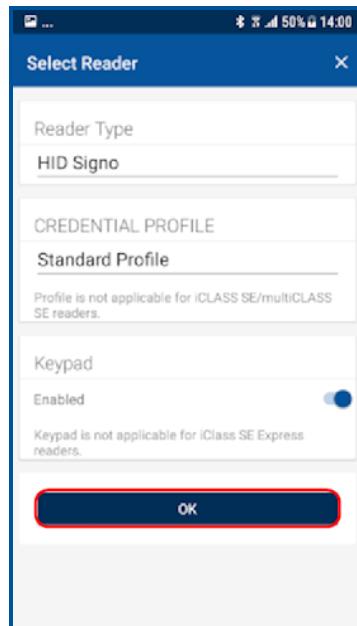
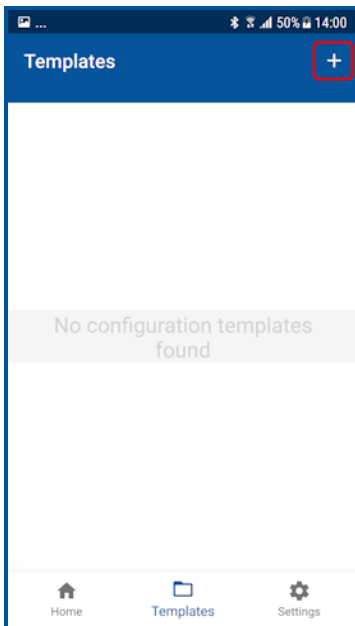
Templates store reader settings. When a template is created it can be applied to multiple readers that require the same configuration or shared with other Technicians to speed up the configuration of multiple readers.

Note: HID is continuously adding new reader features and functionality which can result in technical limitations being introduced into existing older templates. It is therefore recommended that new templates are routinely created so that they continue to be compatible with the latest available versions of Reader Manager that support all reader functions.

To create a new template:

1. On the **Home** screen, tap the **Templates** icon and on the **Templates** screen, tap the plus icon [+].
2. Tap in the **READER TYPE** field and select a reader type from the displayed list.
3. Tap in the **CREDENTIAL PROFILE** field and select a credential profile from the displayed list (HID Signo readers and HID iCLASS SE Express R10 only).
4. If applicable enable the **KEYPAD** option (HID Signo readers and iCLASS SE/multiCLASS SE only).
5. Tap **OK**.

From the **Build Template** screen you can configure and add settings to a template. Templates only need to include the reader configuration settings that are applicable to the selected reader type. Template settings are described in the following sections.



Credential details

1. From the **CREDENTIAL DETAILS** section, tap **Credentials**.

Note: For HID Signo readers, the credential profile is displayed. For HID® Signo™ Express readers the following credential profiles are supported:

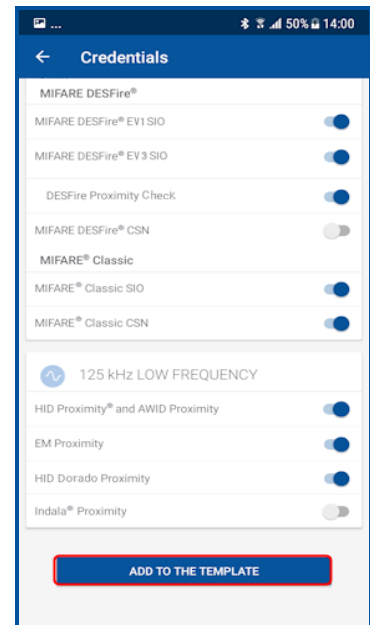
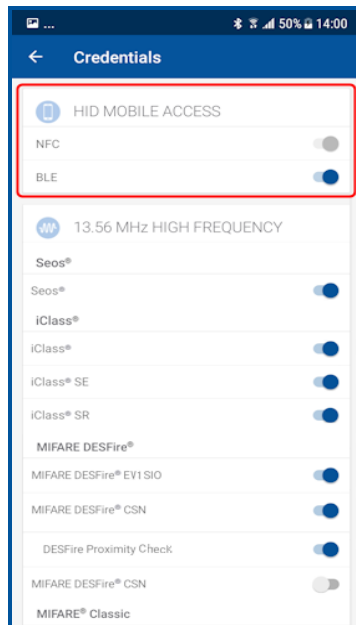
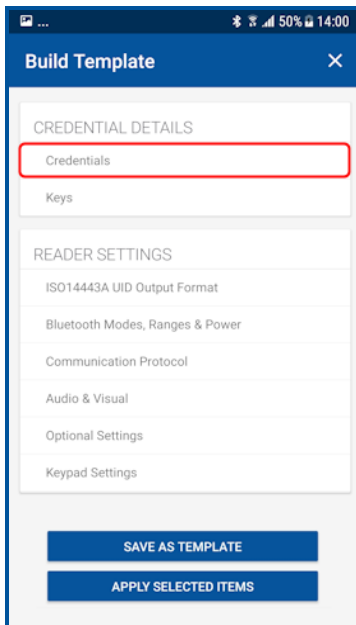
- Seos (without BLE)
- Seos (with BLE)
- Seos + CSN (without BLE)
- Seos + CSN (with BLE)

2. Select the required communication protocol option, **NFC** or **BLE**.
3. Enable/disable the required credential types.

Note:

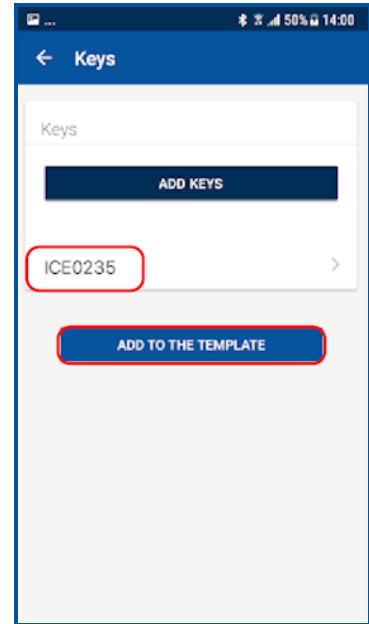
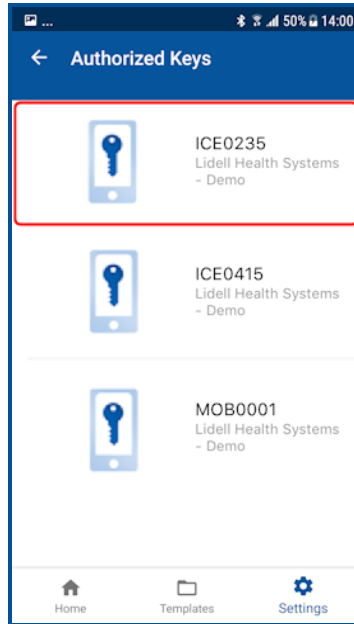
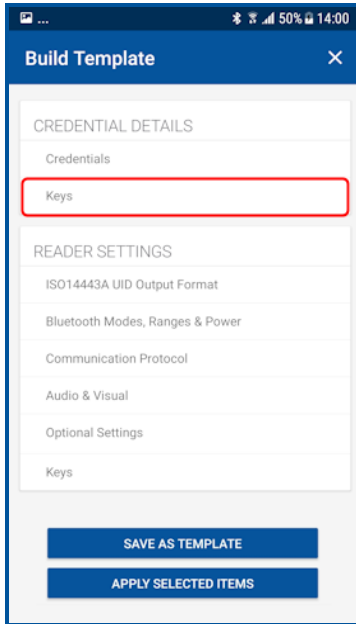
- The list of displayed credential options depends on the selected credential profile.
- The options to enable/disable DESFire® EV3 credential read and Proximity Check are only available for HID Signo readers with firmware version 10.0.2.4.
 - If EV1 SIO is disabled before 10.0.2.4 update, then EV3 should be disabled after update.
 - If EV1 SIO is enabled before 10.0.2.4 update, then EV3 should be enabled after update.
- For the iCLASS SE Express reader BLE, MIFARE® DESFire® UID, and MIFARE Classic® UID settings can only be changed if the reader was initially configured with these options when ordered.

4. Tap **ADD TO THE TEMPLATE** to save.



Key details

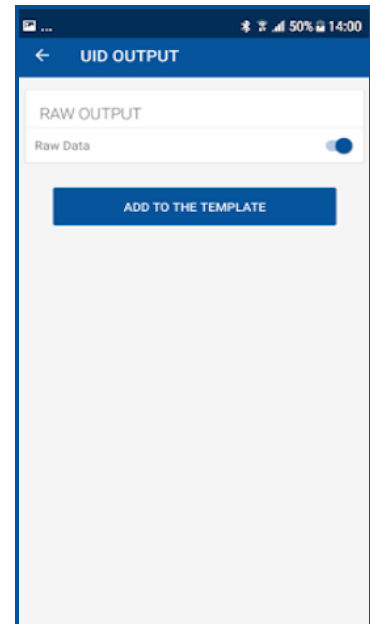
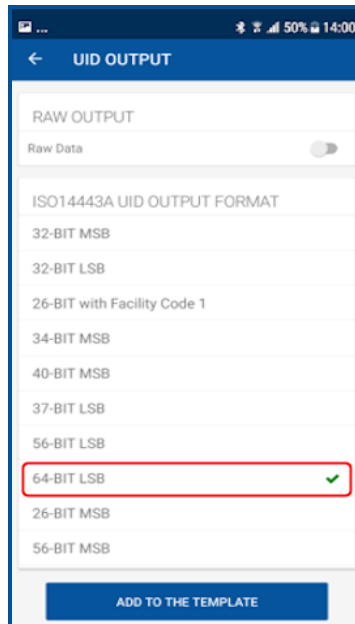
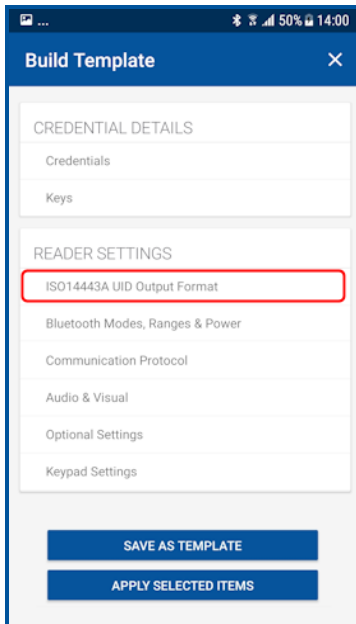
1. From the **CREDENTIAL DETAILS** section, tap **Keys**.
2. In the **Keys** section, tap **ADD KEYS**.
3. Select an authorization key to load onto the reader (only one key can be loaded). The selected authorization key will be displayed on the screen.
4. Tap **ADD TO THE TEMPLATE** to save.



ISO14443A UID Output Format settings

Note: For iCLASS and Signo readers, ISO14443A UID Output Format configuration settings are only valid for certain credential profiles.

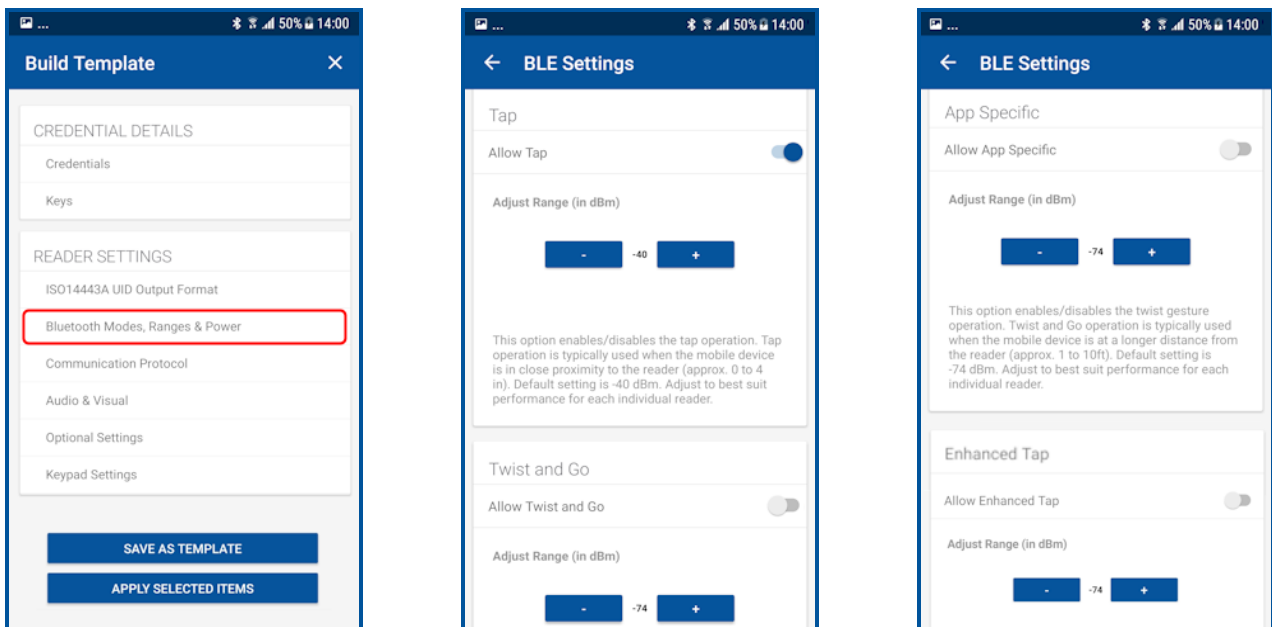
1. From the **READER SETTINGS** section, tap **ISO14443A UID Output Format**.
2. Select output format from the displayed list.
3. If RAW CSN cards are to be supported enable the **Raw Data** option.
4. Tap **ADD TO THE TEMPLATE** to save.



Bluetooth Modes, Ranges & Power settings

1. From the **READER SETTINGS** section, tap **Bluetooth Modes, Ranges & Power**.
2. On the **BLE Settings** screen, tap in the **APPLICATION BRAND** field and select a listed option, or alternatively, enter a **Custom Lock Service Code**.
3. Enable/disable the opening mode and, if necessary, adjust the range settings:
 - **Tap:** Default Tap range for HID Signo is **-45 dBm**. Default tap range for SE readers is **-40 dBm**.
 - **Twist and Go:** Default Twist and Go range is **-74 dBm**.
 - **App Specific:** Default App Specific range is **-74 dBm**.
 - **Enhanced Tap:** For HID Signo readers only, default ranges for iOS Background: **-30 dBm**, iOS Foreground: **-30dBm**, Android: **-45 dBm**.

Note: For each opening mode the default range value is provided on the **BLE Settings** screen.



4. The default Transmit Power setting (Default for HID Signo reader is **-0 dBm**. Default for a SE reader is **-4 dBm**) should not be changed unless absolutely necessary.

Note: For certain installations a higher or lower Transmit Power may be required, however this setting should only be adjusted if the default range settings do not result in the desired read range.
5. Tap **ADD TO THE TEMPLATE** to save.

Note: When connected to an iCLASS SE Express reader or HID Signo reader, the reader must be power cycled to activate updated BLE settings.

As opening ranges deviate between different mobile devices, you should always test and fine tune settings for a specific site. The read range settings listed below provide a starting point for common locations:

SE readers

| Location | Tap | Twist and Go |
|------------------------------|---------|--------------|
| Office environment | -48 dBm | -67 dBm |
| Elevators | -40 dBm | -57 dBm |
| Outdoor entrances | -48 dBm | -67 dBm |
| Garage (user inside vehicle) | -53 dBm | -74 dBm |

HID Signo readers

| Location | Tap | Twist and Go | Enhanced Tap (iOS) ¹ | Enhanced Tap (Android) |
|--------------------|---------|--------------|---------------------------------|------------------------|
| Office environment | -45 dBm | -74 dBm | -30 dBm | -45 dBm |

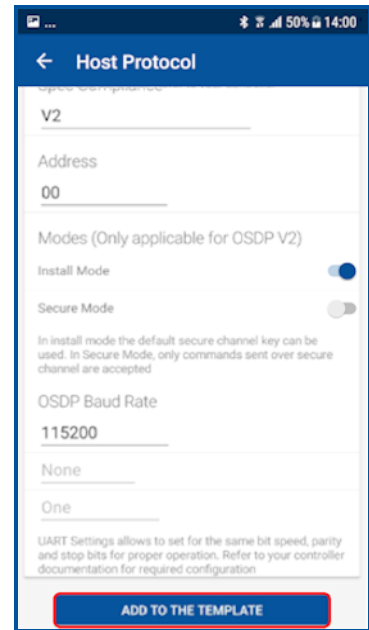
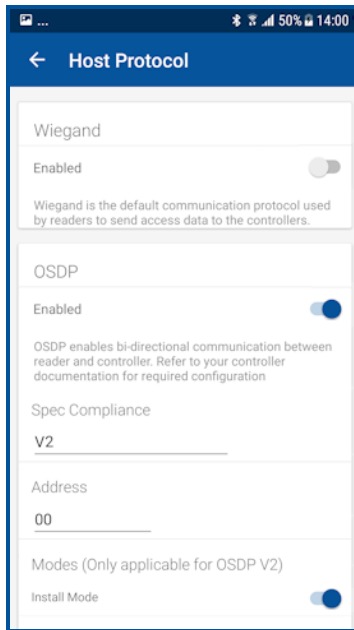
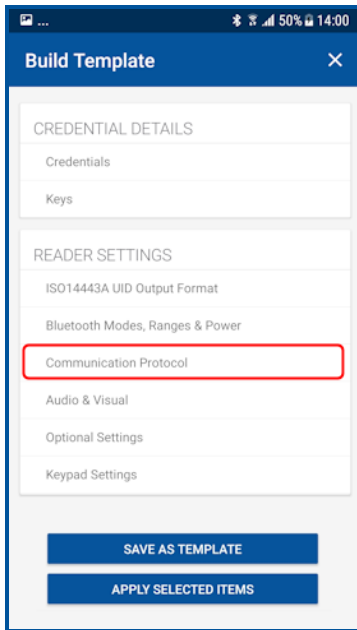
1. iOS Background and iOS Foreground.

Communication Protocol settings

1. From the **READER SETTINGS** section, tap **Communication Protocol**.
2. Enable the Reader to Controller communication protocol, either **Wiegand** or **OSDP** (not both).

Note: OSDP is not applicable to iCLASS SE Express R10 readers as these readers are Wiegand capable only.
3. If **OSDP** is enabled:
 - Select the spec compliance value, **V1** or **V2**.
 - Enable either **Install Mode** or **Secure Mode** (not both). These are only applicable if **V2** is selected as the spec compliance value.
 - Select the **OSDP Baud Rate**.

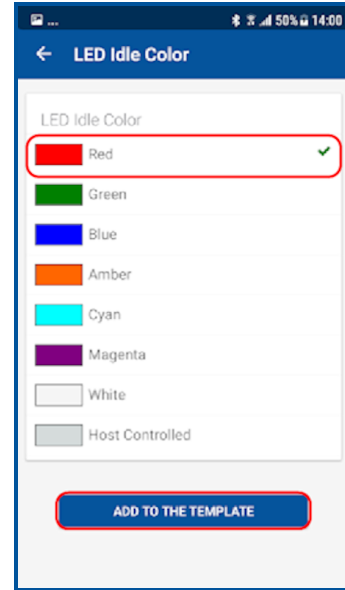
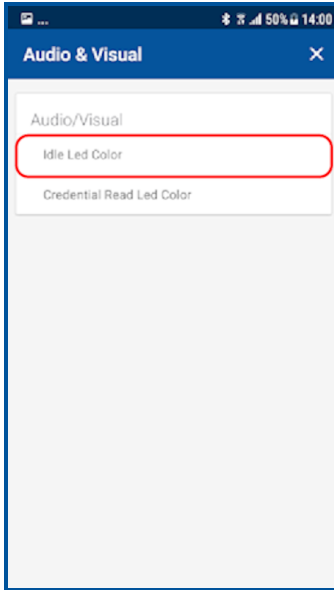
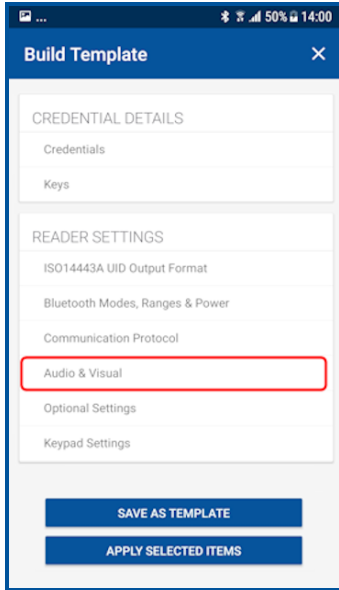
Note: In the **OSDP Baud Rate** section the Stop bit field and Parity field are read only.
4. Tap **ADD TO THE TEMPLATE** to save.



Audio & Visual settings

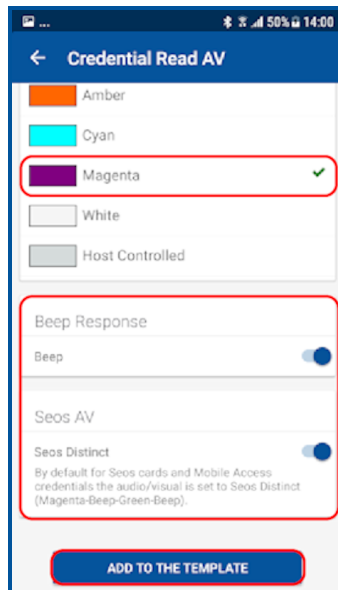
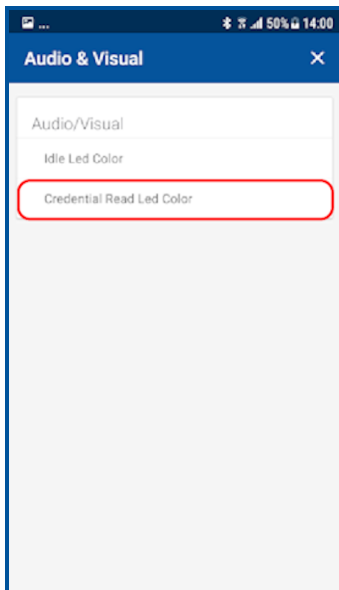
1. From the **READER SETTINGS** section, tap **Audio & Visual**.
2. From the **Audio/Visual** section, tap **LED Idle Color**.
3. Select a color and tap **ADD TO THE TEMPLATE**.

Note: **Idle LED Color** selections for HID Signo and iCLASS SE Express R10 readers are **Red** or **Blue**.



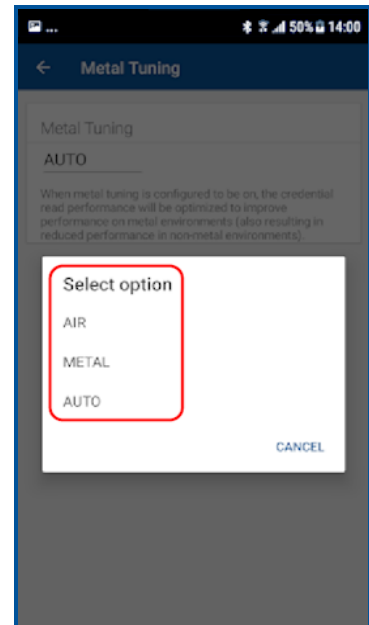
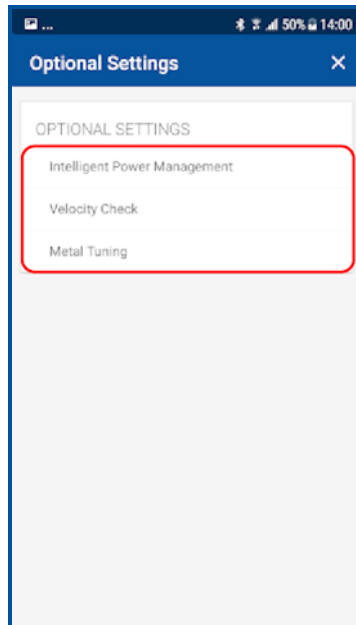
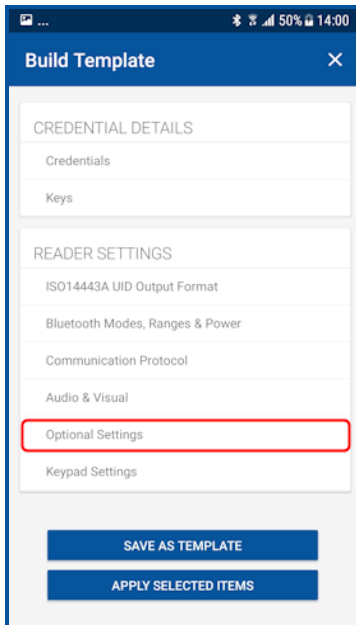
4. Tap **Credential Read Led Color**.
5. Select a color and enable/disable the **BEEP RESPONSE** and **SEOS AV** settings using the options. Tap **ADD TO THE TEMPLATE** to save.

Note: **Credential Read Led Color** selections for HID Signo and iCLASS SE Express R10 readers are **Green** or **No Response**.



Optional Settings

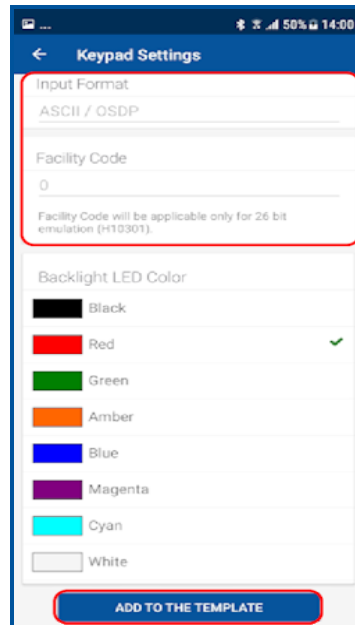
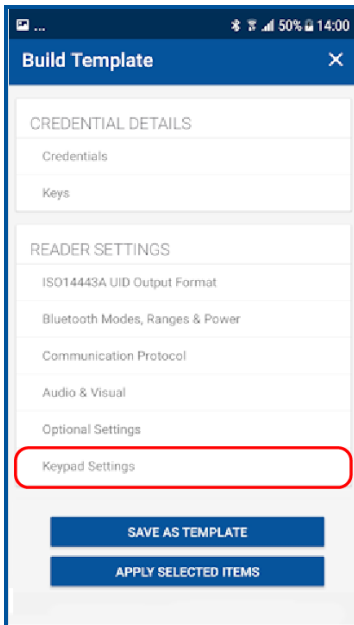
1. From the **READER SETTINGS** section, tap **Optional Settings**.
2. Enable/disable the following options as necessary:
 - **Intelligent Power Management**
 - **Velocity checking**
 - **Metal Tuning**. Select a listed setting (HID Signo readers and iCLASS SE Express R10 only).
 - Tap **ADD TO THE TEMPLATE** for any changed settings.



Keypad Settings

If the **KEYPAD** option is enabled (for HID Signo readers and iCLASS SE/multiCLASS SE only):

1. From the **READER SETTINGS** section, tap **Keypad Settings**.
2. Select an available **INPUT FORMAT** and, if applicable, enter a **FACILITY CODE**.
3. Select a keypad backlight color from the displayed list (HID Signo readers only).
4. Tap **ADD TO THE TEMPLATE** for any changed settings.



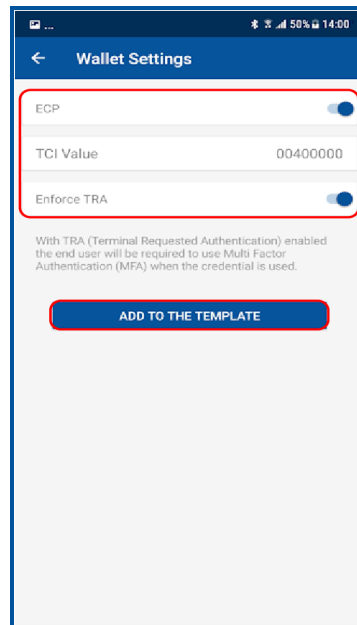
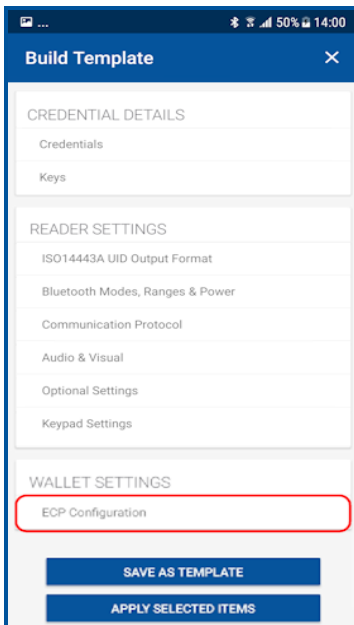
Wallet Settings

Enabling ECP (Enhanced Contactless Polling) will allow Wallet keys to be pushed along with Mobile Access keys. The following reader configuration specifications apply:

- Wallet settings are only applicable for HID Signo/iCLASS SE readers that are loaded with MOB or ICE keys.
- Wallet settings are only supported in HID iCLASS SE/multiCLASS SE Readers running firmware Version 8.9 and above. HID iCLASS/multiCLASS SE Readers running firmware Version 8.8 or below must be upgraded to firmware Version 8.9 for Wallet settings to be supported.
- Wallet settings are supported in HID Signo readers by default for all firmware versions.
- From Reader Manager 1.6.0 Wallet configuration has been optimized, reducing the number of steps needed to complete Wallet setting configuration:
 - For standard readers the user only needs to push MOB keys. The rest of the process is automated.
 - For readers shipped from HID with MOB or ICE Mobile Keysets, the user only needs to enable the TCI value in the reader configuration.

If the reader configuration supports Wallet settings:

1. From the **WALLET SETTINGS** section, tap **ECP Configuration**.
2. Enable the **ECP** option. A **TCI Value** is automatically assigned.
3. To force mobile access users to use MFA (Multi Factor Authentication) when a mobile device is presented to the reader, enable the **Enforce TRA** option.
4. Tap **ADD TO THE TEMPLATE** for any changed settings.



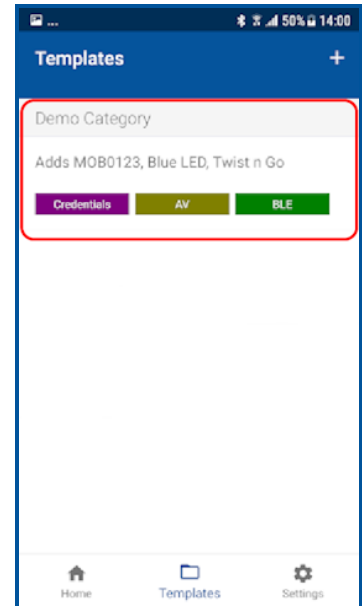
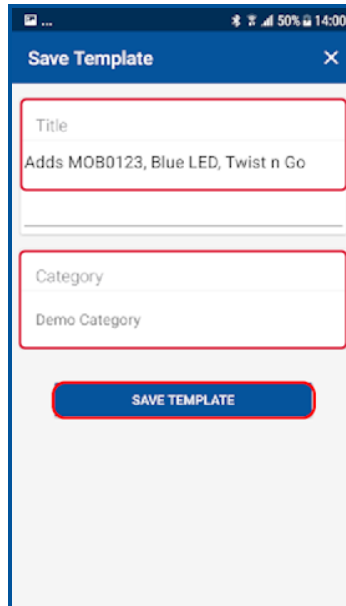
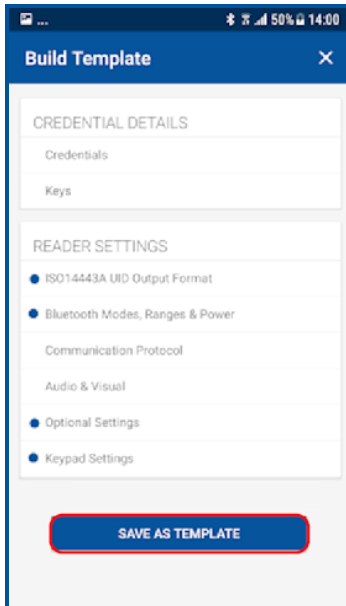
2.4.2 Manage templates

Save a new template

1. When configuration settings are selected and added to the template, tap **SAVE AS TEMPLATE**.
2. Tap in the **TITLE** area and enter a title for the template.
3. Tap in the **CATEGORY** area and tap **Select Category**. Select an existing category from the displayed list or add a new category and select this newly created category. Tap **SAVE TEMPLATE**.

Note: A category must be selected before the template can be saved.

The new template is displayed on the **Templates** screen with indicators for the configuration types within the template.

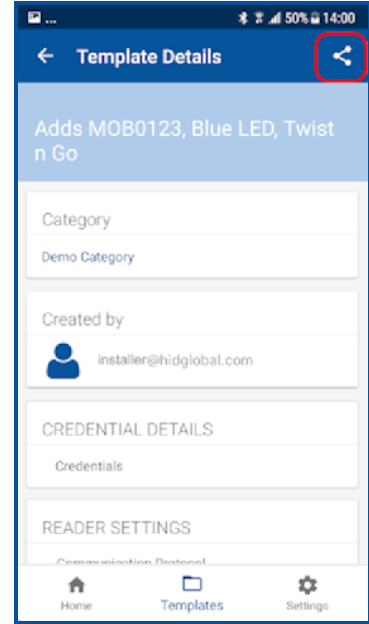
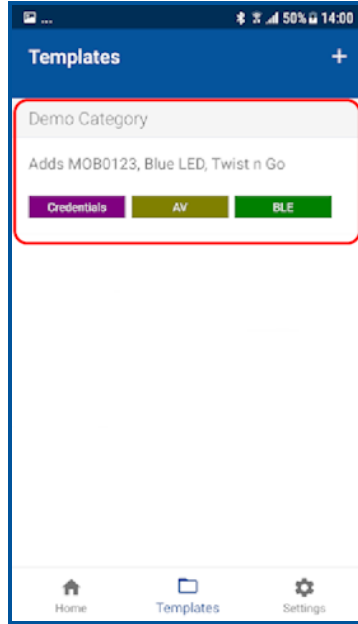
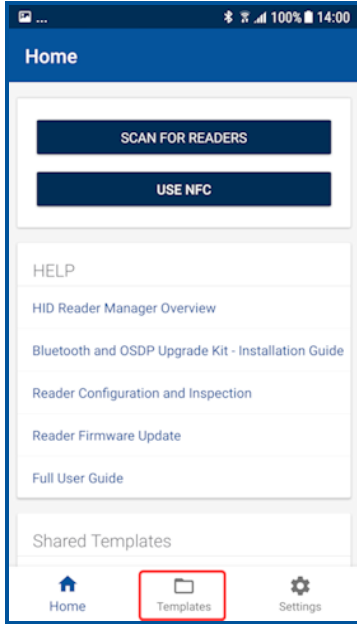


Share a template

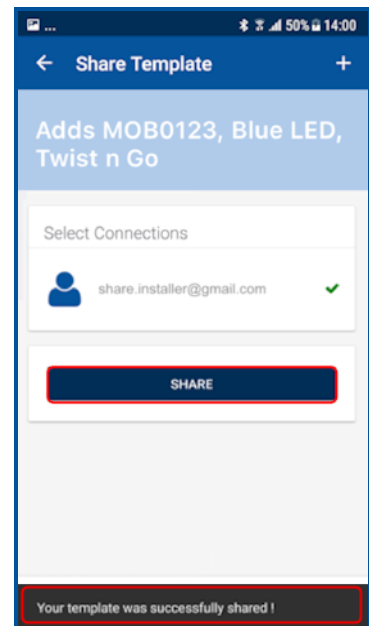
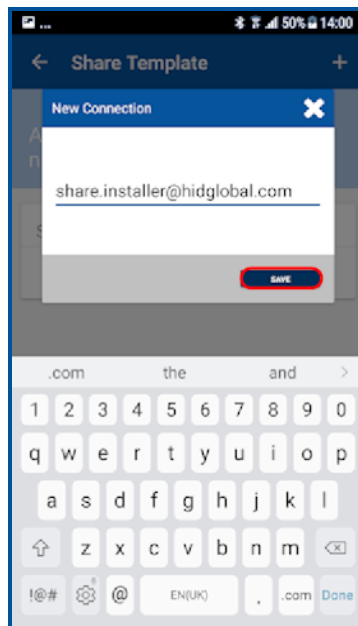
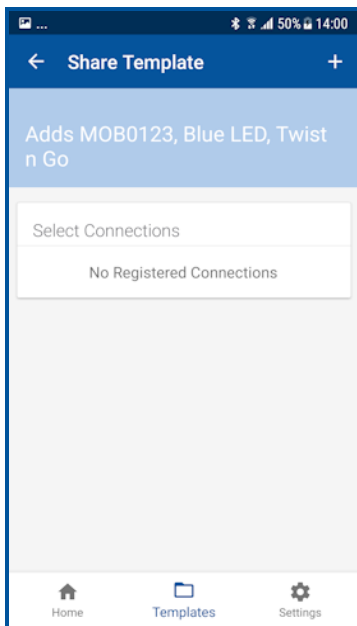
Templates can be shared with other Reader Technicians to speed up the configuration of multiple readers.

Note: Templates that contain a MOB/ICE key can only be shared with reader technicians that are authorized for that specific key.

1. On the **Home** screen, tap the **Templates** icon and select a displayed template to be shared. On the **Template Details** screen tap the share icon [🔗].

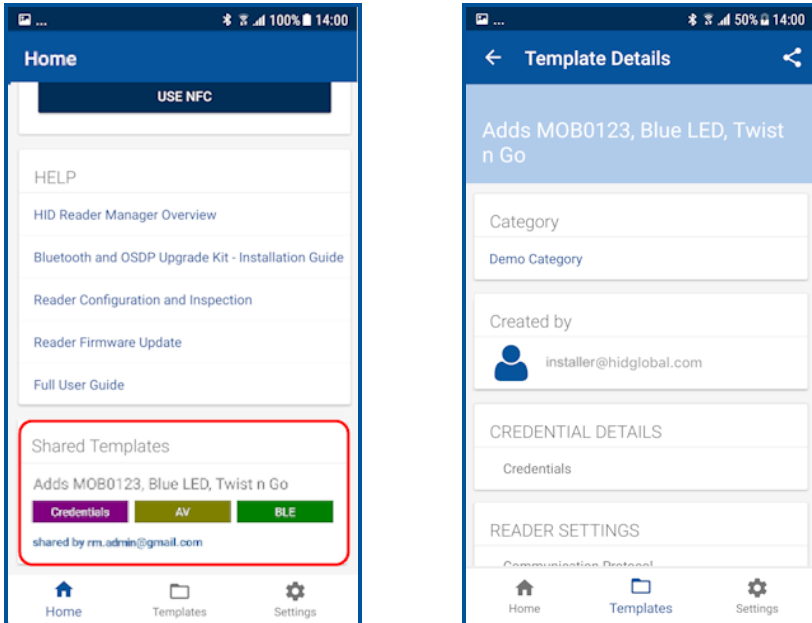


2. Tap the plus icon [⊕] and, in the **New Connection** box, enter the email address of another Technician (this can be any Technician that is already registered). Tap **SAVE**.
3. When the connection has been made, tap **SHARE**. A message will appear at the bottom of the screen to indicate success.

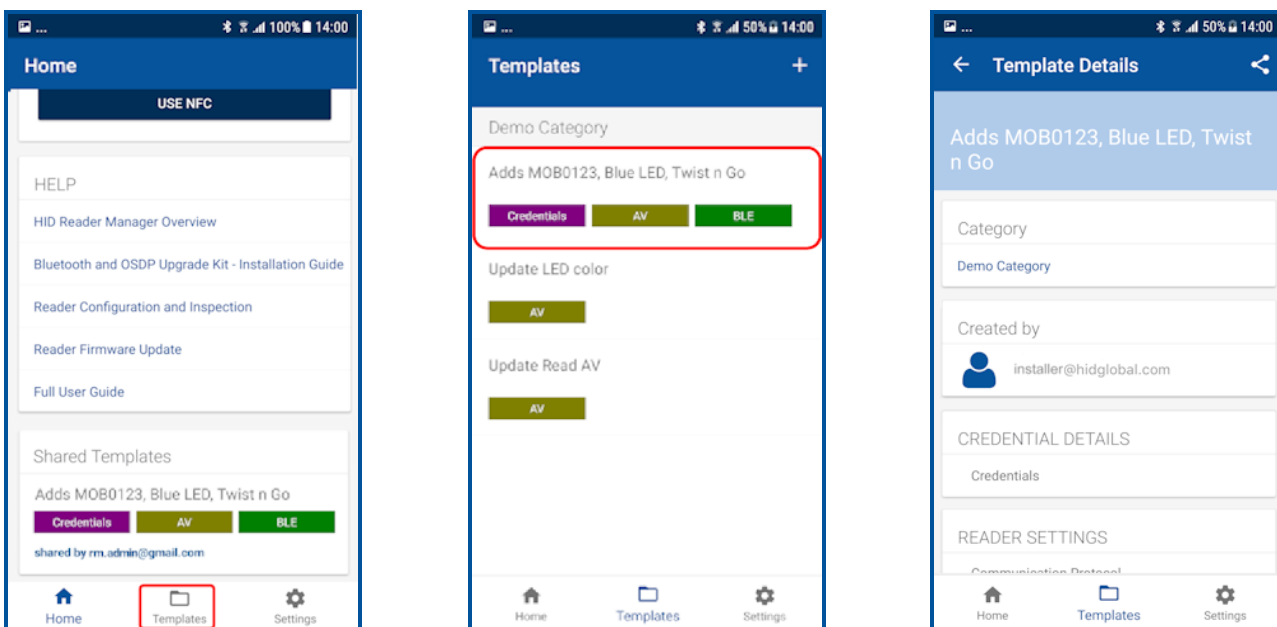


Display template details

Configuration templates shared with a Reader Technician that is logged into HID Reader Manager app are displayed in the **SHARED TEMPLATES** area on the **Home** screen. Tap on a displayed shared template to view the template details.



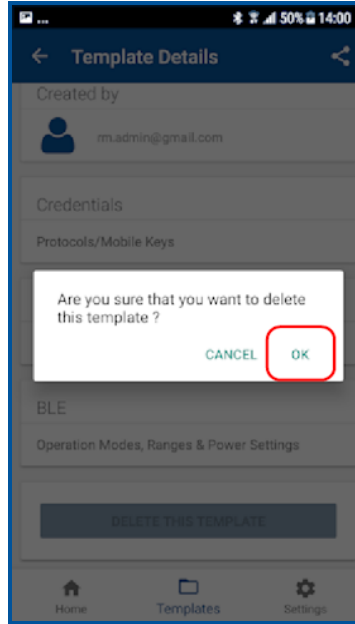
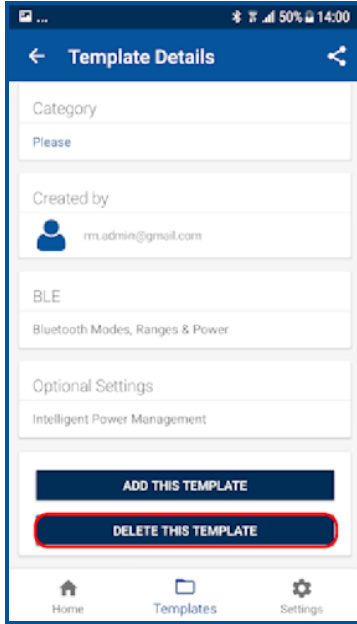
To view the list of created templates tap the **Templates** icon on the HID Reader Manager Home screen. Existing templates are listed on the **Templates** screen. Tap on a displayed template to view the template details.



Delete a template

When template details are displayed, the template can be deleted:

1. Swipe down to the bottom of the **Template Details** screen and tap **DELETE THIS TEMPLATE**.
2. Tap **OK** to delete the template.



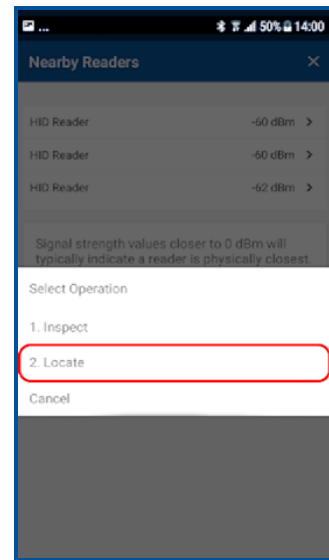
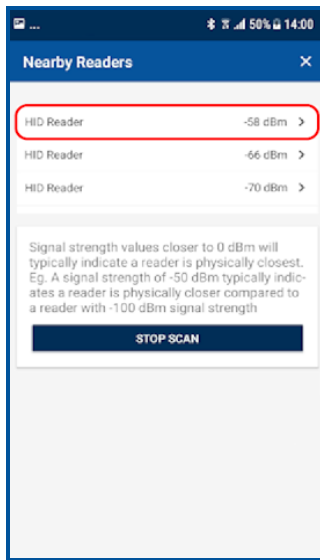
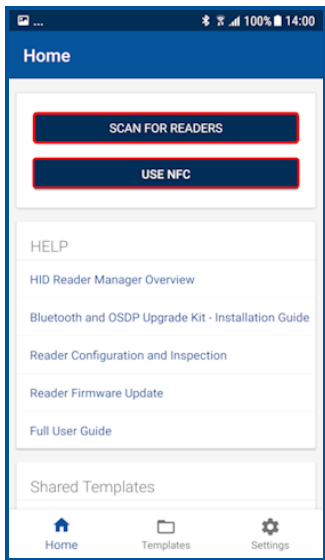
2.4.3 Connect to a reader

1. On the HID Reader Manager **Home** screen, tap **SCAN FOR READERS** or **USE NFC**. This will scan for nearby Mobile-enabled readers.

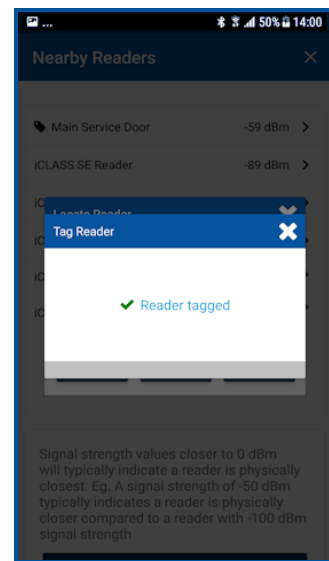
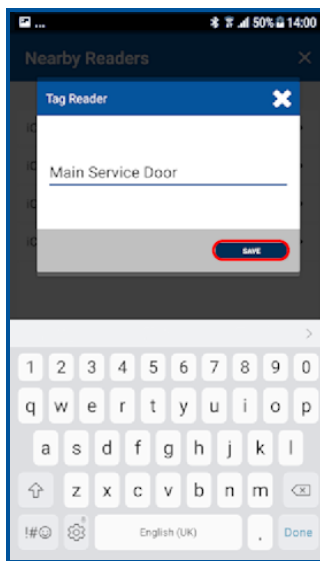
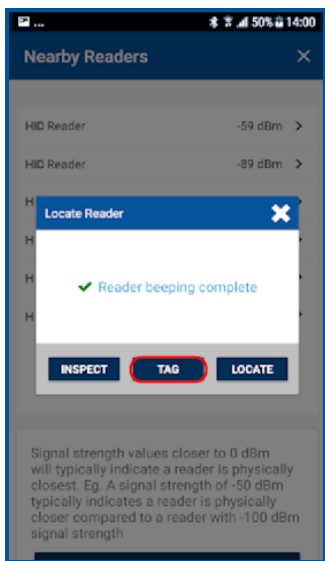
Note: When NFC is used for the reader scan:

- The HID Mobile Access App and any NFC Payment Apps must be stopped and should not be running in the background.
- The mobile device must be placed directly on the reader and should not be moved until the scan operation has finished. If the link is lost the mobile device must be removed from the reader and presented again.

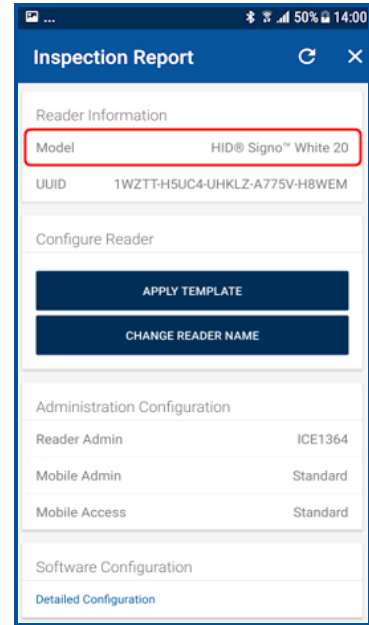
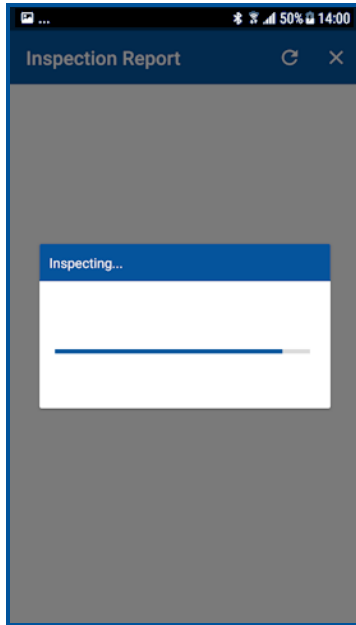
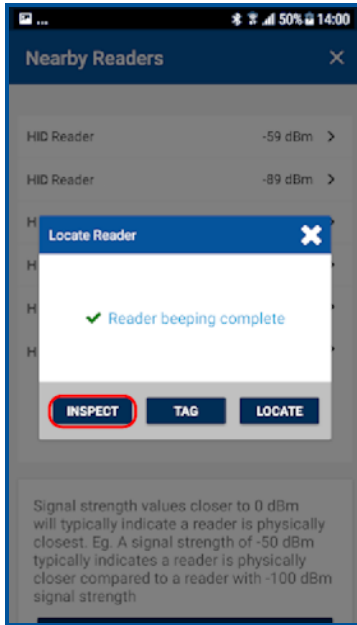
2. Select a displayed reader from the **Nearby Readers** screen and, from the **Select Operation** menu, tap **Locate** to ensure the correct reader is selected. The reader will beep for about eight seconds.



3. If you wish to name the reader for easier identification, tap **TAG**, enter a name (the tagged reader name is only visible on your mobile device), and tap **SAVE**.



4. Tap **INSPECT**. The reader is now connected and reader information is displayed on the **Inspection Report** screen, see **2.4.4 Reader inspection report**.



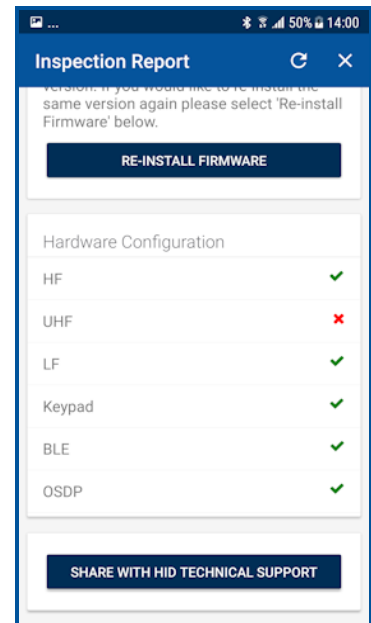
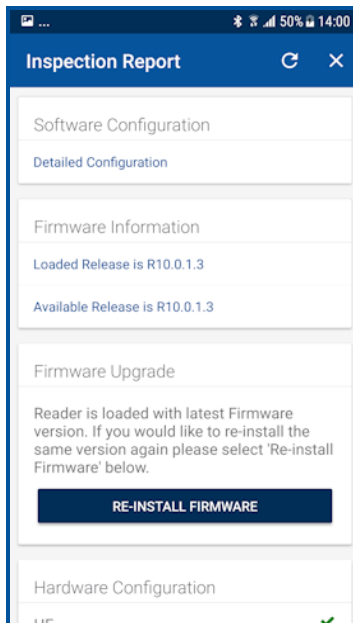
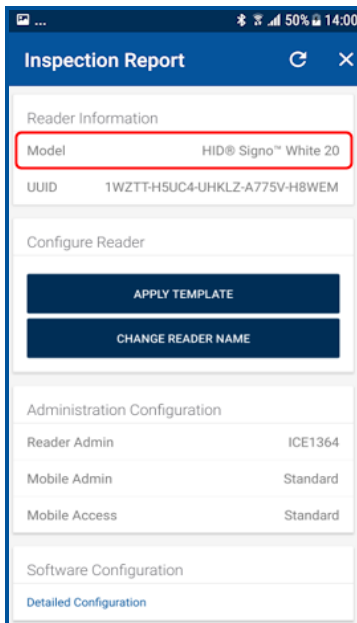
2.4.4 Reader inspection report

The **Inspection Report** screen displays the following configuration details for a connected reader:

- Reader information relating to the Reader Model and UUID (HID Sigo readers only)
- Administration configuration information
- Firmware information
- Hardware configuration information

From the **Inspection Report** screen the following can be carried out:

- **Firmware Upgrade:** If prompted perform a reader firmware upgrade or re-install the same version. See [2.4.5 Firmware upgrade](#).
- **Detailed Configuration:** Select to access detailed reader settings, modify settings and directly apply them to the reader. See [2.4.6 View detailed reader configuration](#).
- **Configure Reader:**
 - Tap **APPLY TEMPLATE** to select and apply template configuration settings to the reader. See [2.4.7 Apply configuration changes](#).
Note: Before applying a template, inspect the reader with the Reader Manager app to determine available configuration settings. Only include valid configurations in the template definition.
 - Tap **CHANGE READER NAME** to assign a name to the reader (iCLASS SE/multiCLASS SE readers only). See [2.4.8 Change reader name](#).
- **SHARE WITH HID TECHNICAL SUPPORT:** Select if you experience an issue while using the application. The issue will be logged in the Incident Reporting System and you will be provided with Incident Id for reference. The Incident Id should be quoted when contacting HID Support. For additional information, see [4.2 Contact HID Technical Support](#).

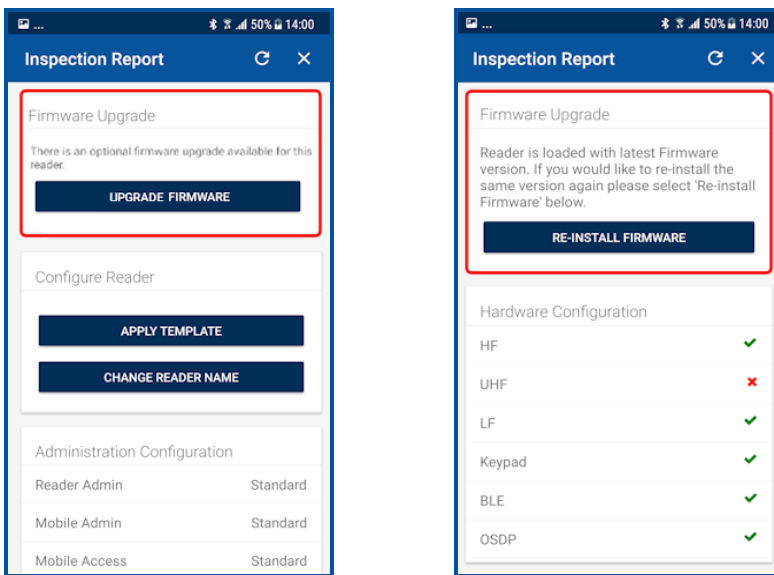


2.4.5 Firmware upgrade

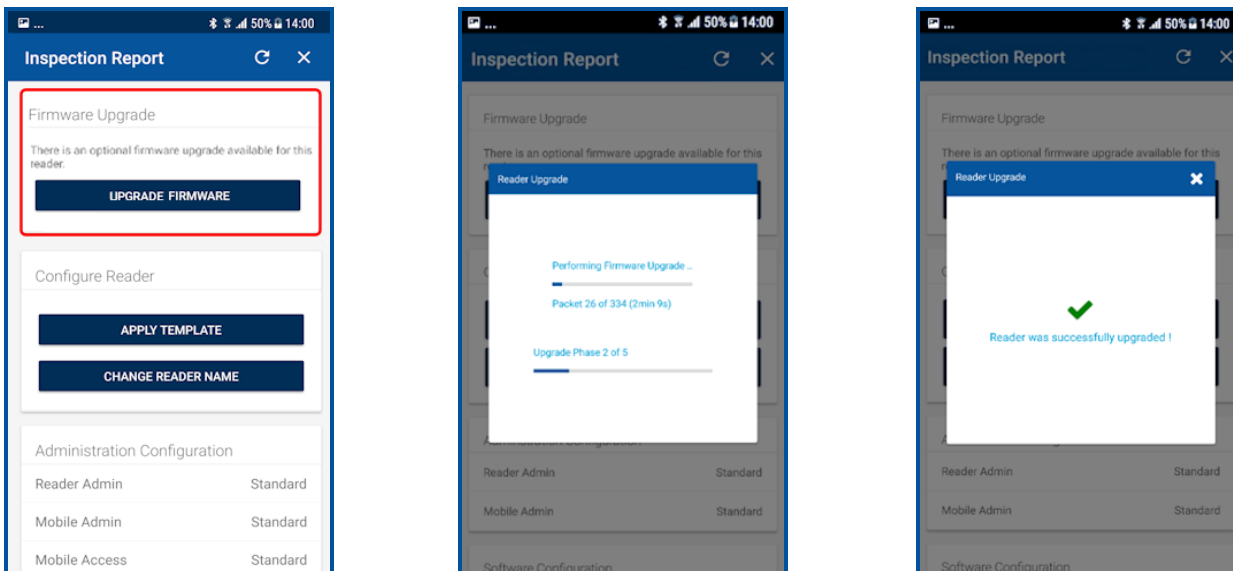
On the **Inspection Report** screen you will be notified about any possible firmware upgrade option in the **FIRMWARE UPGRADE** section of the screen. If the firmware is already at the latest release then an option to re-install the same firmware version is available. It is recommended that optional firmware upgrades are not implemented, other than to resolve a specific issue.

Note:

- A re-install of R8.9.1.4 firmware may fail in phase four of the re-install process. If this occurs reader functionality is not affected as the reader is already running R8.9.1.4 firmware.
- iCLASS SE reader firmware upgrade may require a two step upgrade process which will take longer than a standard upgrade. See [A.1 Supported firmware versions for upgrade](#).



If a firmware upgrade is necessary, tap **UPGRADE FIRMWARE** to begin the firmware update process.



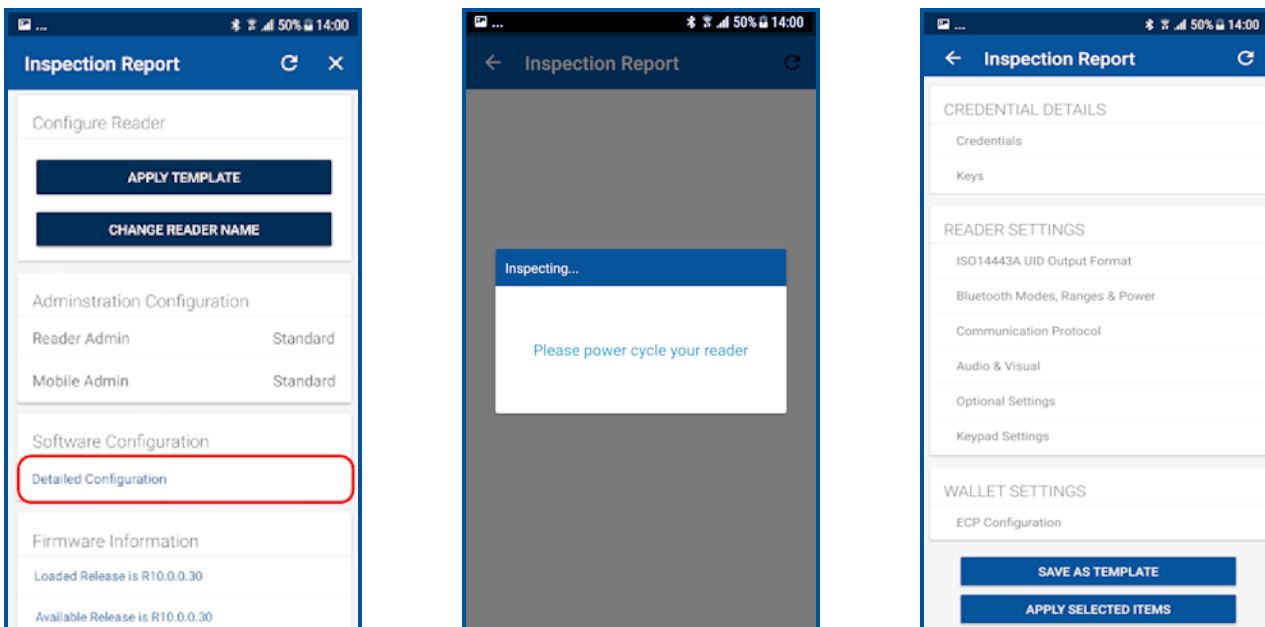
Do not change devices once the firmware upgrade process has started. If a phase of the process is interrupted, restart the process and the upgrade will automatically resume when connection to the device is restored. If the upgrade operation fails, refer to the **Troubleshooting** section for a possible description.

2.4.6 View detailed reader configuration

When connected to a reader, on the **Inspection Report** screen, tap **Detailed Configuration** to view and access detailed reader configuration settings.

Note: If the reader is a Standard enabled reader or an iCLASS SE Express R10 reader you will be prompted to power cycle the reader. For ICE/MOB enabled readers no reader power cycle is required.

From the **Inspection Report** screen you can make configuration changes and either save the changes to a template or apply them directly to the reader.



Credential details

The **CREDENTIAL DETAILS** section provides options to view the reader profile (for HID Signo reader only), enable/disable credential settings and view/add authorization keys:

- **Credentials:** see the [Credential details](#) section.
- **Keys:** see the [Key details](#) section.

Reader Settings

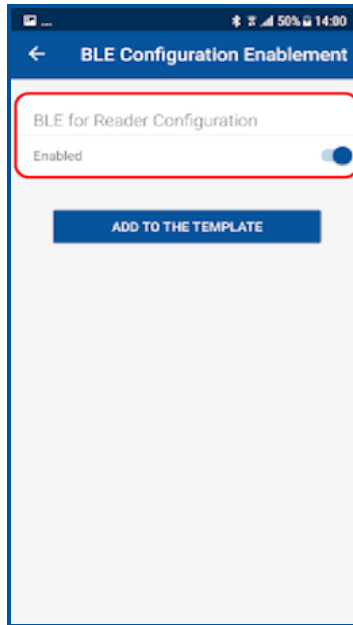
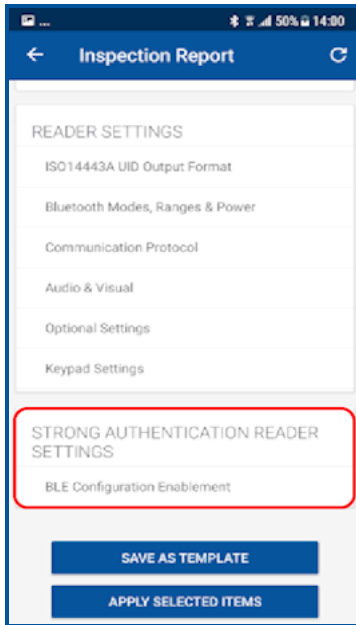
In the **READER SETTINGS** section the following can be configured:

- **ISO14443A UID Output Format:** see the [ISO14443A UID Output Format settings](#) section.
- **Bluetooth Modes, Ranges & Power:** see the [Bluetooth Modes, Ranges & Power settings](#) section.
- **Communication Protocol:** see the [Communication Protocol settings](#) section.
- **Audio & Visual:** see the [Audio & Visual settings](#) section.
- **Optional Settings:** see the [Optional Settings](#) section.
- **Keypad Settings:** see the [Keypad Settings](#) section.
- **Wallet Settings:** see the [Wallet Settings](#) section.

Strong Authentication Reader Settings

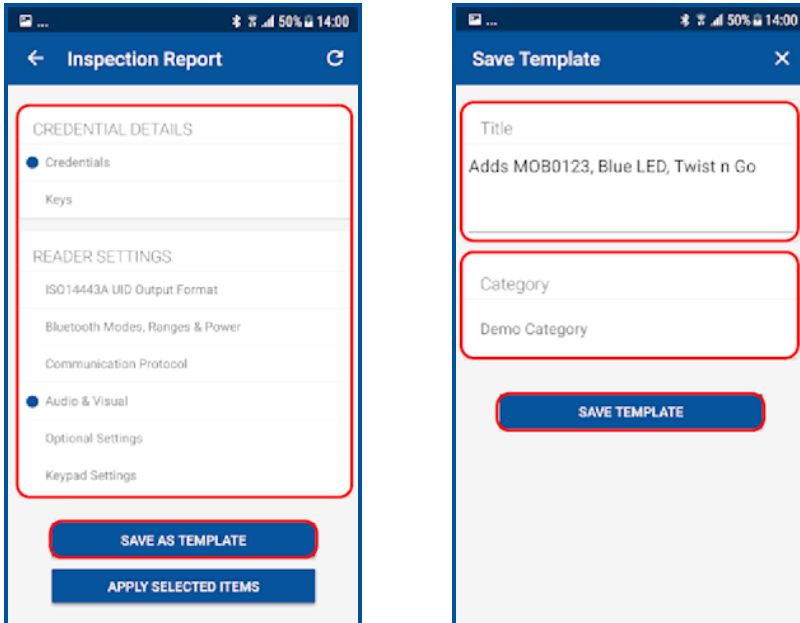
If your Android mobile device supports NFC you can enable/disable the BLE capability of the reader using NFC.

1. On the **Inspection Report** screen, under **STRONG AUTHENTICATION READER SETTINGS**, select the **BLE Configuration Enablement** option.
2. On the **BLE Configuration Enablement** screen, enable or disable the **BLE for Reader Configuration** option, as required.



Save as template

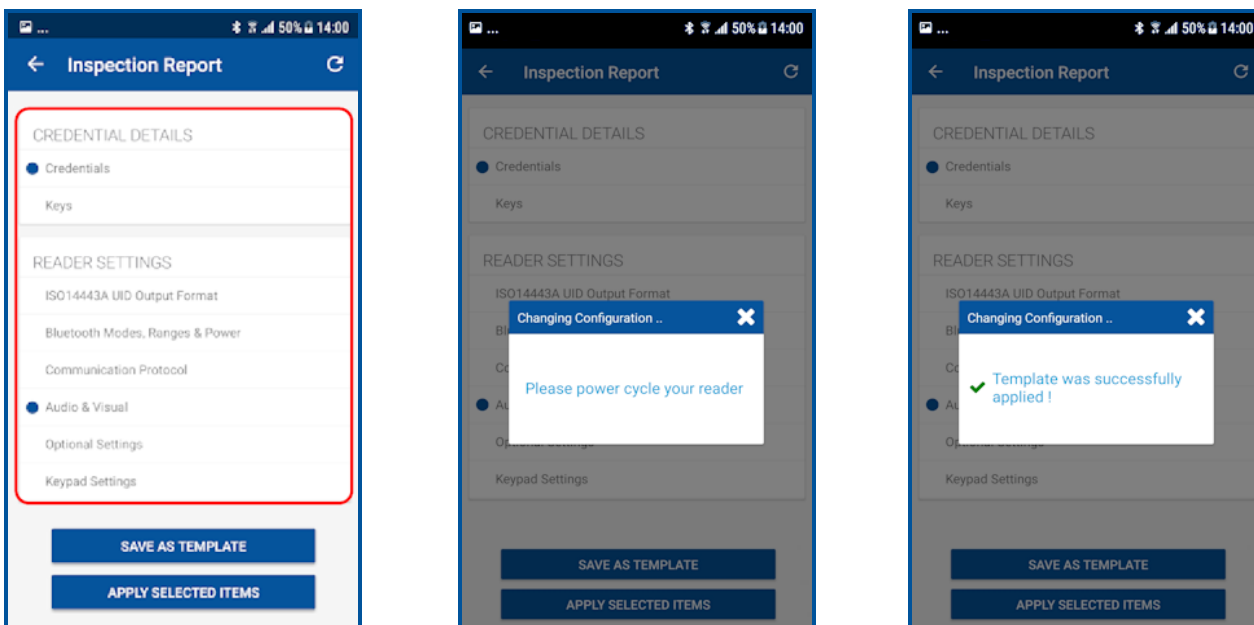
Any changed configuration settings are indicated with a blue circle. To save changed configuration settings to a template, tap **SAVE AS TEMPLATE**, enter a template **Title** and **Category** and tap **SAVE TEMPLATE**. To apply template settings, see [2.4.7 Apply configuration changes](#).



Apply selected items

Any changed configuration settings are indicated with a blue circle. To apply changed configuration changes directly to the connected reader, tap **APPLY SELECTED ITEMS**.

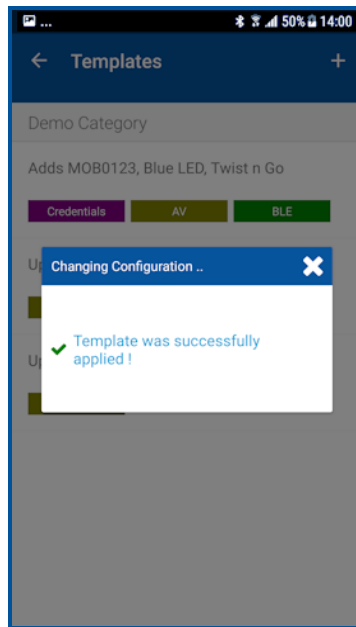
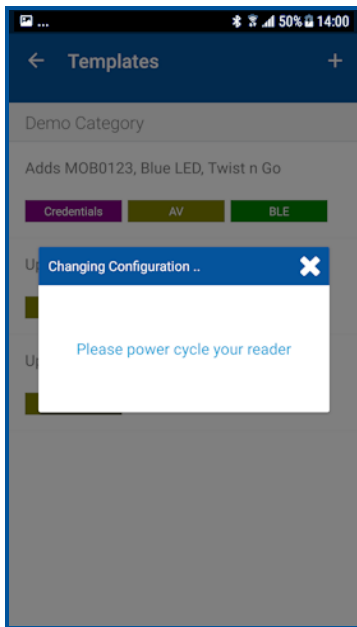
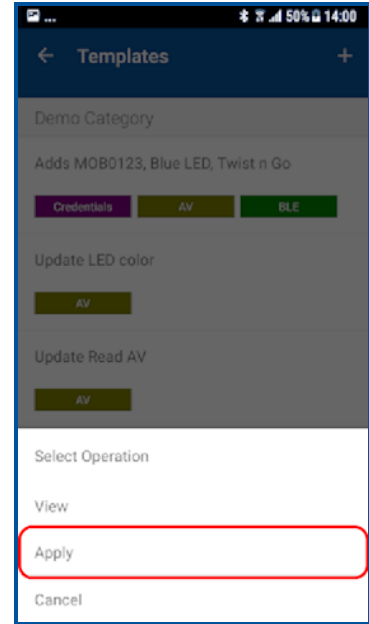
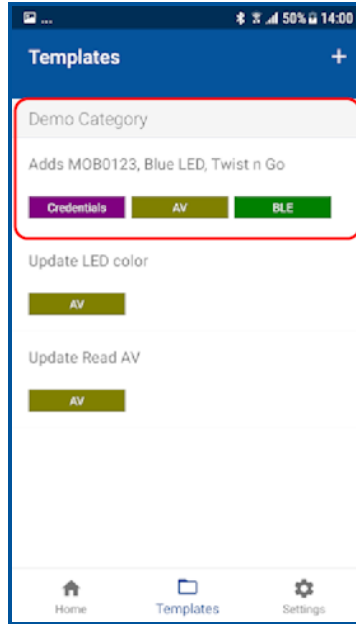
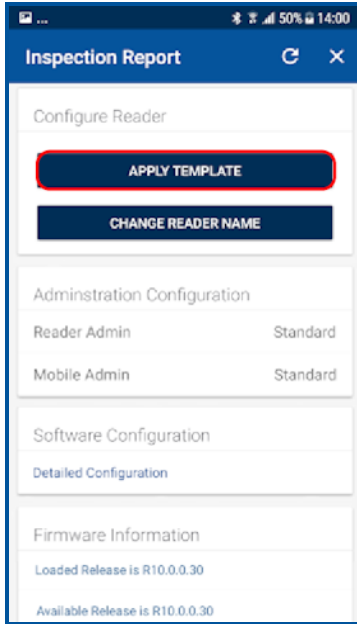
Note: If the reader is a Standard enabled reader you will be prompted to power cycle the reader. For ICE/MOB enabled readers no reader power cycle is required.



2.4.7 Apply configuration changes

When viewing a reader **Inspection Report**:

1. Tap **APPLY TEMPLATE**.
2. Select a listed template from the **Templates** screen. From the **Select Operation** menu, tap **Apply**.
Note: If the reader is a Standard enabled reader or an iCLASS SE Express R10 reader you will be prompted to power cycle the reader. For ICE/MOB enabled readers no reader power cycle is required.



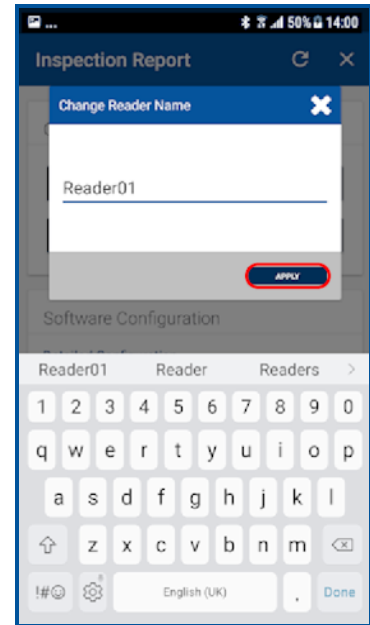
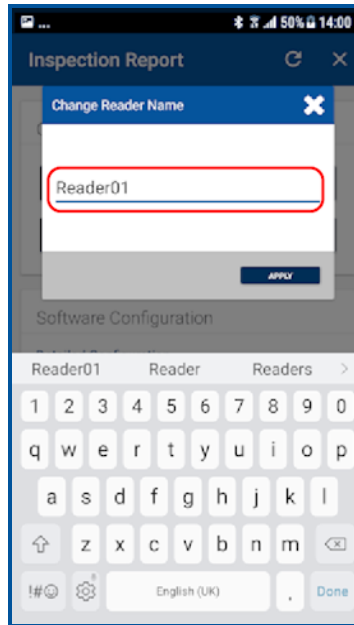
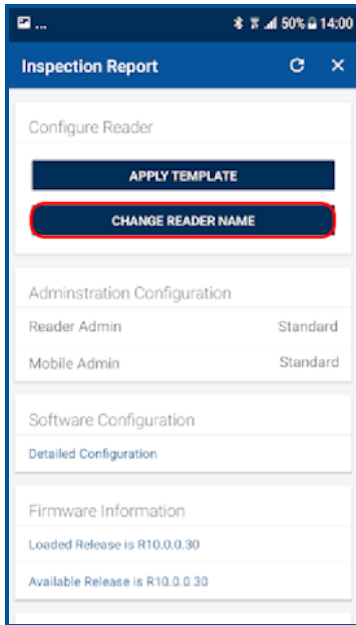
Note: If the operation to apply configuration changes fails, for example “SNMP Authentication Failed”, refer to [Troubleshooting](#) for a possible description of the cause for the failure.

2.4.8 Change reader name

On the **Inspection Report** screen the reader name can be changed. When changing a reader name with **Change Reader Name**, the reader's name, for example, "iCLASS SE Reader", is changed to a custom name. This custom reader name is visible from within any other Technician's Reader Manager app.

Note: Only iCLASS SE/multiCLASS SE readers support the assignment of a reader name.

1. Tap **CHANGE READER NAME**.
2. Enter a new reader name.
3. Tap **APPLY**.



Section **03**

HID Reader Manager Service

3.1 Overview

This section provides the required steps and procedures to be performed by the HID® Reader Manager™ Administrator in order to enroll a Reader Technician in the Reader Manager solution and perform authorization key management.

3.2 Mobile Access setup

A Mobile Access account is established for an organization through a HID Global onboarding process. Once an account is created the Organization can order and purchase subscription user licenses or Mobile IDs through your Access Control Provider. During this process, HID Global will set up an instance of the HID® Origo™ Management Portal for the Organization and create the personalization specification for Mobile IDs and Mobile-Enabled readers.

Automated onboarding is an online self-registration process where an Organization can setup up an account for the HID Origo Management Portal. Automated onboarding provides instant onboarding for new customers and it simplifies the ordering process. To setup a HID Origo Management Portal account via the automated onboarding process go to the following site and follow the online registration steps:

<https://portal.origo.hidglobal.com/selfonboarding/>

Once a new account has been created and the organization has been setup in the system, organization administrators have access to the Mobile Identities service and the Reader Manager service.

3.2.1 Reader Manager service

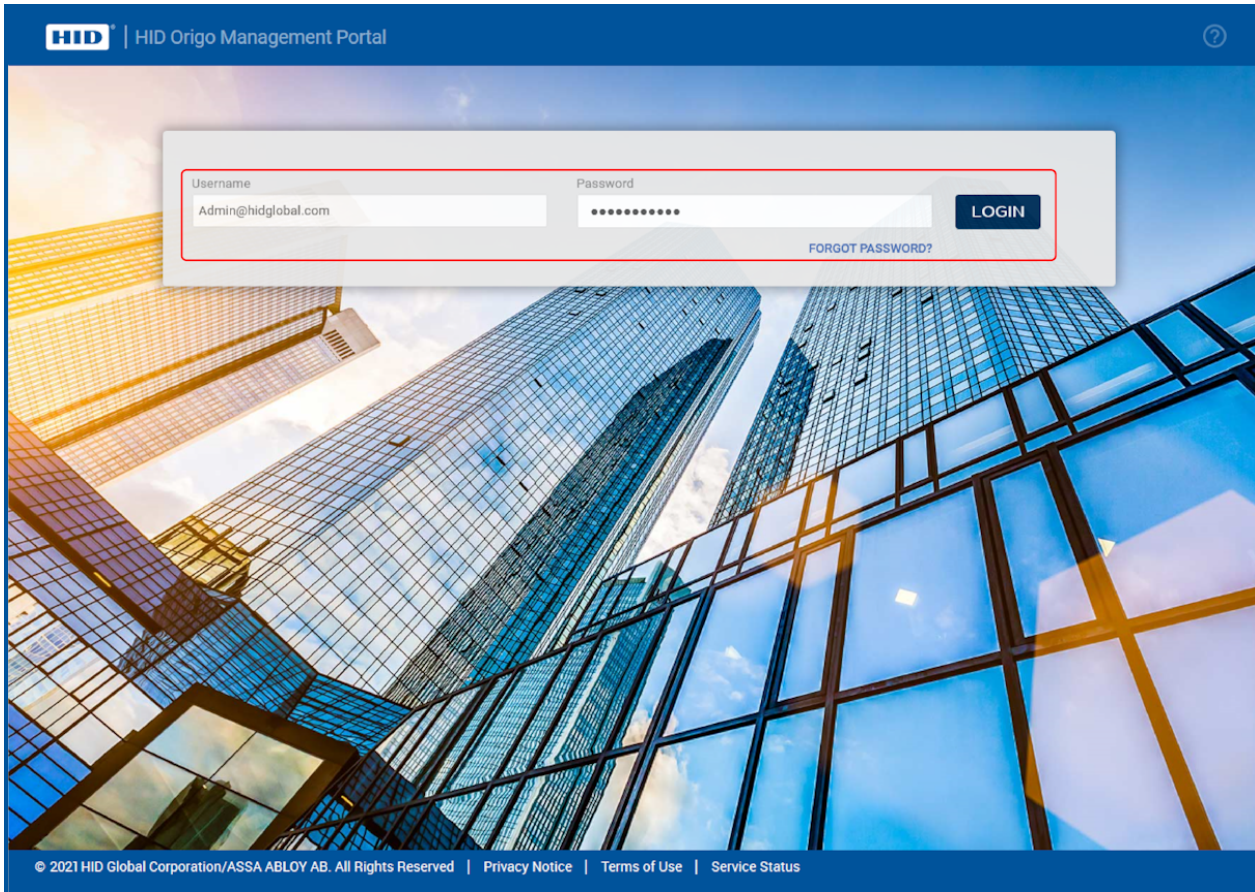
The Reader Manager service allows administrators to enroll and manage Reader Technicians, issue/revoke authorization keys, and carry out Reader Manager service administration.

All organizational accounts setup up on the HID® Origo™ Management Portal have access to the Reader Manager service enabled by default.

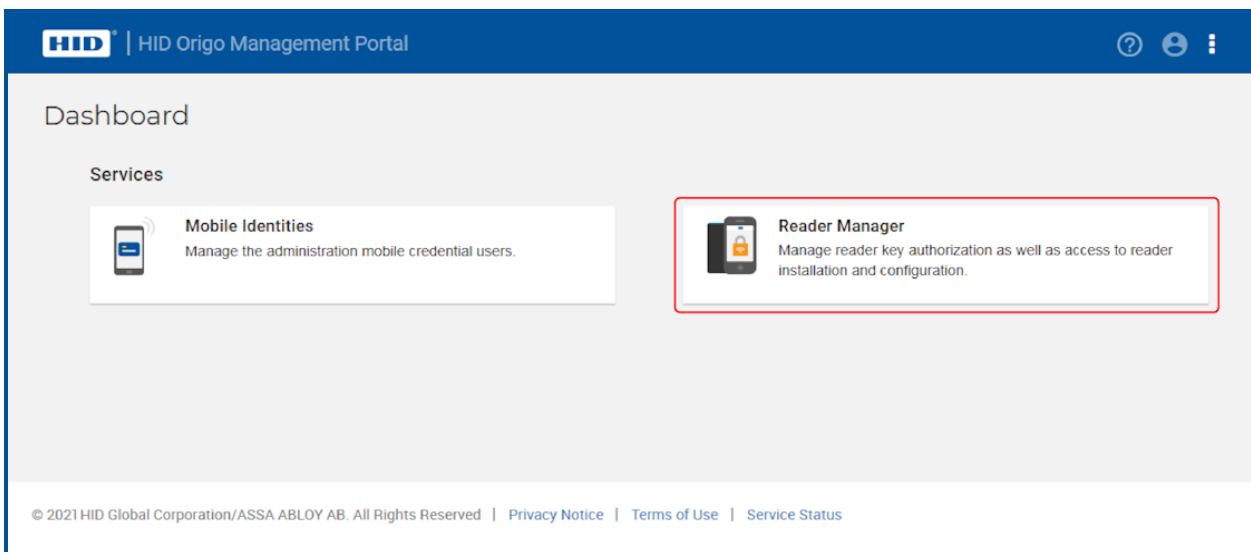
3.3 Access the Reader Manager service

To access the Reader Manager service:

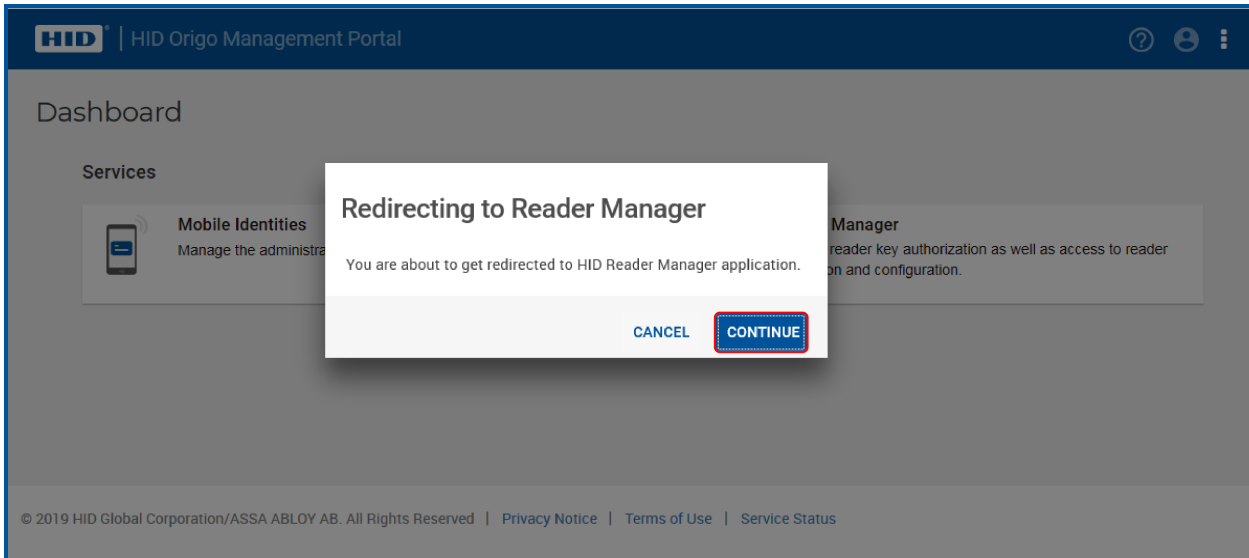
1. Log into the HID Origo Management Portal as Organization Admin.



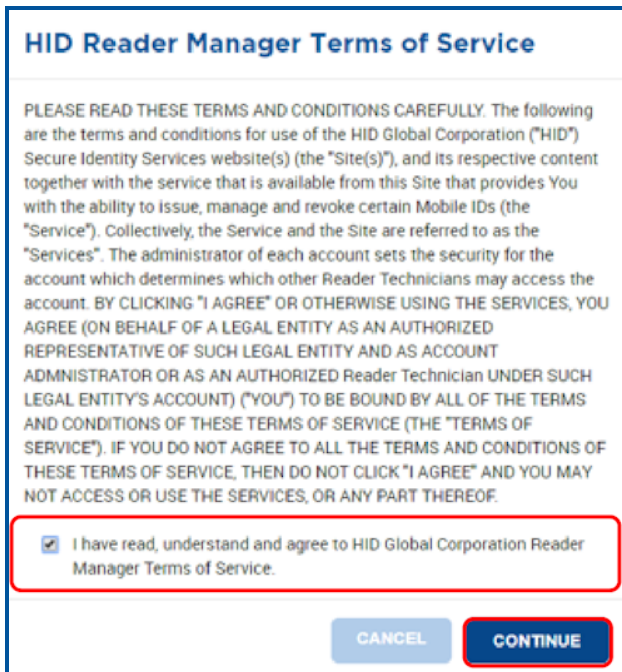
2. Select **Reader Manager** on the **Dashboard** page.



3. Click **CONTINUE** to be redirected to your organizations instance of the Reader Manager service.



4. On the Reader Manager screen login as Reader Manager Administrator using the User name and Password setup in the HID Origo Management Portal.
Note: If this is the initial login as Reader Manager Administrator you will be asked to read and accept the **HID Reader Manager Terms of Service**. Click **Continue**.




The Reader Manager Administrator can now perform Reader Technician enrollment and authorization key issuance tasks in the Reader Manager service.

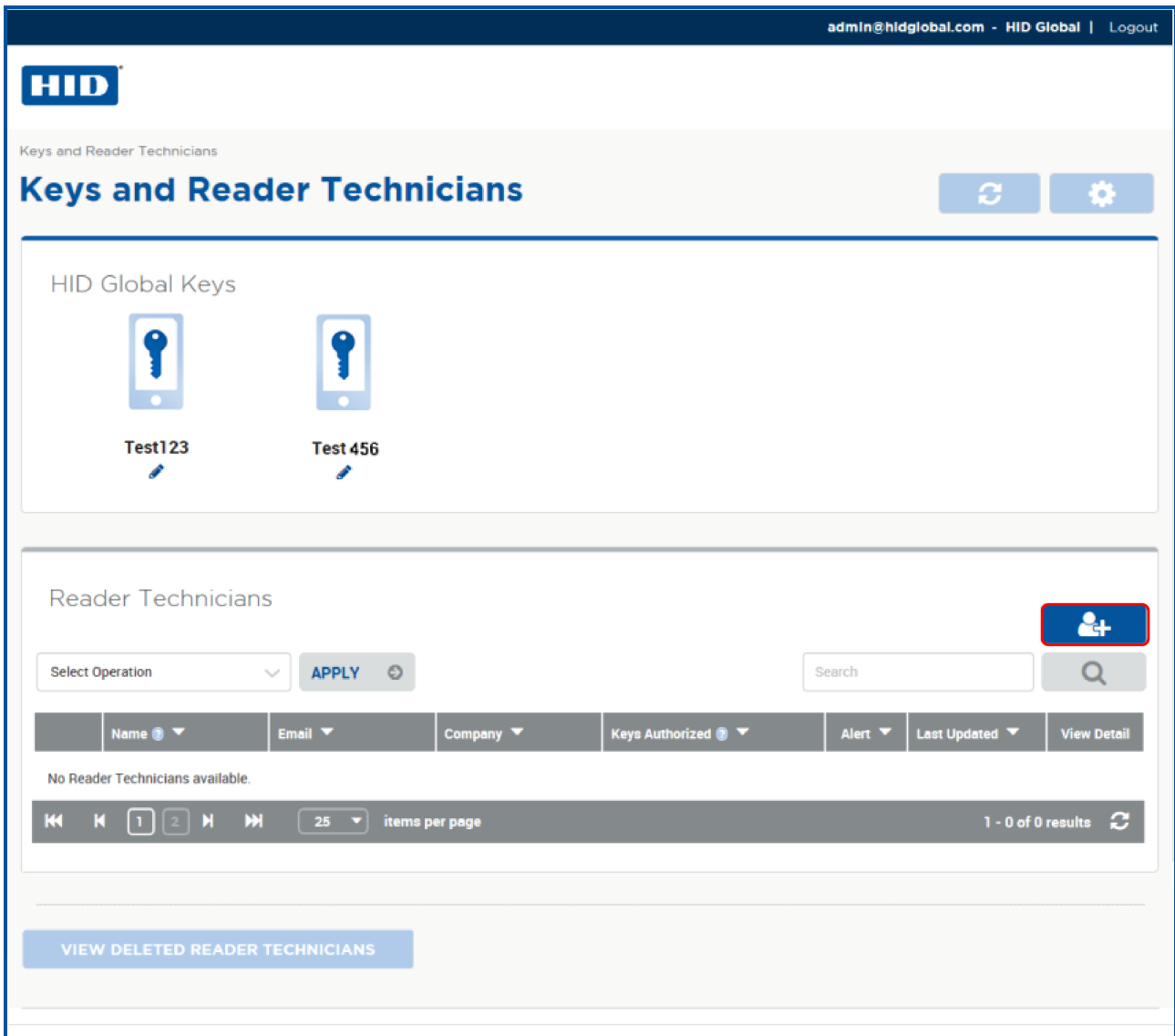
3.4 Enroll a Reader Technician

As a prerequisite to enrolling a Reader Technician, the Reader Technician must have installed and registered the HID® Reader Manager™ App on their mobile device, see [2.2.3 Download and install the Reader Manager app](#) and [2.2.4 Register a new account within the app](#).

Note: If the Reader Technician is an Organization/Reader Manager Admin, they can log into the HID Reader Manager App using their existing portal login credentials.

To enroll a Reader Technician:

1. Scroll to the **Reader Technicians** section on the **Keys and Reader Technicians** page.
2. Select the enroll technician icon [].



3. Enter the **Name**, **Email address**, and **Company** of the new Reader Technician on the **Enroll Reader Technician** page.

The screenshot shows the 'Enroll Reader Technician' page in the HID Administration interface. The page title is 'Enroll Reader Technician' and the breadcrumb is 'Keys and Reader Technicians > Enroll Reader Technician'. The form is titled 'Reader Technician Information' and contains the following fields:

| | | |
|---------------|------------------------------|-----------|
| Name | Demo | Installer |
| Email address | demo.installer@hidglobal.com | |
| Company | HID Global | |

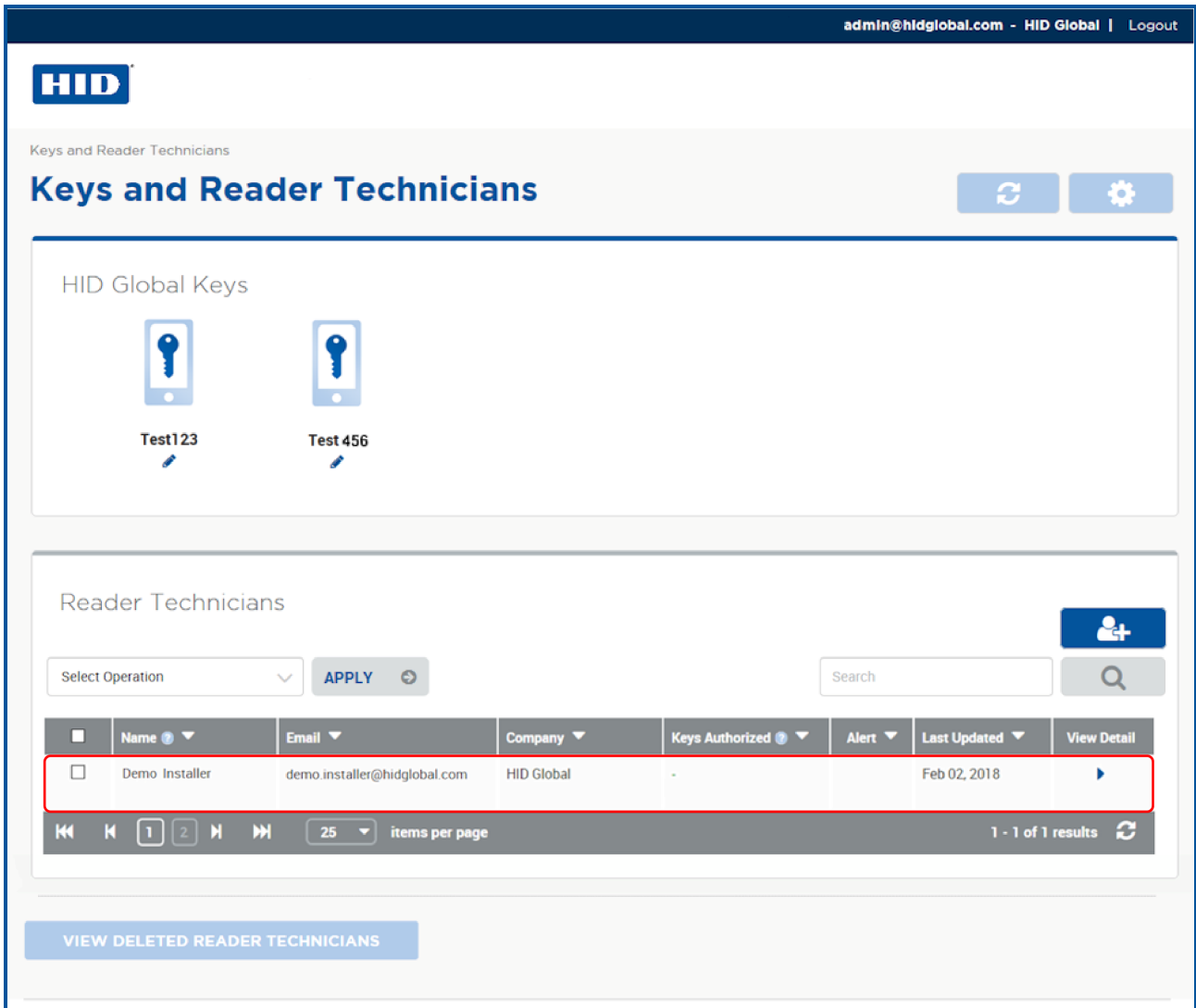
4. In the **Invitation & Key Authorization** section keep the default option:
 - **Send only invitation to the Reader Technician. Key Authorization(s) will need to be issued later.**
5. Click **Enroll**.

The screenshot shows the 'Invitation & Key Authorization' section. The question is 'How do you want to proceed?' and there are two radio button options:

- Send only invitation to Reader Technician. Key Authorization(s) will need to be issued later.
- Send invitation and Key Authorization(s) to Reader Technician.

At the bottom of the form, there are two buttons: 'CANCEL' and 'ENROLL'.

The newly enrolled Reader Technician is listed in the **Reader Technicians** section on the **Keys and Reader Technicians** page.

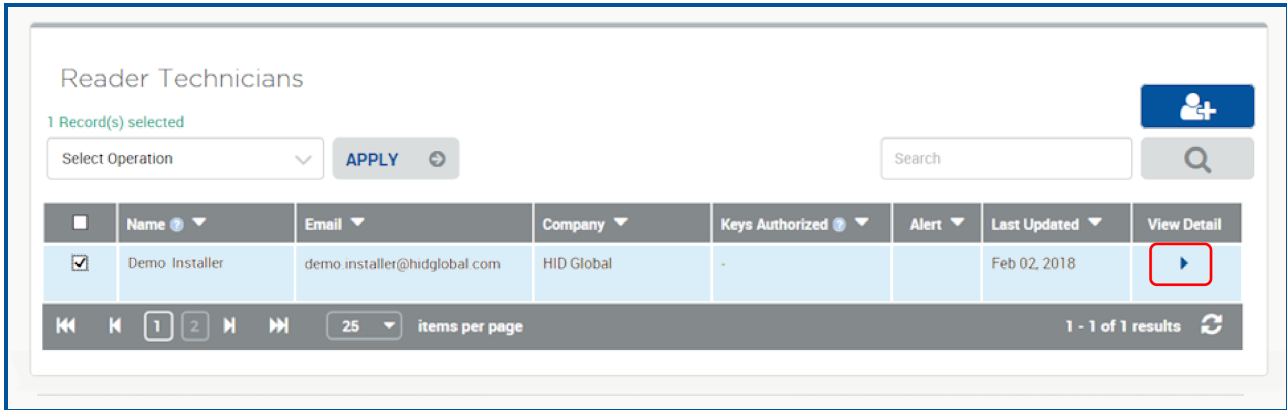


The enrolled Reader Technician will receive a Reader Manager invitation email in their registered email inbox containing an invitation code for activating the HID Reader Manager app. See **2.2.6 Activate the HID Reader Manager app**. When the Reader Manager app is activated the administrator can issue key authorization. See **3.5 Issue authorization keys**.

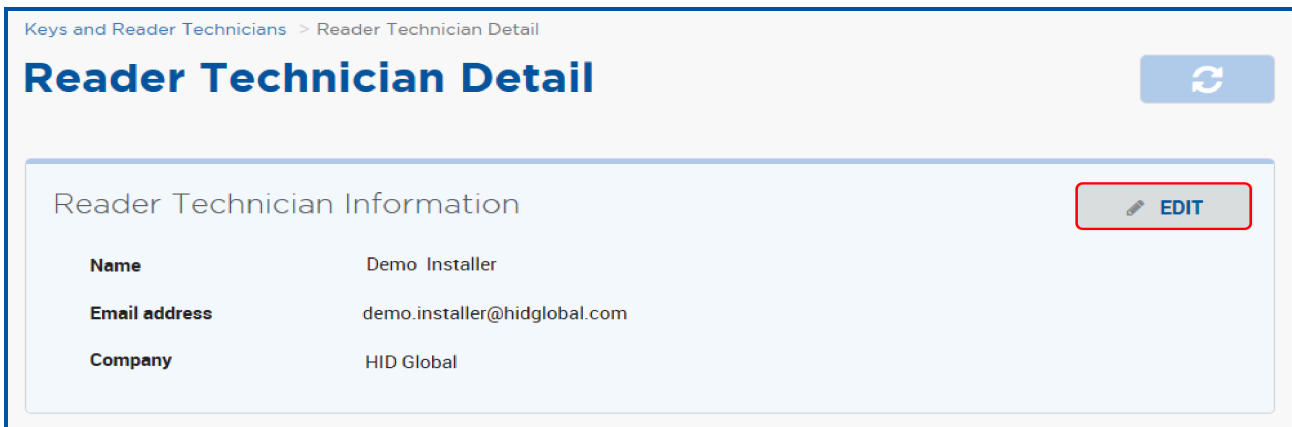
3.4.1 Edit Reader Technician information

To edit enrolled Reader Technician information:

1. Scroll to the **Reader Technicians** section on the **Keys and Reader Technicians** page.
2. Select a displayed Reader Technician entry and click on the associated **View Detail** icon [▶] to access the **Reader Technician Detail** page.



3. Click **EDIT** in the **Reader Technician Information** section.



4. Edit **Reader Technician Information** and click **SAVE**.
On the **Keys and Reader Technicians** page the updated Reader Technician information appears in the **Reader Technicians** list.
Note: If the Reader Technician uses the edited email address to log into the Reader Manager app then the mobile device must be registered again and all the authorization keys must be re-issued.

Keys and Reader Technicians > Reader Technician Detail

Reader Technician Detail

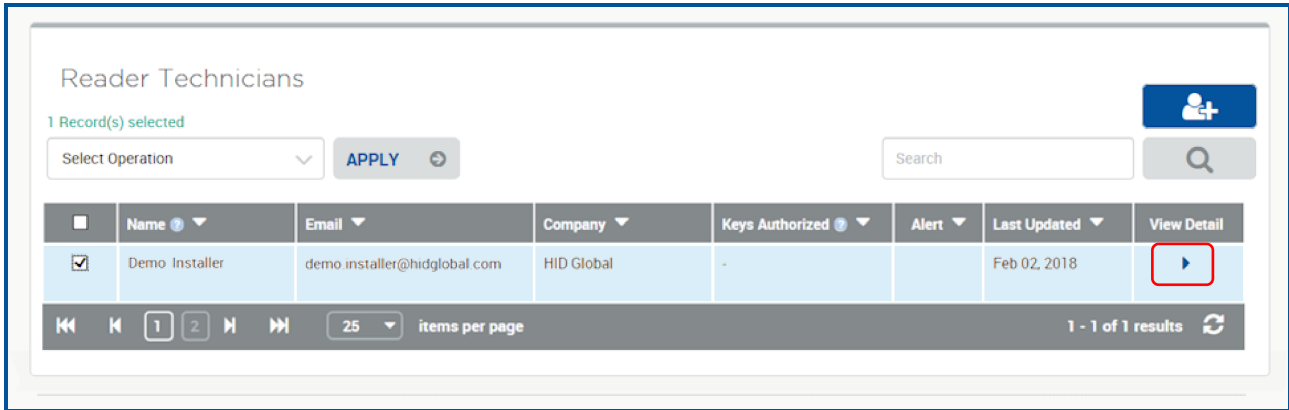
Reader Technician Information

| | | |
|----------------------|---|--|
| Name | <input type="text" value="Demo"/> | <input type="text" value="Installer"/> |
| Email address | <input type="text" value="demo.installer@hidglobal.com"/> | |
| Company | <input type="text" value="HID Global"/> | |

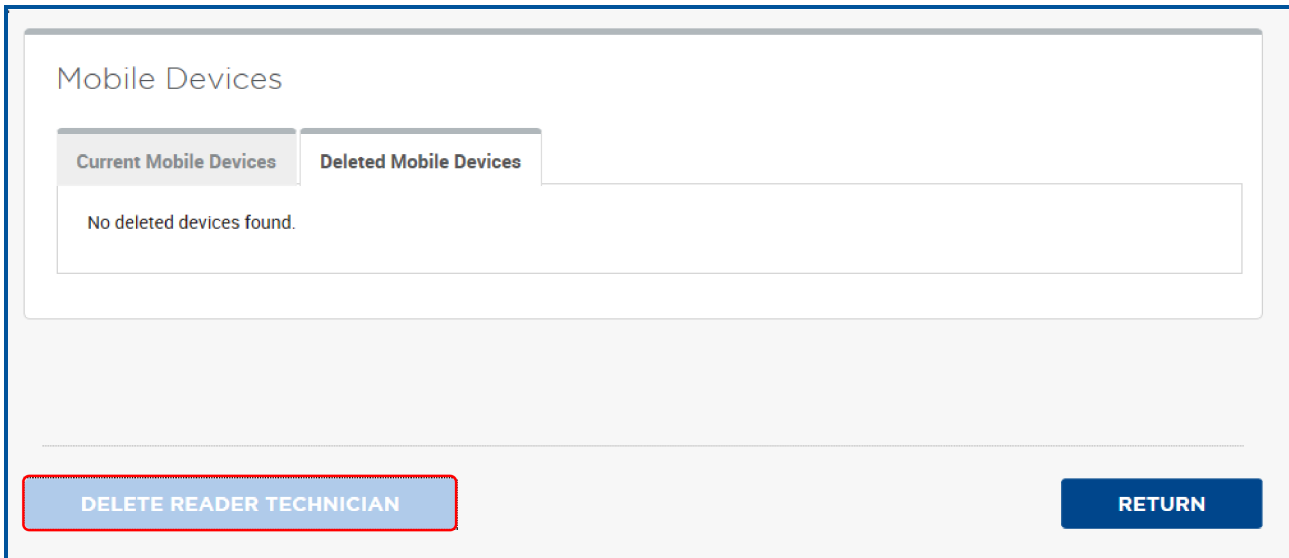
3.4.2 Delete an enrolled Reader Technician

To delete an enrolled Reader Technician:

1. Scroll to the **Reader Technicians** section on the **Keys and Reader Technicians** page.
2. Select a displayed Reader Technician entry and click on the associated **View Detail** icon [▶] to access the **Reader Technician Detail** page.



3. Scroll to the bottom of the **Reader Technician Detail** page and click **DELETE READER TECHNICIAN**.



4. Enter a **Reason for deletion** (optional) and click **YES** to delete the selected Reader Technician.
Note: Any key authorizations issued to the Reader technician will immediately have revocation attempted. If the mobile device is not reachable (for example, turned off or out of range), the system will periodically retry the delete operation.
When the Delete Threshold time (see **3.6.3 Configure Delete Threshold**), has elapsed the system automatically completes the delete operation and places the key authorization in a revoked state.

Delete Reader Technician

You are about to delete the selected Reader Technician. Mobile devices and assigned key authorisations will be deleted permanently from the HID Reader Manager. The Reader Technician will be moved to the Deleted Reader Technician's list.

Reason for deletion

Do you want to delete the selected Reader Technician?

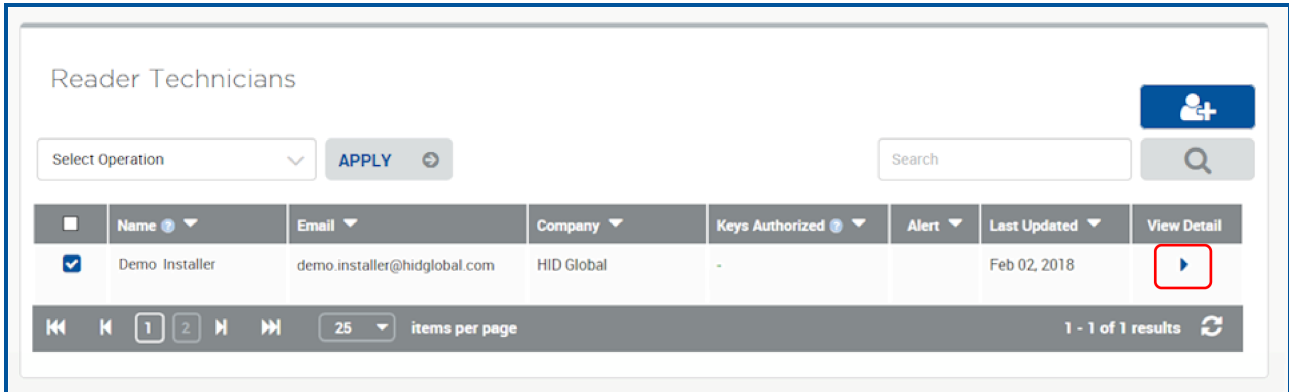
The deleted Reader Technician appears in the list of **Deleted Reader Technicians**.

3.5 Issue authorization keys

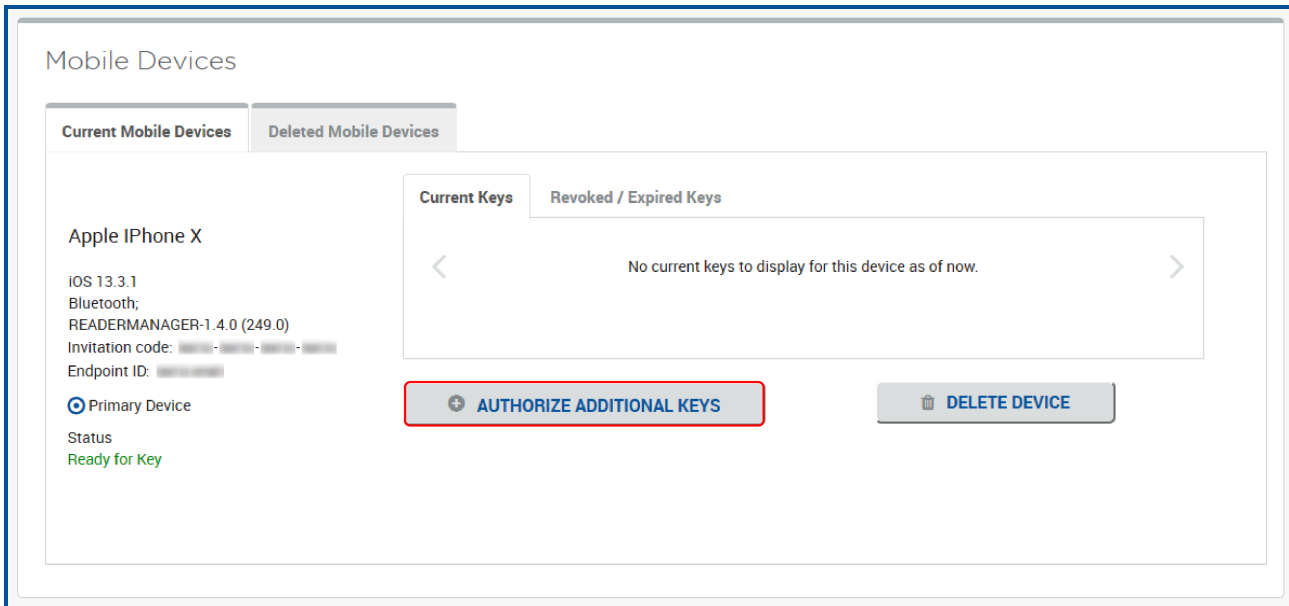
HID Reader Manager uses authorization keys to securely connect and control access by the mobile app.

To issue authorization keys in the HID Reader Manager Portal:

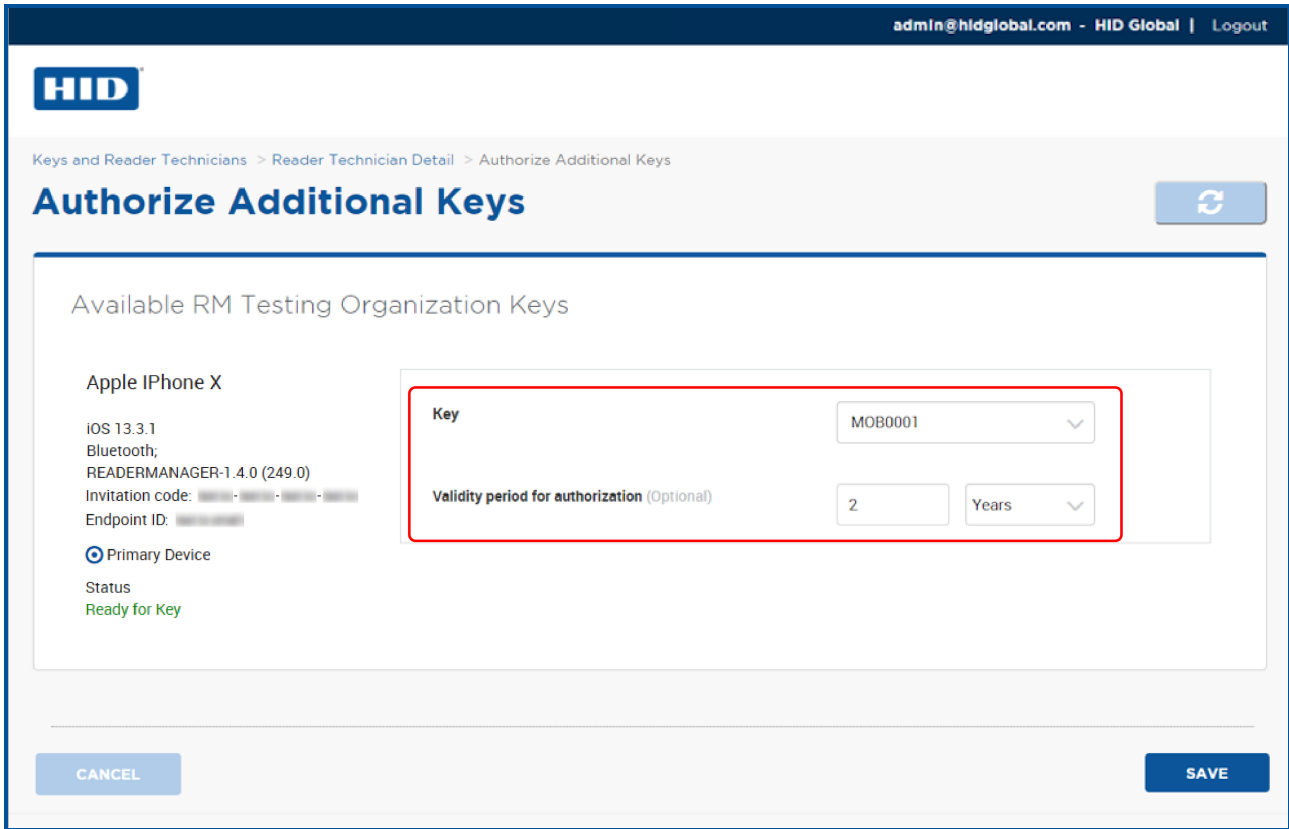
1. Scroll to the **Reader Technicians** section on the **Keys and Reader Technicians** page.
2. Select a displayed Reader Technician entry and click on the associated **View Detail** icon [▶] to access the **Reader Technician Detail** page.



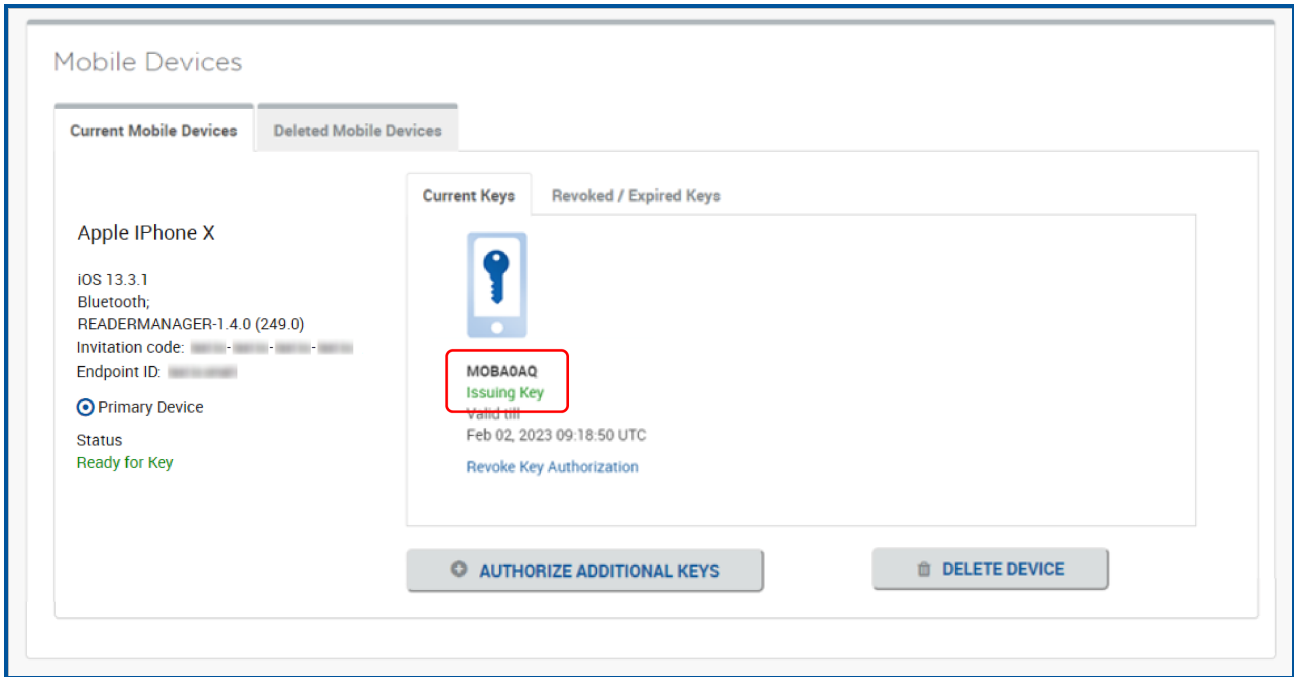
3. Scroll to the **Mobile Devices** section and click **AUTHORIZE ADDITIONAL KEYS**.



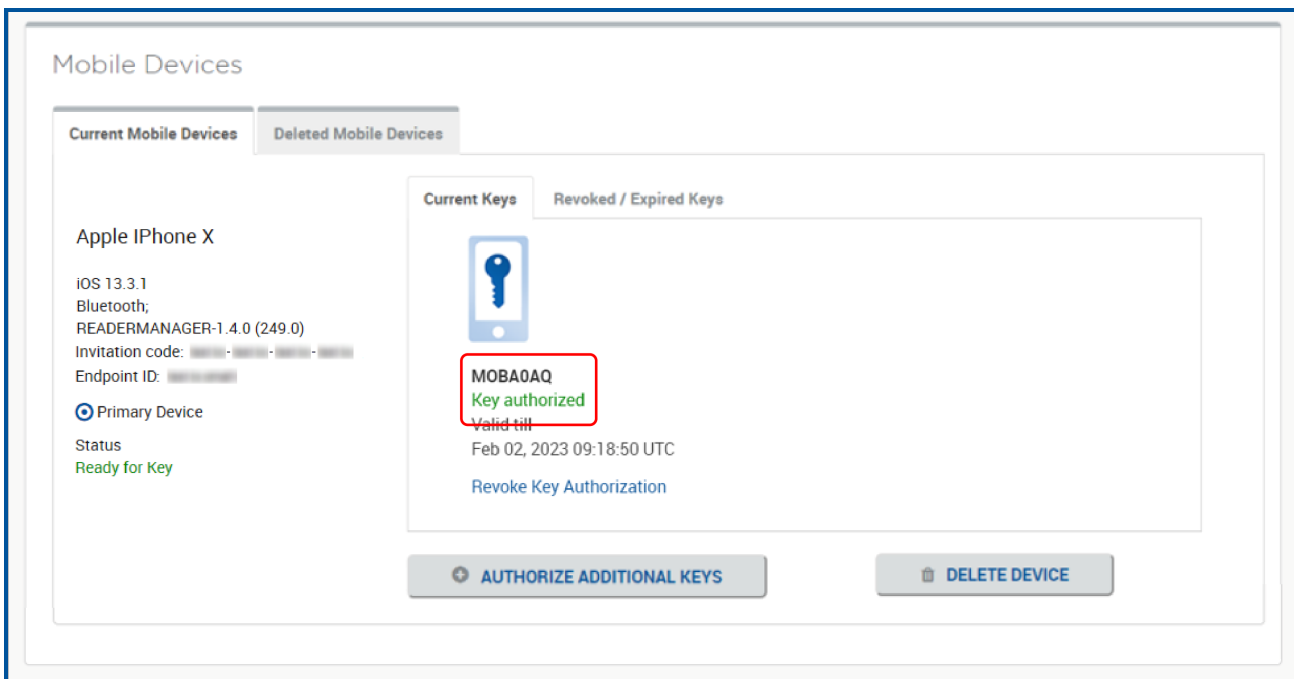
4. On the **Authorize Additional Keys** page select a key reference from the **Key** drop-down menu.
5. As an option set a authorization validity period.
Note: If the validity period for authorization is not set the default period is five years.
6. Click **SAVE**.



The status of the authorization key will change to **Issuing Key**.



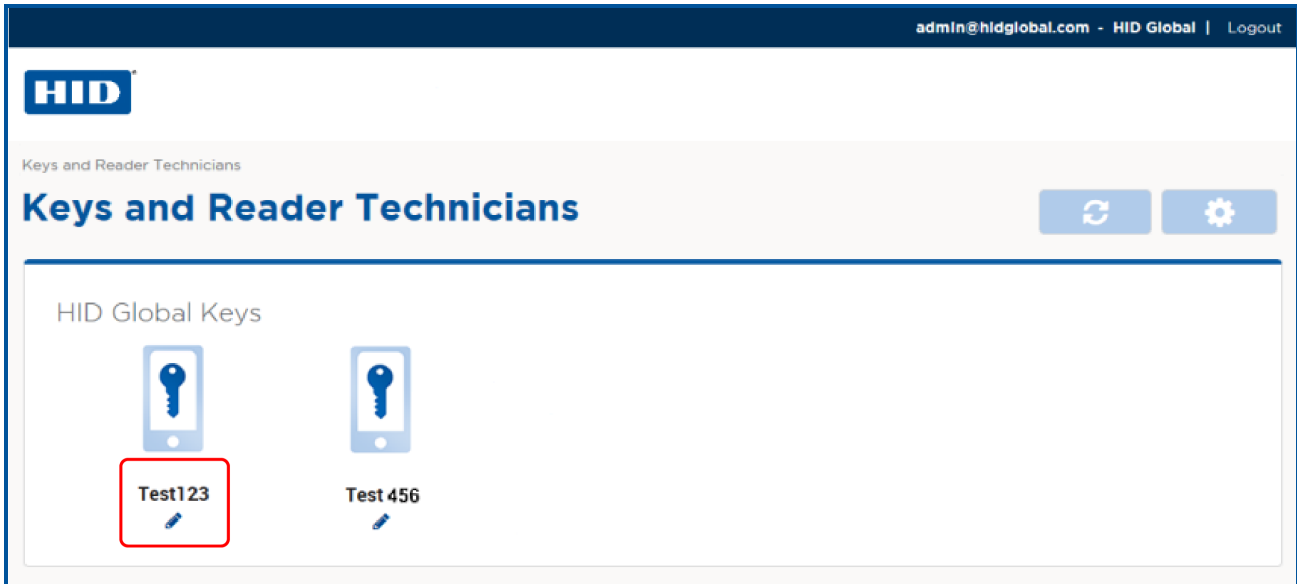
7. Check with the Reader Technician that the authorization key has been issued to the Reader Manager app. See **2.2.7 Display authorized keys**.
8. Refresh the **Reader Technician Detail** page and verify that the key status is changed to **Key authorized**.



3.5.1 Edit authorization key information

To edit authorization key information:

1. Click the edit icon [✎] associated with a displayed HID Global Key on the **Keys and Reader Technicians** page.

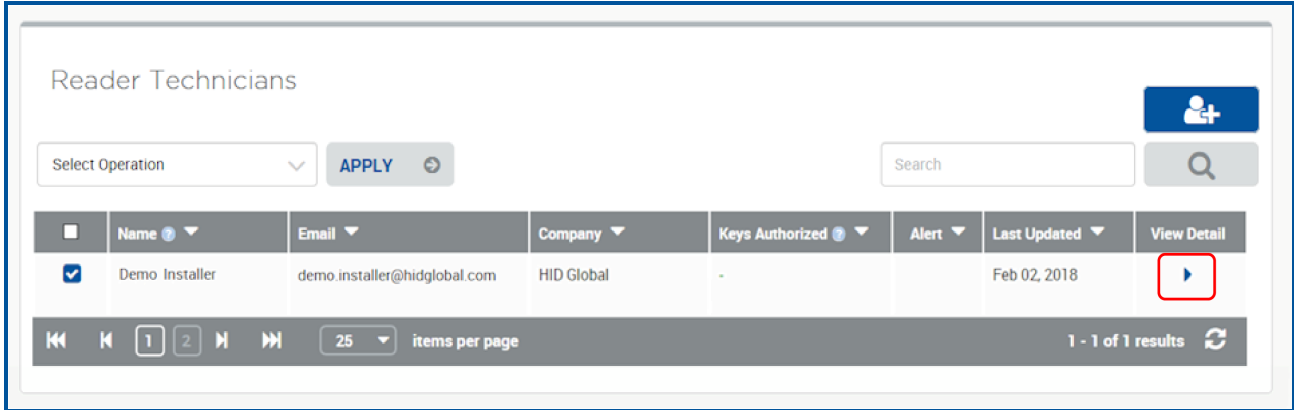


2. Edit the authorization key information as required and click **SAVE**.

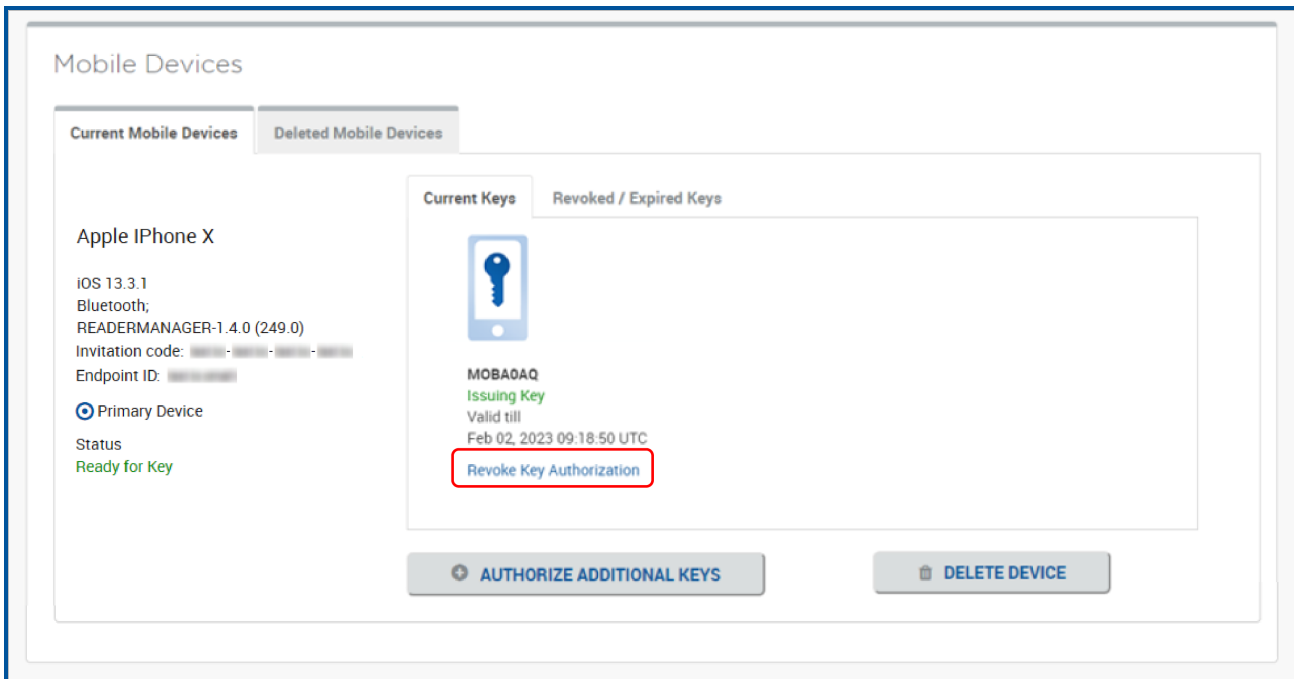
The screenshot shows the 'Edit Key Details' form. The form has a title 'Edit Key Details' and three input fields. The first field is labeled 'Key reference' and contains the value 'ICE65789'. The second field is labeled 'Friendly name of key' and contains the value 'Test123'. The third field is labeled 'Description (Optional)' and is empty. At the bottom of the form, there are two buttons: 'CANCEL' and 'SAVE'. The 'SAVE' button is highlighted with a red border.

3.5.2 Revoke (delete) an authorization key

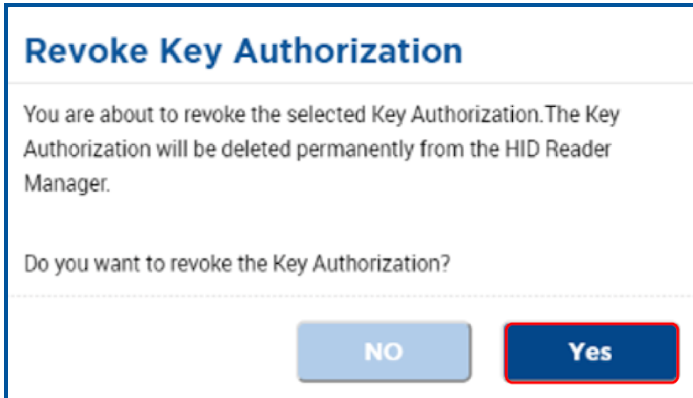
1. Scroll to the **Reader Technicians** section on the **Keys and Reader Technicians** page.
2. Select a displayed Reader Technician entry and click on the associated **View Detail** icon [▶] to access the **Reader Technician Detail** page.



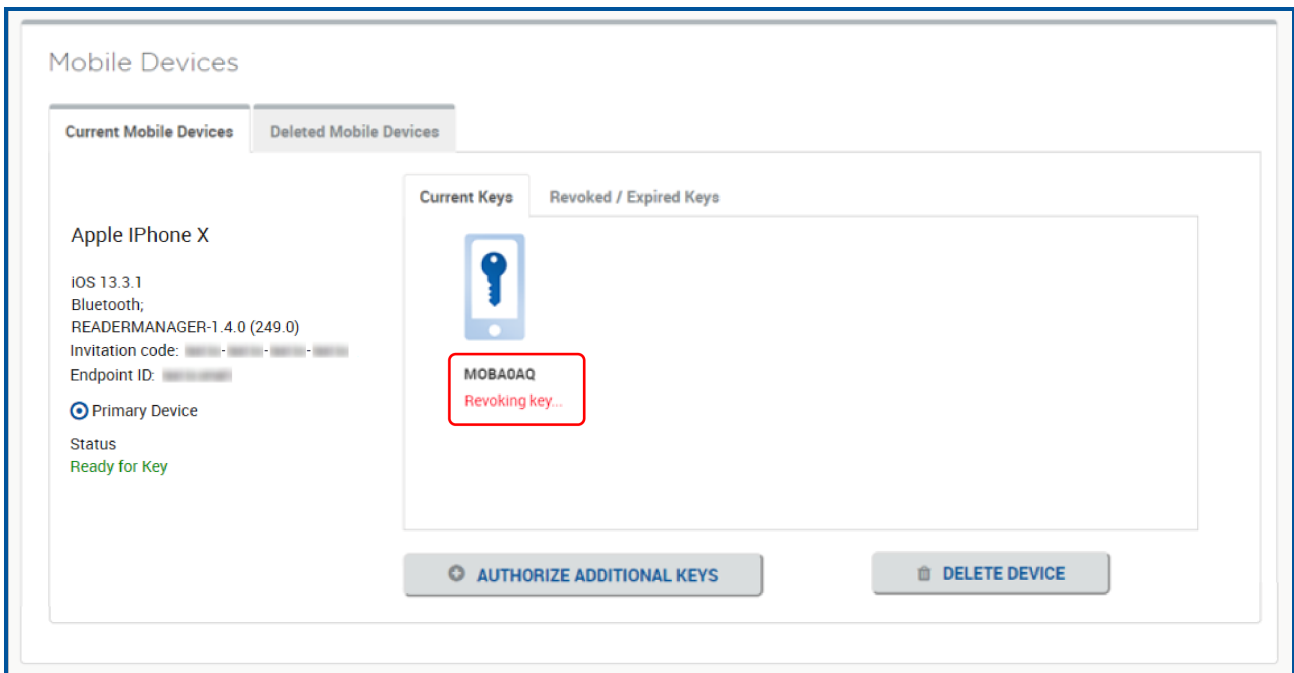
3. Scroll to the **Mobile Devices** section. For the authorization key to revoke, click **Revoke Key Authorization**.



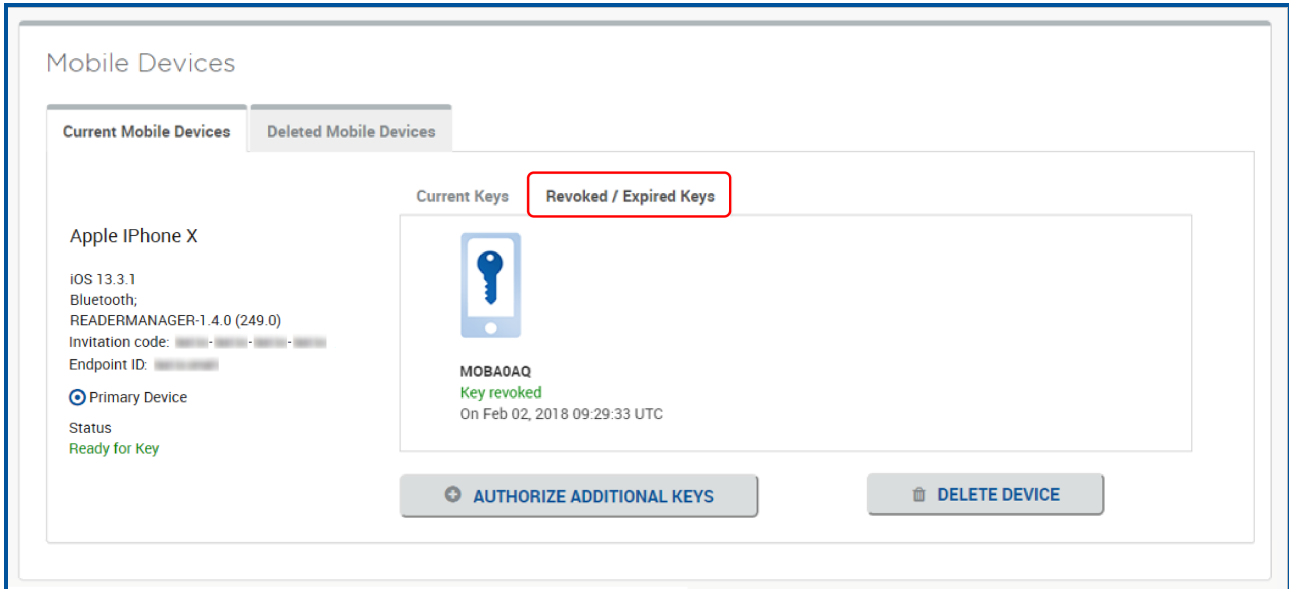
- Click **YES** to revoke the selected key authorization from the HID Reader Manager.
Note: Any key authorizations issued to the Reader technician will immediately have revocation attempted. If the mobile device is not reachable (for example, turned off or out of range), the system will periodically retry the delete operation.
When the Delete Threshold time (see **3.6.3 Configure Delete Threshold**), has elapsed the system automatically completes the delete operation and places the key authorization in a revoked state.




The authorization key status will change to **Revoking Key**.

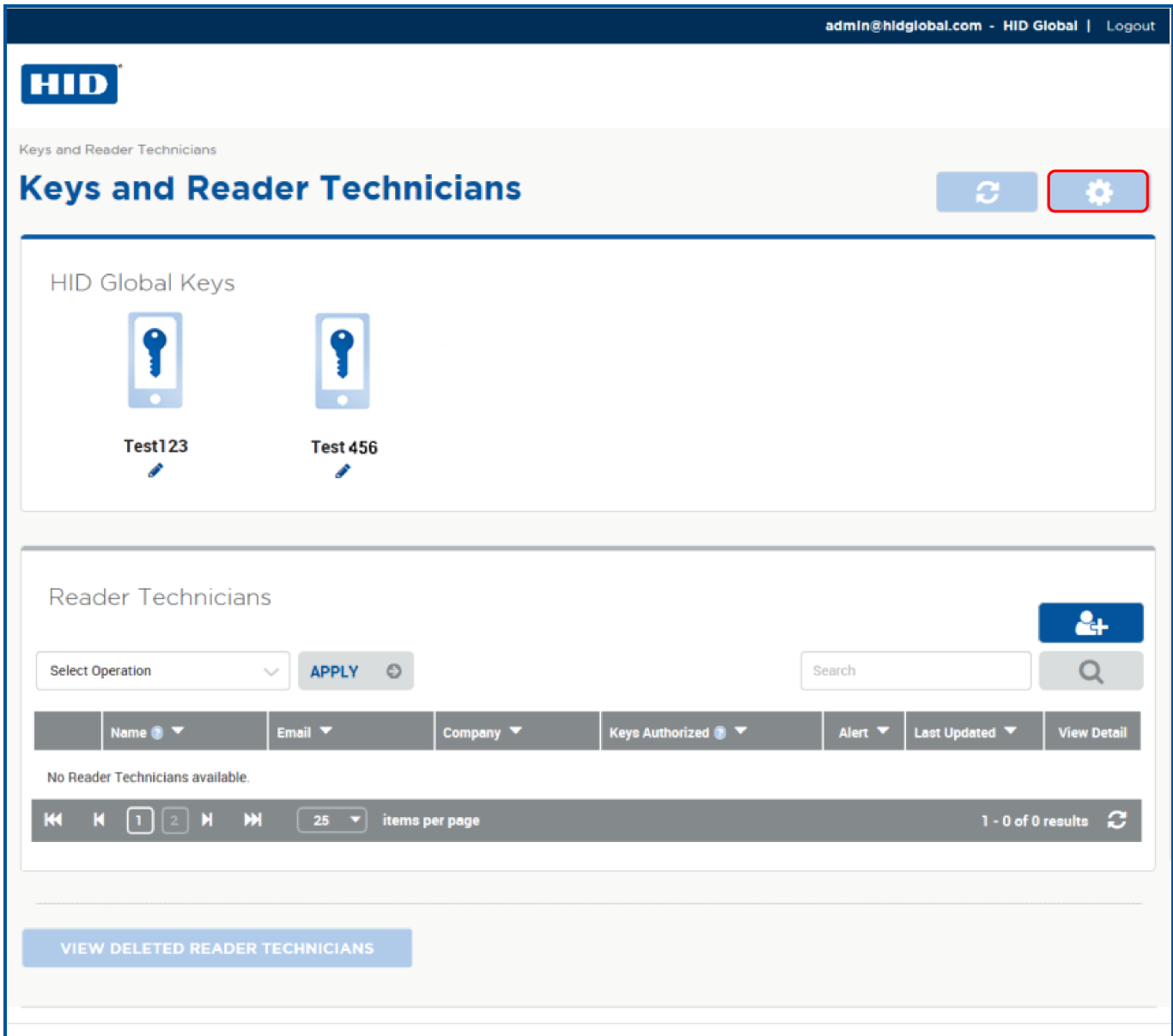


5. Check with the Reader Technician that the authorization key has been revoked in the HID Reader Manager app.
6. Refresh the **Reader Technician Detail** page and verify that the revoked key has been moved to the **Revoked / Expired Keys** tab.



3.6 Configure HID Reader Manager service settings

To access HID Reader Manager service settings click the **Settings** icon [] on the **Keys and Reader Technicians** page.



3.6.1 Export Reader Technician record settings

In the Export Settings section the options selected will determine the information fields included when Reader Technician records are exported.

Once the selections have been made, click **SAVE** to implement.

The screenshot shows the 'Export Settings' interface. At the top, it says 'Export Settings' and 'When Reader technician records are exported, they will include'. Below this, there are three sections with checkboxes:

- Reader Technician**: Name, Email, Company, Alert, Last updated
- Device**: Make, Model, Device status, End point ID, Invitation code
- Key Authorization**: Friendly name, Description, Key reference

3.6.2 Invitation Email settings

Select **VIEW / EDIT INVITATION EMAIL TEMPLATE** in the **Invitation Email Settings** section to access settings that allow you to edit the invitation email template.

Once template edits have been made, click **SAVE** to implement.

The screenshot shows the 'Invitation Email Settings' interface. It says 'When invitation email messages are sent, this template will be used'. Below this, there is a button with a document icon and the text **VIEW / EDIT INVITATION EMAIL TEMPLATE**.

3.6.3 Configure Delete Threshold

In the **Configure Delete Threshold** section set the **Delete threshold** period to determine when the system automatically completes a delete operation on an Authorization Key.

Note: When a change is made to the **Delete threshold** value, it does not apply to any keys revoked prior to the setting change.

Once the delete threshold period has been set, click **SAVE** to implement.

Configure Delete Threshold

When attempting to delete a mobile device or Revoke Key Authorization, if the mobile device is not reachable (e.g turned off or out of range), the system will periodically retry the delete operation.

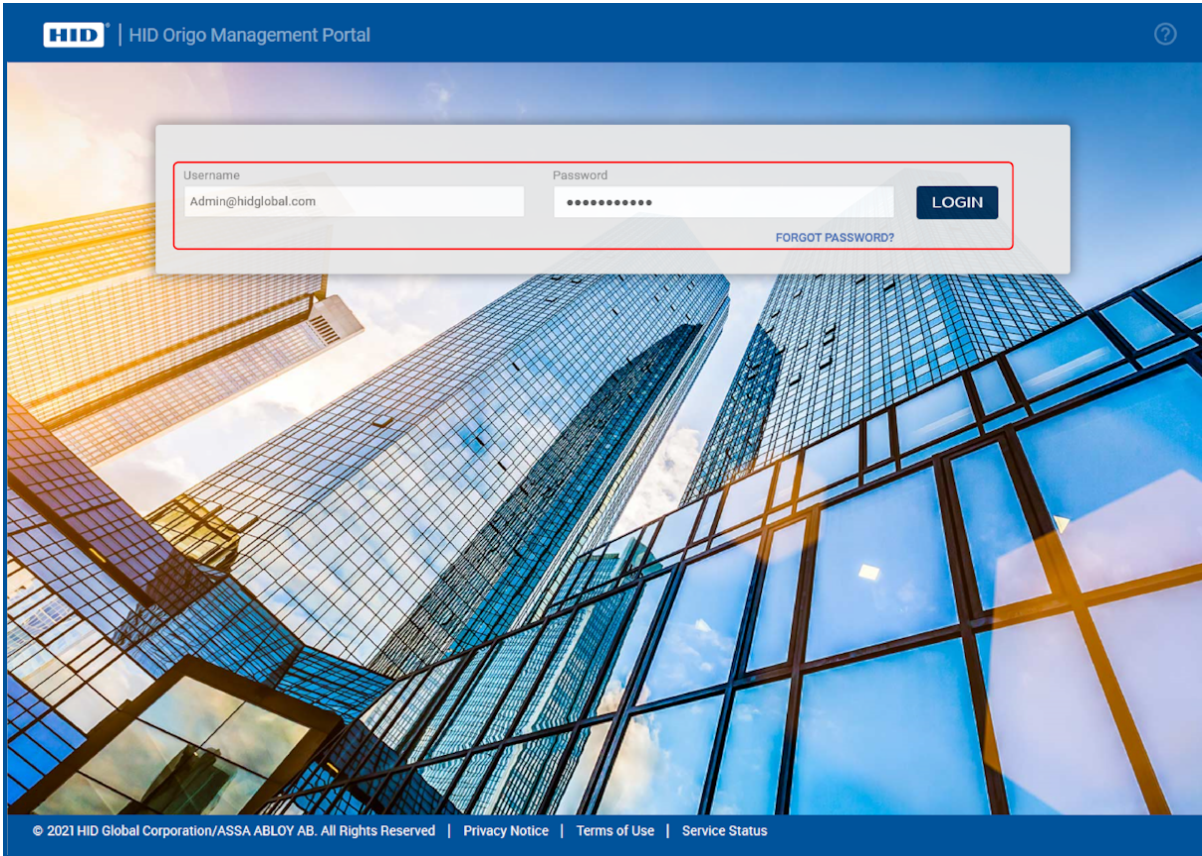
After the time configured below, the system automatically completes the delete operation and places the Key Authorization in a revoked state.

Delete threshold

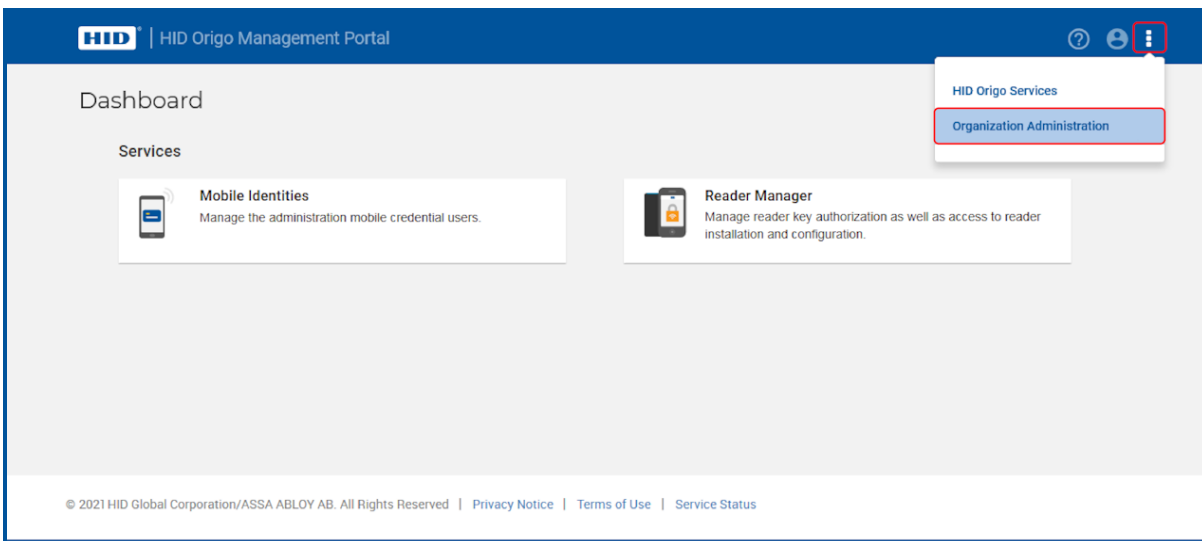
3.7 Add additional Reader Manager Admin

When adding a Reader Manager Admin for an Organization, the Organization Administrator must login to the HID Origo Management Portal and add the Administrators under the **Organization Administration** menu option.

1. Log into the Portal as Organization Admin.



2. Select the menu icon [☰] on the **Dashboard** screen, then select **Organization Administration**.



3. In the **Administrative Users** section, click **ADD ADMIN USER**.

| Administrative Person's Name | Email Address | Phone Number | Status | Services | Roles | Actions |
|------------------------------|----------------------|--------------|--------|-----------------------------------|------------------------------------|---------|
| Adminuser1 | Adminuser1@gmail.com | | Active | Mobile Identities, Reader Manager | MI Administrator, RM Administrator | |
| Adminuser2 | Adminuser2@gmail.com | | Active | Mobile Identities, Reader Manager | MI Administrator, RM Administrator | |
| Adminuser3 | Adminuser3@gmail.com | | Active | Mobile Identities, Reader Manager | MI Administrator, RM Administrator | |

4. Enter **User Information** and in the **Service/Role** table enable the **RM Administrator** role. Click **Save**.

Note: The email address can only be an Admin to one account. Existing Admins cannot be added.

Add Administrative User [CANCEL] [SAVE]

User Information

Name: Admin [User4]

Business email address (this will be used as the user ID): Adminuser4@gmail.com

Confirm email address: Adminuser4@gmail.com

Phone number: [] Country: United States of America Country code: 1 Phone (Area code + Phone number): []

Select the services and roles to be assigned to this administrative user

| Service | Role |
|-----------------------------|---|
| | <input checked="" type="checkbox"/> None |
| | <input type="checkbox"/> MI Reviewer Read only access. Can not add or edit data nor issue or revoke Mobile IDs. |
| Mobile Identities | <input type="checkbox"/> MI Operator Partial access to functionality. Able to add mobile users and issue and revoke Mobile IDs, but cannot perform configuration operations. |
| | <input type="checkbox"/> MI Administrator Full access to all functionality. |
| Organization Administration | <input checked="" type="checkbox"/> Org Admin Enables the 'Administration' feature. Able to add, edit, delete portal users and perform password resets on their accounts. |
| Reader Manager | <input checked="" type="checkbox"/> RM Administrator Service for the Reader Manager, Full access to all the RM activity |

5. You will be notified that a new administrative user has been added. Click **Logout** to exit the Portal.

HID | HID Origo Management Portal

Administration Dashboard

✓ New Administrative user has been added successfully!

Organization Summary

| | | | |
|----------------------|--|----------|--|
| Organization name | HID Origo Demo | Services | Mobile Identities, Organization Administration, Reader Manager |
| Organization ID | 5551859 | Status | Active |
| Organization Address | Tech Ridge Austin, TX 78753 United States of America | | |

[SETTINGS] [EDIT]

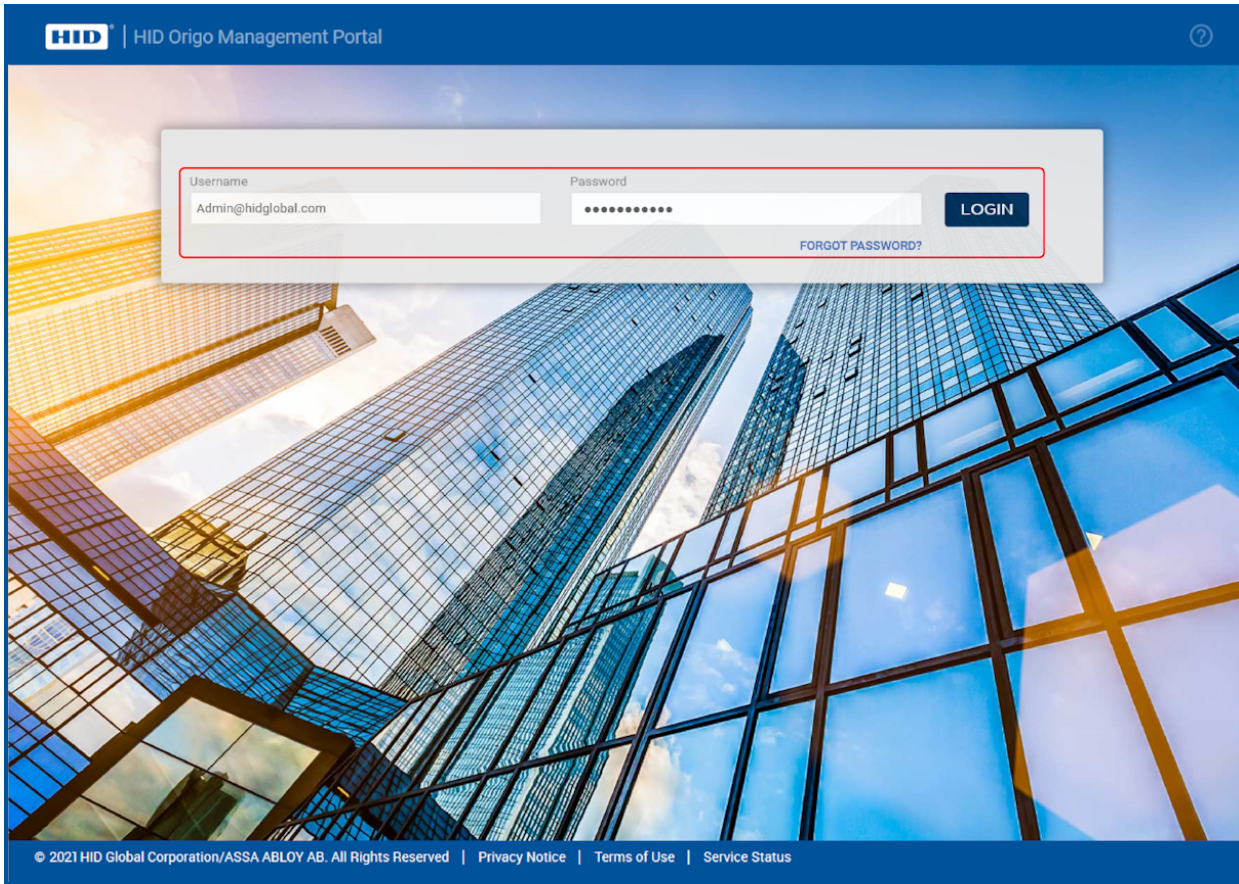
- The newly created Reader Manager Administrator should check their email inbox for an email containing a username, a temporary password, and a Portal landing page link. Click the **Here** link in the email to be directed to the portal **Set Up Account** page.
- On the **Set Up Account** page, create a new password (refer to the on screen password requirements). If required, opt for additional login security. Accept the Privacy Statement Agreement and click **SAVE** to log out of the portal.

The screenshot shows the 'Set Up Account' page. At the top left is the HID logo. Below it, the text 'Set Up Account' is displayed. The main heading is 'Set Up Account'. Underneath, there is a section titled 'Login & Security' with a sub-heading 'Control your password and account access. Your password protects your account. You can also add a second layer of protection with 2-Step Authentication, which sends a one-time-verification code to your phone for you to enter when you sign in.' Below this is a 'Password' section with 'Password guidelines' listed: Minimum 8 characters, Upper case and lower case letters, Minimum one number, Minimum one special character, and Should not use your email address. There are two password input fields: 'New password' and 'Confirm password'. The 'New password' field has a strength indicator showing '72%'. Below the password fields is a 'Multi-Factor Authentication' section with a checkbox labeled 'Turn on the MultiFactor authentication'. At the bottom of the page, there are 'CANCEL' and 'SAVE' buttons.

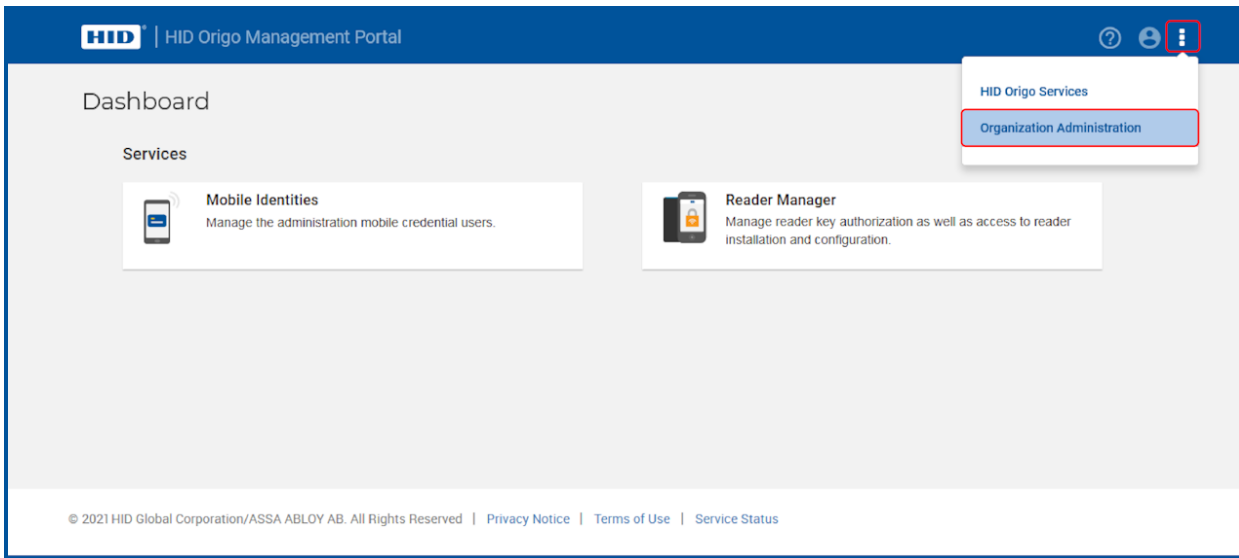
- The RM Administrator can now log back into the HID Origo Management Portal using their new password and select the **Reader Manager** option to be redirected to HID Reader Manager. For detailed information, see [3.3 Access the Reader Manager service](#).


3.8 Edit existing Admin Services and Roles

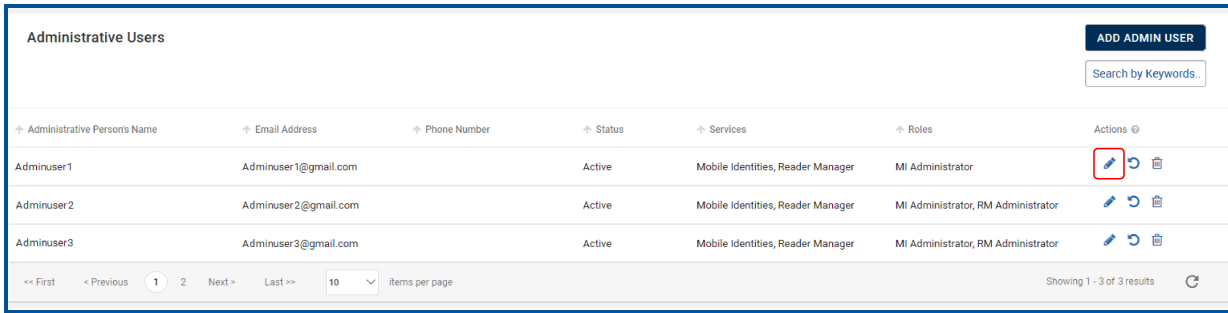
1. Log into the HID Origo Management Portal as Organization Admin.












2. Select the menu icon [⋮] on the **Dashboard** screen, then select **Organization Administration**.



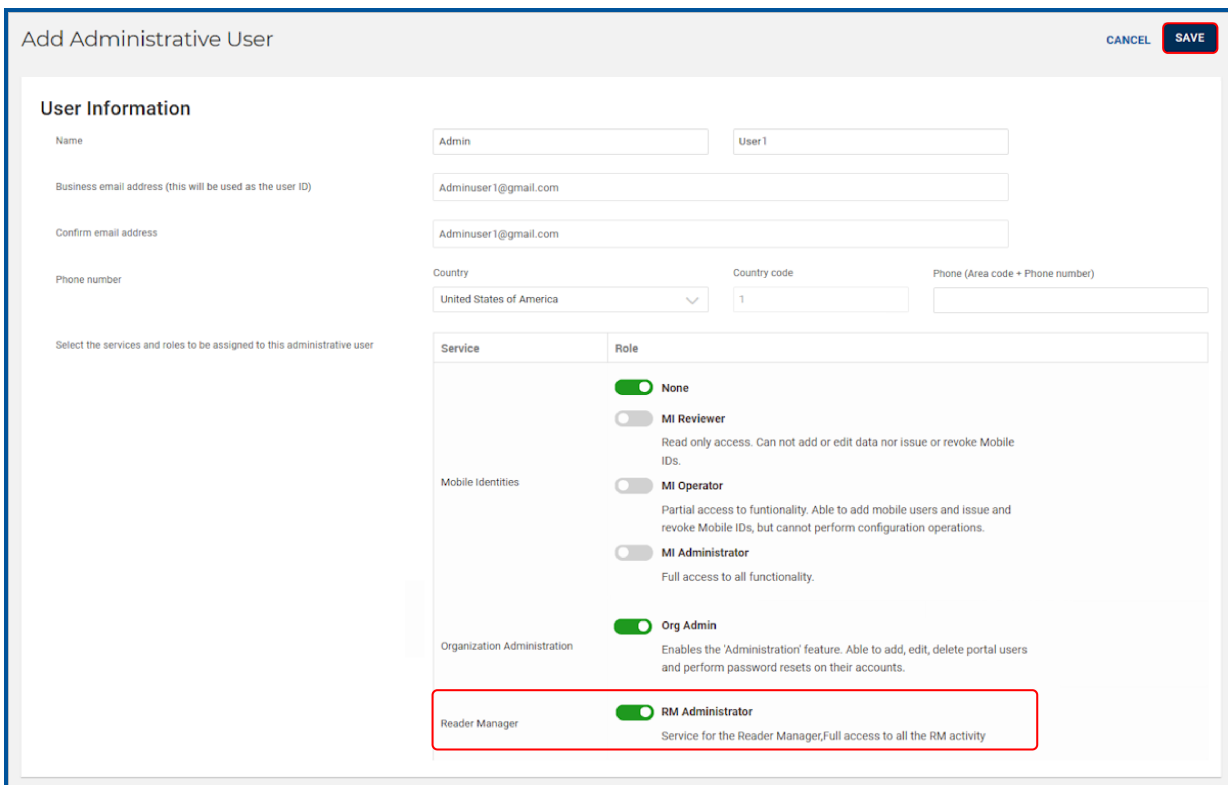
3. In the **Administrative Users** section, click the on the edit icon [] associated with a listed user.



| Administrative Person's Name | Email Address | Phone Number | Status | Services | Roles | Actions |
|------------------------------|----------------------|--------------|--------|-----------------------------------|------------------------------------|---|
| Adminuser1 | Adminuser1@gmail.com | | Active | Mobile Identities, Reader Manager | MI Administrator |    |
| Adminuser2 | Adminuser2@gmail.com | | Active | Mobile Identities, Reader Manager | MI Administrator, RM Administrator |    |
| Adminuser3 | Adminuser3@gmail.com | | Active | Mobile Identities, Reader Manager | MI Administrator, RM Administrator |    |

4. In the **Service/Role** table enable the **RM Administrator** option.

5. Click **Save** and log out of the portal.



Add Administrative User [CANCEL] [SAVE]

User Information

Name: Admin | User1

Business email address (this will be used as the user ID): Adminuser1@gmail.com

Confirm email address: Adminuser1@gmail.com

Phone number: []

Country: United States of America | Country code: 1 | Phone (Area code + Phone number): []

| Service | Role |
|-----------------------------|---|
| | <input checked="" type="checkbox"/> None |
| | <input type="checkbox"/> MI Reviewer Read only access. Can not add or edit data nor issue or revoke Mobile IDs. |
| Mobile Identities | <input type="checkbox"/> MI Operator Partial access to functionality. Able to add mobile users and issue and revoke Mobile IDs, but cannot perform configuration operations. |
| | <input type="checkbox"/> MI Administrator Full access to all functionality. |
| Organization Administration | <input checked="" type="checkbox"/> Org Admin Enables the 'Administration' feature. Able to add, edit, delete portal users and perform password resets on their accounts. |
| Reader Manager | <input checked="" type="checkbox"/> RM Administrator Service for the Reader Manager, Full access to all the RM activity |

6. The RM Administrator can now log back into the HID Origo Management Portal and select the **Reader Manager** option to be redirected to the Reader Manager service. For detailed information, see [3.3 Access the Reader Manager service](#).

Section **04**

Troubleshooting

4.1 Reader Manager App messages

4.1.1 Error and warning messages

| Message | Description and next step to attempt resolution |
|--|---|
| <i>"There does not seem to be an internet connection."</i> | Internet connectivity is not available for the mobile device. Check the mobile device Settings > Connections. |
| <i>"Problem connecting to HID Servers."</i> | The Reader Manager app could not reach HID Reader Manager servers. Please check mobile device Internet connection. |
| <i>"Issues at HID Servers, please try again."</i> | HID Reader Manager servers are down. Please periodically try again and check your email for any service distribution notification. If the issue persists uninstall and reinstall the app and try to log in again. |
| <i>"Invalid Email or Password."</i> | The entered username or password or both are incorrect. Passwords cannot contain the following characters Please enter a valid email or password. |
| <i>"Invalid Email."</i> | The entered email address is incorrect. Please enter a valid email. |
| <i>"This user already exists."</i> | During registration the entered user is already registered. Login using existing email or reset password for this email. |
| <i>"Failed to register the user."</i> | The user tries to register when HID Reader Manager servers are down. Please periodically try again and check your email for any service distribution notification. |
| <i>"This category already exists."</i> | The user tries to add a template category that already exists. Please use a new category or select the existing category. |
| <i>"You are not authorized to apply this template."</i> | The user is not authorized to apply the template. Please request key authorization for this reader from the Reader Manager Service Administrator. |
| <i>"The template can not be applied. iCLASS SE reader does not support the selected {configuration_item} in the template."</i> | The template being applied to the reader contains configuration items not supported by the reader. Make sure the configuration items in the template are valid for your reader. |
| <i>"Invalid Invitation Code, Please Try again."</i> | The user has entered an incorrect or invalid invitation code. Please ensure the code was entered correctly. If the issue persists contact the Reader ManagerService Administrator to check if the code has already been redeemed and to request a new invite code. |
| <i>"Failed to connect to reader."</i> | Lost BLE connection. The reader does not respond to the Reader Manager app. Ensure the BLE module is seated securely (iCLASS SE reader only), devices is compatible HID Reader Manager, and the reader is properly powered. Please try again with the mobile device closer to the reader. |
| <i>"There was an error during the name change."</i> | During a Change Reader Name transaction the BLE/Internet connection is disrupted. Please try again. |

| Message | Description and next step to attempt resolution |
|---|--|
| <i>"You are not authorized to configure this reader."</i> | The user does not have authorization keys/credentials to access the reader. Please request key authorization for this reader from the Reader Manager Service Administrator. |
| <i>"An unknown error has occurred."</i> | A general non-specific error has occurred. Please try again. |
| <i>"Please close all other applications on this device and ensure it remains unlocked during upgrade."</i> | Before upgrade close all open applications on the mobile device to avoid BLE collision. |
| <i>"Required permission to access Readers."</i> | The user has disabled device Location Services for the Reader Manager app. Please enable location services for the reader manager app in the mobile device settings. |
| <i>"To reenable, please go to Settings and turn on Location Service for this app."</i> | The user should ensure mobile device Location Services is enabled for the Reader Manager app. |
| <i>"Please power cycle your reader."</i> | Power cycle the reader to authenticate the user and proceed with transactions such as upgrade firmware, updating config items. |
| <i>"The version of firmware currently loaded is not supported with the HID Reader Manger application. Please refer to the user guide located on home screen for supported firmware versions."</i> | The firmware version is unsupported by the Reader Manager app. |
| <i>"This module can not be used to upgrade the Reader. Use the module with the latest firmware."</i> | The BLE smart module firmware/hardware version is unsupported by the Reader Manager app. Please ensure the module used for the upgrade is from an Bluetooth and OSDP Upgrade Kit. See A.2.1 iCLASS SE Bluetooth & OSDP upgrade kits . |
| <i>"This reader is protected using Custom Admin keys and can not be configured or upgraded."</i> | The reader is configured with custom keys. The reader technician cannot proceed with configuration changes or upgrade as this reader is not supported. |
| <i>"SNMP Authentication Failed. This reader has previously been updated with SNMP keys which have not been synched with the Reader Manager service due to this Reader Manager cannot be used to configure or upgrade the Reader."</i> | HID Reader Manager does not upgrade and/or configure a reader that has had the SNMP keys rolled using Configuration Cards (specifically, SEC9X-CRD-E-P000, SEC9X-CRD-E-P002, or CP1000D Configuration Cards), as the new SNMP keys have not been synched with the Reader Manager Service. A resolution for this issue is targeted for a future HID Reader Manager release. |

4.1.2 Information messages

| Message | Description and next step to attempt resolution |
|--|--|
| <i>"You will receive an email at {registered_email} to activate your Account."</i> | Information message to the user to activate the account with the mail sent to registered email address. Please activate account to use the application. |
| <i>"No reader found"</i> | No nearby readers found during Scan For Readers action. Please move the mobile device closer to the reader and scan for readers again. |
| <i>"Reader beeping complete"</i> | Locating the reader is completed. Reader is identified and can now be tagged or inspected. |
| <i>"A new category was saved"</i> | A new template category added has been successfully added and saved. |
| <i>"Your template has been saved"</i> | A new template has been successfully added and saved. |

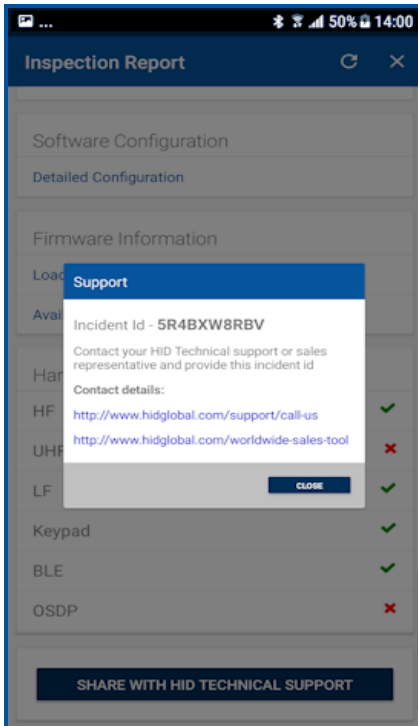
4.1.3 Validation messages

| Message | Description and next step to attempt resolution |
|---|--|
| <i>"New Password is not compliant to requirements"</i> | The new Password entered has not met the password requirement rules. Please use a password which meets the requirements detailed on the screen. |
| <i>"New Password & Confirm New Password are not same"</i> | The entered Password and Confirm password do not match. Please re-enter passwords. |
| <i>"Invalid old Password"</i> | A previously used password has attempted to be used. Please use a different password. |
| <i>"No Configuration item has been selected"</i> | User tries to save reader configuration options without selecting any configuration values. Please select a configuration option before saving. |

4.2 Contact HID Technical Support

When using the Reader Manager app, if any issues are experienced with a reader, for example, Locate reader, Inspect reader, View Detailed Inspection Report, Configure reader, Upgrade firmware, an **Incident Id** can be generated.

1. On the **Inspection Report** screen, tap **Share with HID Technical Support**.
2. An **Incident Id** reference number will be generated and HID Support contact details are displayed. Take a note of the **Incident Id** reference number and provide this when contacting HID Technical Support about the issue.



Appendix **A**

Reader upgrade

A.1 Supported firmware versions for upgrade

A.1.1 HID SE readers

| Reader FW | Admin Configuration | Supported? | Comment |
|-----------|---------------------|------------|---|
| R7 SP1 | Standard | No | Requires module firmware from 8.6.0.4 release |
| R7 SP1 | ICE | No | Requires module firmware from 8.6.0.4 release |
| R7 SP3 | Standard | No | Requires module firmware from 8.6.0.4 release |
| R7 SP3 | ICE | No | Requires module firmware from 8.6.0.4 release |
| R7 SP8 | Standard | No | Requires module firmware from 8.6.0.4 release |
| R7 SP8 | ICE | No | Requires module firmware from 8.6.0.4 release |
| R8.2.1 | Standard | No | |
| R8.2.1 | ICE | No | |
| R8.2.2 | Standard | No | |
| R8.2.2 | ICE | No | |
| R8.3.0 | Standard | No | |
| R8.3.0 | ICE/MOB | No | Under investigation |
| R8.3.1.6 | Standard | No | |
| R8.3.1.6 | ICE/MOB | No | Under investigation |
| R8.3.2.1 | Standard | No | |
| R8.3.2.1 | ICE/MOB | No | Under investigation |
| R8.4.0.6* | Standard | Yes | From Reader Manager 1.6.0 or higher an upgrade path to the latest firmware is provided through a two step approach which includes upgrade to 8.6.0.4 and then to the latest firmware. Please note that this requires user intervention as it includes initiation of the reader upgrade process twice. |
| R8.4.0.6 | ICE/MOB | Yes | From Reader Manager 1.6.0 or higher an upgrade path to the latest firmware is provided through a two step approach which includes upgrade to 8.6.0.4 and then to the latest firmware. Please note that this requires user intervention as it includes initiation of the reader upgrade process twice. |
| R8.4.1.0* | Standard | Yes | From Reader Manager 1.6.0 or higher an upgrade path to the latest firmware is provided through a two step approach which includes upgrade to 8.6.0.4 and then to the latest firmware. Please note that this requires user intervention as it includes initiation of the reader upgrade process twice. |
| R8.4.1.0 | ICE/MOB | Yes | From Reader Manager 1.6.0 or higher an upgrade path to the latest firmware is provided through a two step approach which includes upgrade to 8.6.0.4 and then to the latest firmware. Please note that this requires user intervention as it includes initiation of the reader upgrade process twice. |

| Reader FW | Admin Configuration | Supported? | Comment |
|-----------|---------------------|------------|---|
| R8.4.2.0* | Standard | Yes | From Reader Manager 1.6.0 or higher an upgrade path to the latest firmware is provided through a two step approach which includes upgrade to 8.6.0.4 and then to the latest firmware. Please note that this requires user intervention as it includes initiation of the reader upgrade process twice. |
| R8.4.2.1 | ICE/MOB | Yes | From Reader Manager 1.6.0 or higher an upgrade path to the latest firmware is provided through a two step approach which includes upgrade to 8.6.0.4 and then to the latest firmware. Please note that this requires user intervention as it includes initiation of the reader upgrade process twice. |
| R8.5.0.9* | Standard | Yes | From Reader Manager 1.6.0 or higher an upgrade path to the latest firmware is provided through a two step approach which includes upgrade to 8.6.0.4 and then to the latest firmware. Please note that this requires user intervention as it includes initiation of the reader upgrade process twice. |
| R8.5.0.9 | ICE/MOB | Yes | From Reader Manager 1.6.0 or higher an upgrade path to the latest firmware is provided through a two step approach which includes upgrade to 8.6.0.4 and then to the latest firmware. Please note that this requires user intervention as it includes initiation of the reader upgrade process twice. |
| R8.6.0.4 | Standard | Yes | |
| R8.6.0.4 | ICE/MOB | Yes | |
| R8.7 | Standard | Yes | SE Biometric readers only |
| R8.7 | ICE/MOB | Yes | SE Biometric readers only |
| R8.8.0.11 | Standard | Yes | |
| R8.8.0.11 | ICE/MOB | Yes | |
| R8.9.0.11 | Standard | Yes | |
| R8.9.0.11 | ICE/MOB | Yes | |
| R8.9.1.3 | Standard | Yes | |
| R8.9.1.3 | ICE/MOB | Yes | |
| R8.9.1.4 | Standard | Yes | Firmware upgrade from R8.9.1.3, R8.9.0.11, R8.6.0.4, R8.5.0.9, R8.4.2.1, R8.4.2.0, and R8.4.1.0 to R8.9.1.4 is supported. |
| R8.9.1.4 | ICE/MOB | Yes | Firmware upgrade from R8.9.1.3, R8.9.0.11, R8.6.0.4, R8.5.0.9, R8.4.2.1, R8.4.2.0, and R8.4.1.0 to R8.9.1.4 is supported. |

*Support for R8.4.0.6, R8.4.1.0, R8.4.2.0, and R8.5.0.9 Standard readers does not enforce the power cycle requirement, however, as they require the 8.6.0.4 version of module they indirectly require power cycle.

A.1.2 HID SE Express readers

| Reader FW | Admin Configuration | Supported? | Comment |
|-----------|---------------------|------------|---------|
| R9.0.0.17 | Standard | Yes | |
| R9.0.0.17 | ICE/MOB | Yes | |

A.1.3 HID Signo reader

| Reader FW | Admin Configuration | Supported? | Comment |
|------------|---------------------|------------|---|
| R10.0.0.31 | Standard | Yes | |
| R10.0.0.31 | ICE/MOB | Yes | |
| R10.0.1.0 | Standard | Yes | |
| R10.0.1.0 | ICE/MOB | Yes | |
| R10.0.1.1 | Standard | Yes | |
| R10.0.1.1 | ICE/MOB | Yes | |
| R10.0.1.3 | Standard | Yes | |
| R10.0.1.3 | ICE/MOB | Yes | |
| R10.0.1.7 | Standard | Yes | |
| R10.0.1.7 | ICE/MOB | Yes | |
| R10.0.2.4 | Standard | Yes | Firmware upgrade from 10.0.1.0, 10.0.1.1, 10.0.1.3 (SP1), and 10.0.1.7 (SP1.5) to R10.0.2.4 is supported. Firmware upgrade from R10.0.0.31 to R10.0.2.4 is implemented through an automatic two step upgrade process and therefore can take longer (approx. nine minutes). |
| R10.0.2.4 | ICE/MOB | Yes | Firmware upgrade from 10.0.1.0, 10.0.1.1, 10.0.1.3 (SP1), and 10.0.1.7 (SP1.5) to R10.0.2.4 is supported. Firmware upgrade from R10.0.0.31 to R10.0.2.4 is implemented through an automatic two step upgrade process and therefore can take longer (approx. nine minutes). |

A.2 iCLASS SE reader upgrade

A.2.1 iCLASS SE Bluetooth & OSDP upgrade kits

iCLASS SE Bluetooth & OSDP upgrade kits allow iCLASS SE/multiCLASS SE Rev E readers, that do not already have Bluetooth/OSDP capability, to be upgraded to support these technologies.

If your iCLASS SE/multiCLASS SE, Rev E reader does not already have Bluetooth/OSDP capability you will need to upgrade the reader using one of the following upgrade kits. Depending on the reader model the following upgrade kits are available:

| Upgrade kit part number | Description | Reader model |
|-------------------------|--|--------------|
| BLEOSDP-UPG-A-900 | iCLASS SE Bluetooth & OSDP upgrade kit | R10/RP10 |
| BLEOSDP-UPG-A-910 | iCLASS SE Bluetooth & OSDP upgrade kit | R15/RP15 |
| BLEOSDP-UPG-A-920 | iCLASS SE Bluetooth & OSDP upgrade kit | R40/RP40 |
| BLEOSDP-UPG-A-921 | iCLASS SE Bluetooth & OSDP upgrade kit | RK40/RPK40 |

Note: The above iCLASS SE Bluetooth & OSDP upgrade kits can only be used for upgrading iCLASS SE/multiCLASS SE Rev E readers.

A.2.2 iCLASS SE/multiCLASS SE Bluetooth & OSDP upgrade kit instructions

1. Disconnect power to the reader.
2. Remove the reader from the reader backplate.
3. On the back of the reader remove the electrical tape covering the module expansion slot.
Note: If the reader has a module already installed, remove this as it will be replaced with the module from the iCLASS SE Bluetooth & OSDP upgrade kit.



Electrical tape



Installed module

4. Insert the upgrade module into the expansion slot. Take care not to touch the expansion slot with anything apart from the module as this could remove the colorless anti-corrosive compound.

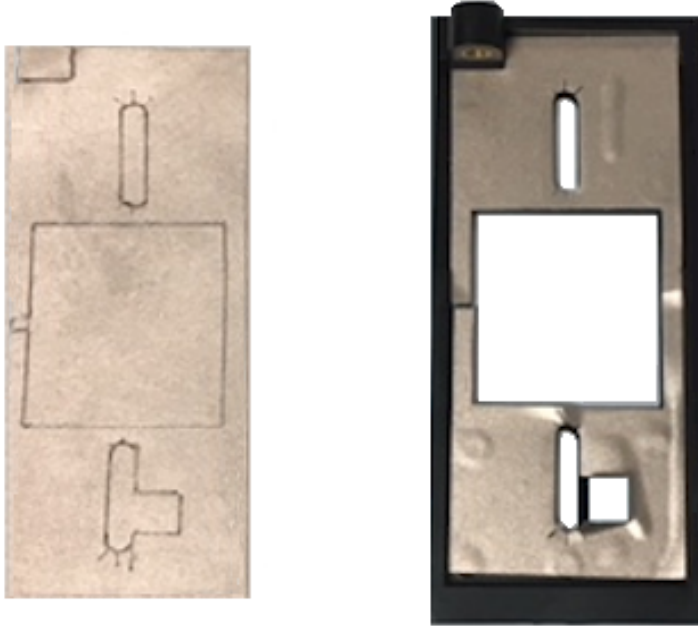


Expansion slot



Module from upgrade kit

5. Remove the reader backplate from the wall.
6. With paper backing still intact, align the metallic sticker from the upgrade kit with the reader backplate to ensure correct orientation.
7. Remove paper backing from metallic sticker and carefully adhere the sticker to the inside of the reader backplane.
Note: The metallic sticker has cutouts to allow reader wiring to remain intact during installation.



8. Re-install the reader backplate to the wall.
9. Re-install the reader onto the reader backplate. Ensure the reader wiring is correct, refer to the reader installation guide.
Note: Different conductors are used for Wiegand vs OSDP communication.

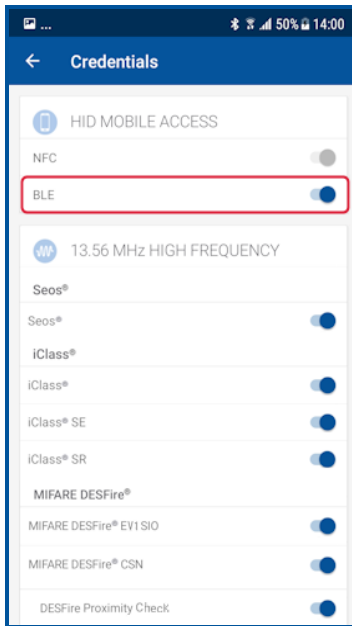
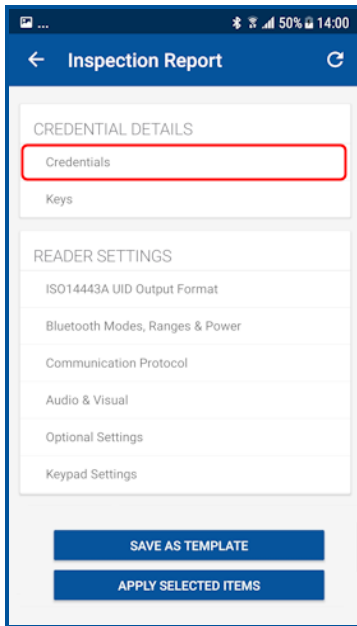
A.2.3 Configure reader in HID Reader Manager

If the reader is ready to be configured, use the following procedure to configure the reader to support Bluetooth for HID Mobile Access and/or OSDP controller communication.

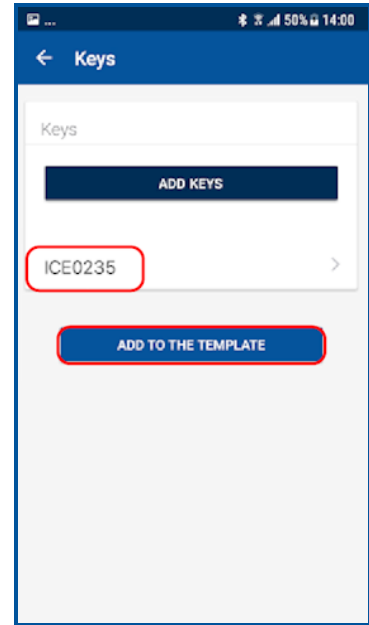
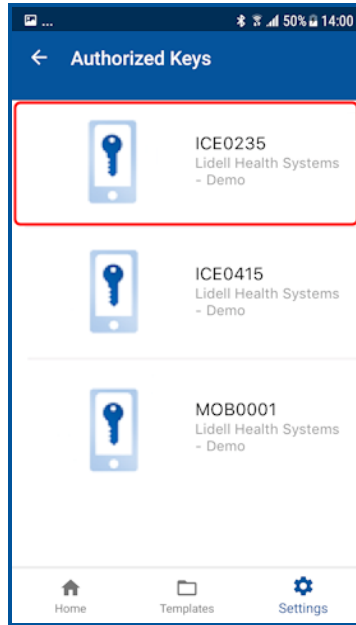
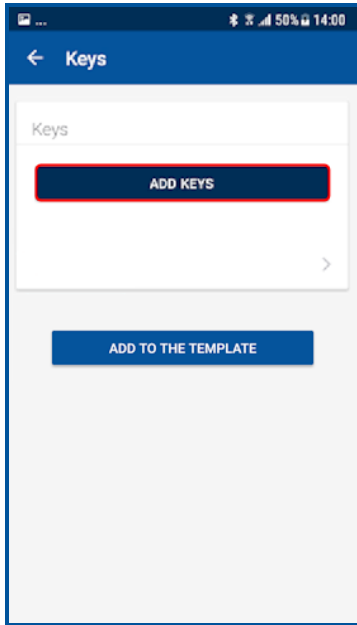
Note: This procedure assumes the Reader Technician has setup the HID Reader Manager app on a mobile device and the Reader Manager Administrator has enrolled the Reader Technician and issued key authorization in the HID Reader Manager Service. See [2.2 Mobile application setup overview](#).

1. Log into the HID Reader Manager app.
2. Connect the HID Reader Manager app to the reader. See [2.4.3 Connect to a reader](#).
3. In the HID Reader Manager app inspect the reader configuration and, if indicated, upgrade the reader firmware. See [2.4.4 Reader inspection report](#).
4. To configure the reader to support Bluetooth for HID Mobile Access and/or OSDP controller communication, on the **Inspection Report** screen tap **Detailed Configuration**.
5. In the **CREDENTIAL DETAILS** section, tap **Credentials**.
6. In the **HID MOBILE ACCESS** section, enable the **BLE** option.

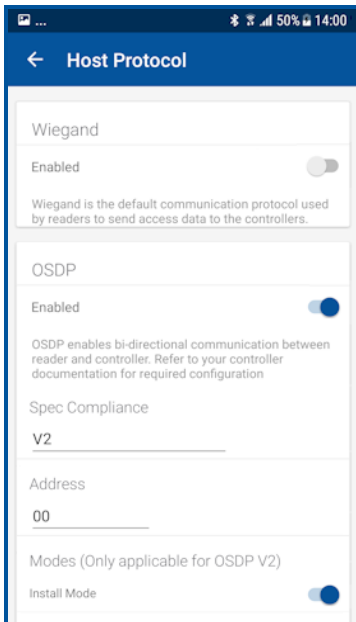
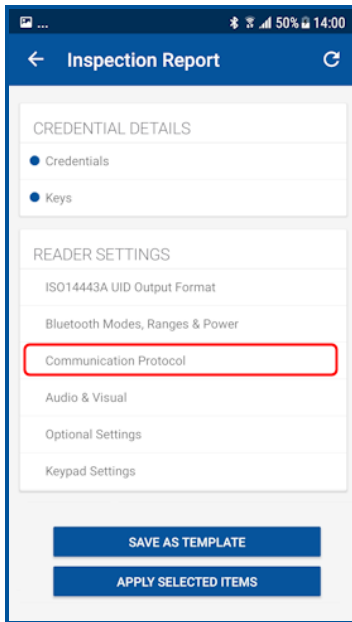
iCLASS SE / multiCLASS SE



7. Back on the **Inspection Report** screen, in the **CREDENTIAL DETAILS** section, tap **Keys**.
8. Tap **ADD KEYS** and select the authorization key to be loaded onto the reader (only one key can be loaded). The selected authorization key will be displayed on the screen.
9. Tap **ADD TO THE TEMPLATE** to save.

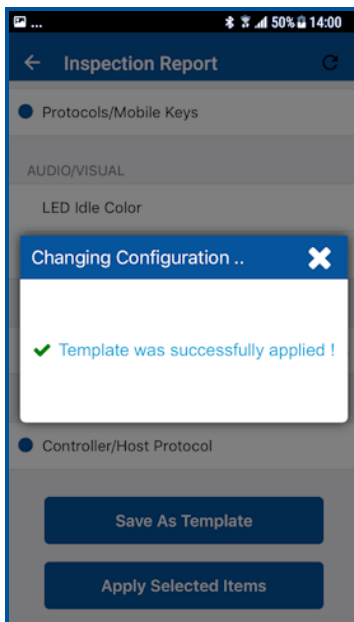
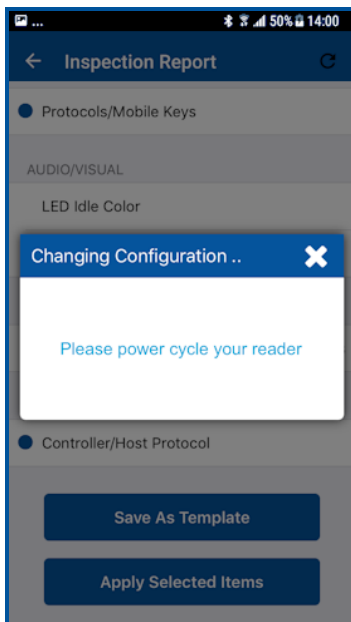
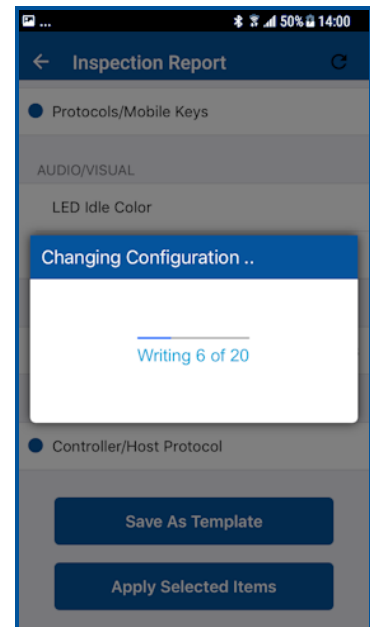
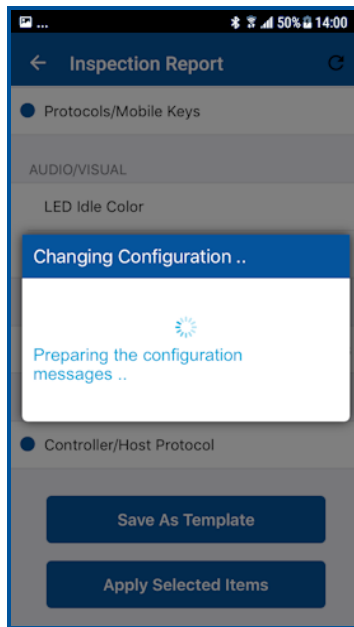
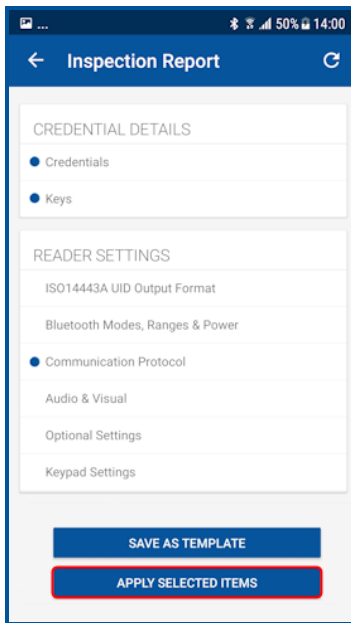


10. To configure the reader for OSDP controller communication (optional), in the **READER SETTINGS** section, tap **Communication Protocol**.
11. Enable the **OSDP** option and tap **ADD TO THE TEMPLATE** to save.



- On the **Inspection Report** screen, tap **APPLY SELECTED ITEMS**. The selected configuration settings are applied to the reader.

Note: If the reader is a Standard enabled reader you will be prompted to power cycle the reader. For ICE/MOB enabled readers no reader power cycle is required.



- Test configuration changes, see [2.3.1 Test configuration changes](#).

Appendix **B**

Identify HID reader models

B.1 Physically inspect reader

The following provides a number of ways you can identify the reader product model through physical inspection of the reader:

1. Check the size of the reader to identify the reader model. HID® Signo™ readers, iCLASS SE®, and multiCLASS SE® readers are available in different form factors for various installation environments. For reader specifications refer to: <https://www.hidglobal.com/products/readers>.
2. Check the reader front product labeling:
 - HID Signo readers have grayscale HID labels.
 - HID Signo Express readers have a blue HID label.
 - iCLASS SE Express R10 readers have a blue HID label.
 - iCLASS/multiCLASS readers have a blue HID label with “iCLASS SE” or “multiCLASS SE”.

HID Signo R20



HID Signo Express



iCLASS SE Express R10



iCLASS/multiCLASS SE R10



B.2 Check the product labeling

B.2.1 HID Signo readers

The HID Signo reader model and part number is printed on the product labeling, for example:

40TKS-00-000000 (HID Signo 40, terminal strip)

For detailed information on HID Signo reader order part numbers refer to the *HID Readers and Credentials How to Order Guide* (PLT-02630) or the *HID Signo™ Express How to Oder Guide* (PLT-06063).

The product label is located on:

- The original box packaging in which the reader was supplied.



- The back of the reader.
Note: If the reader is already installed, the reader will have to be removed from it's housing to access the product label.



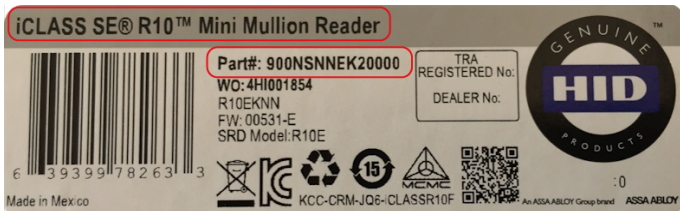
B.2.2 iCLASS SE readers

The HID reader model and part number is printed on the product labeling. iCLASS SE part numbers start with a three-digit number containing the number nine (9xx), for example: **900NSNNEK20000**

For detailed information on iCLASS SE reader order part numbers refer to the *HID Readers and Credentials How to Order Guide* (PLT-02630).

The product label is located on:

- The original box packaging in which the reader was supplied.



- The back of the reader.
Note: If the reader is already installed, the reader will have to be removed from it's housing to access the product label.



B.2.3 Mobile-Capable readers

iCLASS SE (R10, R15, R40, and RK40) readers and multiCLASS SE (RP10, RP15, RP40, and RPK40) readers, Revision E or newer. You can identify this version of reader via the part number, either on POs, invoices or the reader label on inside of the reader. Part numbers that have an **A** as the eighth digit are the iCLASS SE Rev D readers, whereas part numbers that have an **E** as the eighth digit are the iCLASS SE Rev E readers.

- **Rev D Example:** 900NTNNAK00000 (not Mobile-Capable)
- **Rev E Example:** 900NTNNEK00000

B.2.4 Mobile-Enabled and Mobile-Ready readers

Mobile-Enabled and Mobile-Ready readers with BLE will have a part number that contains the letter **M** as the fifth character location, for example:

- 920**P**MNNEKMA010
- 920**P**MNNEKEA003

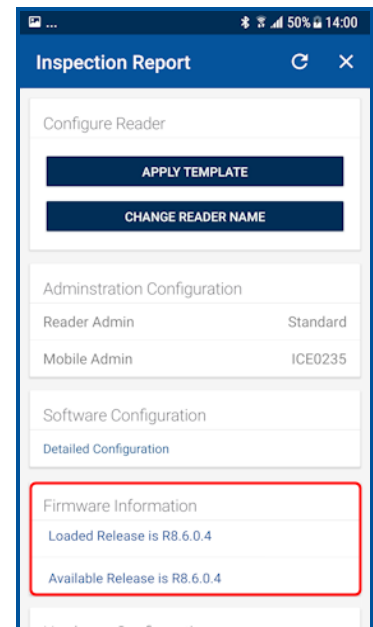
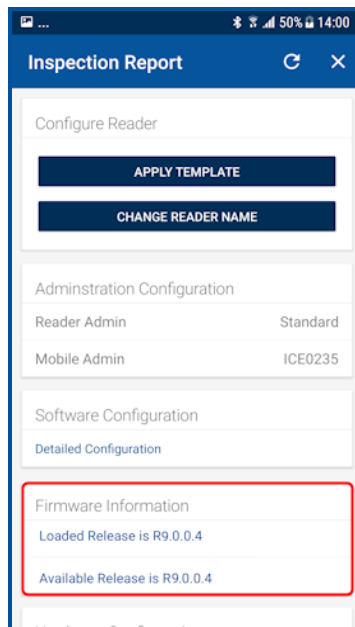
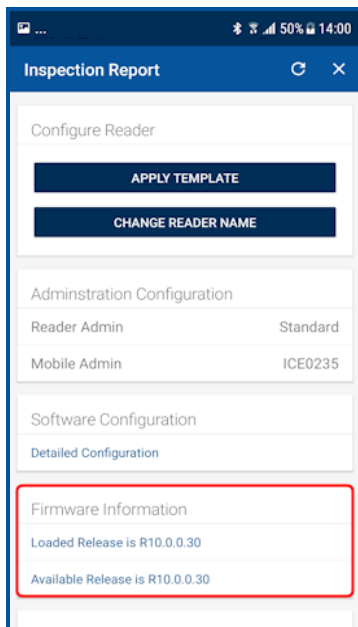
B.3 Check the reader firmware version with Reader Manager

1. Connect the Reader Manager app to a reader and inspect the reader configuration, see [2.4.3 Connect to a reader](#).
2. In the **FIRMWARE INFORMATION** section check the displayed **Loaded Release** version number:
 - If the **Loaded Release** version number is **10.x.x.x**, then the reader is HID® Signo™ reader.
 - If the **Loaded Release** version number is **9.x.x.x**, then the reader is an iCLASS SE® Express R10 connected reader.
 - If the **Loaded Release** version number is **8.x.x.x**, then the reader is an iCLASS/multiCLASS SE® Rev E R10 connected reader.

HID Signo

iCLASS SE Express R10

iCLASS/multiCLASS SE Rev E R10



Appendix **C**

Glossary

C.1 Glossary

| Term | Description |
|-----------------------------|---|
| BLE | Bluetooth Low Energy (formerly marketed as Bluetooth Smart) is a wireless personal area network technology. |
| Credential Container | A mobile device which holds a credential. |
| End customer | The Organization that uses HID products and services. |
| Invitation code | Invitation codes are issued to users as the first step in registering a new device. Invitation codes consist of a 16 character alphanumeric sequence and are used to authenticate devices and associate them with the relevant user. |
| MA | HID Mobile Access®. Mobile access is the use of a mobile device, such as a smartphone, tablet or wearable, to gain access to secured doors, gates, networks, services and more. |
| MFA | Multi-Factor Authentication. A security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login or other transaction. |
| Mobile credential/Mobile ID | Virtual credentials that are stored on a mobile device. Mobile IDs are issued and/or revoked via the HID Mobile Access portal. Mobile IDs are unique to each device and cannot be copied. If a user switches devices, a new Mobile ID must be issued. |
| Mobile-enabled readers | Mobile-enabled readers are fully activated and personalized to support an organization's specific Mobile ID's. These readers can only be ordered after the organization has completed registration for HID Mobile Access or HID Elite program. MOB or ICE Mobile Keyset will be required at time of order. |
| Mobile-ready readers | Mobile-ready readers are prepared to support HID Mobile Access but lack the personalized configuration (Mobile Keyset) to read an organization's specific Mobile ID's. These readers can be ordered at any time but will require field activation after the organization has completed registration for HID Mobile Access. To support a specific organization's Mobile IDs, these readers need to be personalized (Mobile Keyset loaded) using the HID Reader Manager App or a Mobile Key Card. |
| Mobile Keyset (MOB or ICE) | Mobile Keyset is a reference number for a set of cryptographic keys loaded into a reader. Mobile IDs, Mobile Key cards, and Mobile Admin cards will securely authenticate only with readers programmed with a matching keyset. An organization is assigned a Mobile Keyset upon registration into either the HID Elite™ (ICE) or HID Mobile Access (MOB) programs. The correct Mobile Keyset must be supplied when ordering mobile-enabled readers, Mobile IDs, Mobile Key cards, and Mobile Admin cards. |
| Opening modes | The following opening modes can be enabled/disabled using the HID Reader Manager App. When approaching a reader these interactions can be performed with a mobile device for access: <ul style="list-style-type: none"> ■ Tap (including Enhanced Tap): The mobile device is brought very close to, or touching, the reader (a similar user experience to using a physical credential). ■ Twist and Go: The mobile device holder initiates access by twisting the mobile device in a sharp 90 degree rotation in either direction (a similar motion to using a physical door handle). Typically used when the mobile device is at a longer distance from the reader. ■ App Specific: This entrance opening mode is specific to an application, for example, widget opening from a wearable such as a smartwatch. |

| Term | Description |
|------------------------------|--|
| Organization Administrator | User with sufficient privileges to add new Reader Manager Administrator users. |
| Organization ID | Organization ID is a reference number for a unique account within the Mobile Access Portal. It is assigned at the conclusion of account registration. The correct Organization ID must be supplied when ordering Mobile IDs and Mobile Admin cards. |
| OSDP | Open Supervised Device Protocol (OSDP) is an access control communications standard developed by the Security Industry Association (SIA) to improve interoperability among access control and security products. |
| Reader Manager Administrator | User with full access to all HID Reader Manager Service functionality, including enrolling Reader Technicians, issuing invitation codes and authorization keys. |
| Reader Technician | The person that performs reader upgrades and reader configuration changes using the HID® Reader Manager™ app. |

Revision history

| Date | Description | Revision |
|----------------|---|----------|
| July 2021 | <ul style="list-style-type: none"> ■ Section 1.1 and B.1. Updated sections to state HID Reader Manager support for HID Signo Express readers. ■ Section 2.4.1 (Credential details). Updated section to state the credential profiles that are available for HID Signo Express readers. ■ Section 2.4.1 (ISO14443A UID Output Format settings). Updated section for the ability to enable/disable the Raw Data option and the 64-Bit LSB format option. ■ Section 2.4.4 Reader Inspection report. Updated section and screenshots for the ability to identify the Reader Model for Signo readers. | A.9 |
| May 2021 | <ul style="list-style-type: none"> ■ Section 2.4.1 (Credential details). Updated section for the capability to enable/disable DESFire EV3 credential read and Proximity Check. ■ Appendix A.1.3. HID Signo readers table. Added entries for R10.0.2.4 firmware support. | A.8 |
| May 2021 | <ul style="list-style-type: none"> ■ Section 2.4.1 (Create a new template). User note added related to template creation. ■ Appendix A.1.1. HID SE readers table. Added entries for R8.9.1.4 firmware support. | A.7 |
| September 2020 | <ul style="list-style-type: none"> ■ Section 2.2.8. Added NFC Options section. ■ Section 2.4.1 (Wallet Settings). Updated section for optimized Wallet setting configuration in Reader Manager 1.6.0. ■ Section 2.4.4. Updated Reader Inspection Report section. ■ Section 2.4.5. Updated Firmware Upgrade section for the re-install firmware function. ■ Section 3. Removed sections relating to the Legacy SIS Portal. ■ Appendix A.1.1. Table comments updated for the Reader Manager 1.6.0 two step FW upgrade path to 8.9.1.3. ■ Appendix B.2. Updated section for HID Signo reader product labeling. | A.6 |
| September 2020 | <ul style="list-style-type: none"> ■ Section 2.3.1. Updated the Credential settings sub-section for the ability to enable/disable an Indala Proximity credential and the display of credential profile information for HID Signo readers. ■ Section 2.3.1. Updated the Bluetooth Modes, Ranges & Power settings sub-section to add default range values. ■ Section 2.3.1. Updated the Communication Protocol settings sub-section for the ability to change/configure OSDP baud rate for both HID iCLASS SE and HID Signo readers. ■ Section 2.3.1. Updated the Keypad settings sub-section for setting the keypad backlight color for HID Signo readers. ■ Appendix A.1. Updated section to list reader firmware versions that can be upgraded. | A.5 |
| May 2020 | Updates throughout document for HID Reader Manager 1.4.0. | A.4 |
| September 2019 | Updated the following sections for the functionality to enable/disable High Frequency and Low Frequency credentials for iCLASS SE readers: <ul style="list-style-type: none"> ■ Section 2.3.1.1 Credential and Keys settings. ■ Section 2.3.6 View detailed reader configuration. ■ Appendix A - Configure reader in HID Reader Manager. | A.3 |

| Date | Description | Revision |
|----------------|--|----------|
| July 2019 | <ul style="list-style-type: none"> ■ Section 2.3.1 Create a new template. Updated section for the select reader option and select charging profile option for iCLASS SE Express. ■ Section 2.3.6 View detailed reader configuration. Updated section for enable/disable Mifare & Desfire UID and Priority options for iCLASS SE Express. ■ Section A.2.2.1 Configure reader in HID Reader Manager. Updated section for enable/disable Mifare & Desfire UID and Priority options for iCLASS SE Express. ■ Section 2.3.5 Update reader firmware and Section 2.3.7 Apply configuration changes. Added note relating to “SNMP Authentication Failed” message. ■ Section 4.1.1 Error and warning messages. Updated Error and warning message table for “SNMP Authentication Failed” message. | A.2 |
| January 2019 | Updates implemented for Reader Manager 1.1.0 and for the iCLASS SE Express R10: <ul style="list-style-type: none"> ■ Section 2.3 Basic app functionality. Updated sections for new and changed template configuration settings. ■ Section 3.5.2 Enroll Reader Manager Admin (HID Origo Management Portal) ■ Appendix A - Configure reader in HID Reader Manager. Updated section for new settings. ■ Appendix B - Identify HID reader models. New section. | A.1 |
| September 2018 | Initial release. | A.0 |



Powering Trusted Identities

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

Support: +1 866-607-7339

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

Support: +852-3160-9833

Europe, Middle East & Africa
3 Cae Gwyrdd
Green Meadow Springs
Cardiff, CF15 7AB
United Kingdom

Support: +44 (0) 1440 711 822

Brazil
Condomínio Business Center
Av. Ermanno Marchetti, 1435
Galpão A2 - CEP 05038-001
Lapa - São Paulo / SP, Brazil
Phone: +55 11 5514-7100

PLT-03858, A.9