

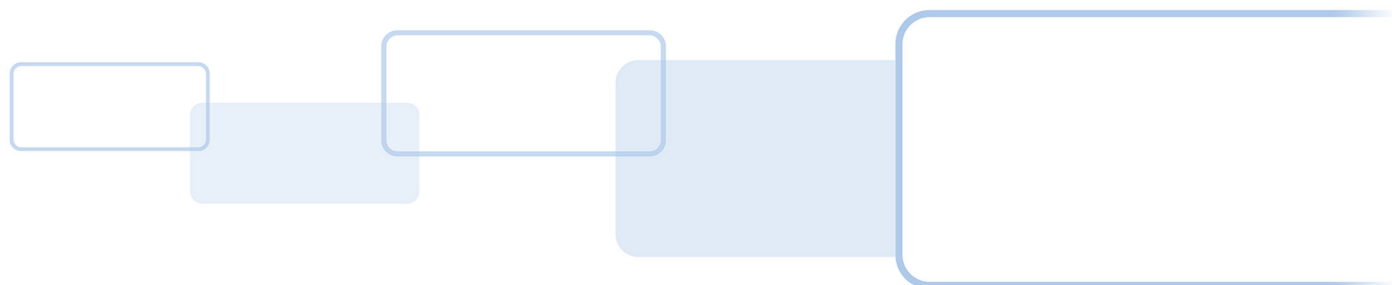


# **HID<sup>®</sup> READER MANAGER<sup>™</sup> SOLUTION**

## **USER GUIDE (ANDROID)**

PLT-03858, Rev. A.0

September 2018



## Copyright

© 2018 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, 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.

## Revision history

Date	Description	Revision
September 2018	Initial release.	A.0

## Contacts

For additional offices around the world, see [www.hidglobal.com/contact/corporate-offices](http://www.hidglobal.com/contact/corporate-offices)

### Americas and Corporate

611 Center Ridge Drive  
Austin, TX 78753  
USA  
Phone: 866 607 7339  
Fax: 949 732 2120

### Asia Pacific

19/F 625 King's Road  
North Point, Island East  
Hong Kong  
Phone: 852 3160 9833  
Fax: 852 3160 4809

### Europe, Middle East and Africa (EMEA)

Haverhill Business Park Phoenix Road  
Haverhill, Suffolk CB9 7AE  
England  
Phone: 44 (0) 1440 711 822  
Fax: 44 (0) 1440 714 840

### Brazil

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

**HID Global Technical Support:** [www.hidglobal.com/support](http://www.hidglobal.com/support)



# Contents

<b>Section 1: Introduction</b>	<b>7</b>
1.1 Document purpose	7
1.2 Intended audience	7
1.3 HID Reader Manager solution overview	8
1.3.1 Key authorization	9
1.4 Reader and Mobile device compatibility	9
1.4.1 Readers	9
1.4.2 Mobile devices	9
1.5 Related Products and Services	10
1.5.1 HID Mobile Access solution overview	10
<b>Section 2: HID Reader Manager mobile application</b>	<b>11</b>
2.1 Mobile application setup	11
2.1.1 HID Reader Manager app setup prerequisites	11
2.1.2 Setup process overview	11
2.1.3 Download and install the Reader Manager app	12
2.1.4 Register a new Reader Technician within the app	13
2.1.5 Log into the HID Reader Manager app	15
2.1.6 Activate invitation code in the HID Reader Manager app	16
2.1.7 Display authorized keys	18
2.1.8 HID Reader Manager app settings	19
2.1.8.1 About HID Reader Manager	19
2.1.8.2 MY ACCOUNT	20
2.1.8.3 Administration keys	20
2.2 Reader configuration	21
2.2.1 Test configuration changes	21
2.3 Basic app functionality	22
2.3.1 Create a new template	22
2.3.1.1 Credential settings	23
2.3.1.2 Audio/Visual settings	24
2.3.1.3 BLE settings	25
2.3.1.4 Controller Communication settings	26

2.3.2 Manage templates. . . . .	27
2.3.2.1 Save a new template. . . . .	27
2.3.2.2 Share a template. . . . .	28
2.3.2.3 Display template details. . . . .	29
2.3.2.4 Delete a template. . . . .	30
2.3.3 Connect to a reader. . . . .	31
2.3.4 Reader inspection report. . . . .	33
2.3.5 Update reader firmware. . . . .	34
2.3.6 View detailed reader configuration. . . . .	35
2.3.7 Apply configuration changes. . . . .	37
2.3.8 Change reader name. . . . .	38
<b>Section 3: HID Reader Manager Portal. . . . .</b>	<b>39</b>
3.1 Portal setup overview. . . . .	39
3.2 Access the HID Reader Manager Portal. . . . .	40
3.3 Enroll a Reader Technician. . . . .	43
3.3.1 Edit Reader Technician information. . . . .	46
3.3.2 Delete an enrolled Reader Technician. . . . .	47
3.4 Issue authorization keys. . . . .	49
3.4.1 Edit authorization key information. . . . .	52
3.4.2 Revoke (delete) key authorization. . . . .	53
3.5 Configure HID Reader Manager Portal settings. . . . .	56
3.5.1 Export Reader Technician Record settings. . . . .	57
3.5.2 Invitation Email settings. . . . .	57
3.5.3 Configure Delete Threshold. . . . .	58
3.6 Enroll additional Reader Manager Admin. . . . .	59
<b>Section 4: Troubleshooting. . . . .</b>	<b>65</b>
4.1 Reader Manager app messages. . . . .	65
4.1.1 Error messages. . . . .	65
4.1.2 Warning messages. . . . .	66
4.1.3 Warning messages. . . . .	67
4.1.4 Information messages. . . . .	67
4.1.5 Validation messages. . . . .	68
4.2 Contact HID Technical Support. . . . .	68
<b>Appendix A: Reader upgrade. . . . .</b>	<b>69</b>
A.1 iCLASS SE and multiCLASS SE Bluetooth and OSDP Upgrade Kit. . . . .	69
A.1.1 Verify reader compatibility. . . . .	69

A.1.2 iCLASS SE and multiCLASS SE Upgrade Kits . . . . .	69
A.1.3 iCLASS SE and multiCLASS SE Bluetooth and OSDP Upgrade Kit instructions . . .	70
A.1.3.1 Configure reader in HID Reader Manager. . . . .	72
<b>Appendix B: Release notes. . . . .</b>	<b>75</b>
B.1 HID Reader Manager release feature summary . . . . .	75
B.1.1 HID Reader Manager app 1.0 release items. . . . .	75
B.1.2 HID Reader Manager Portal release items . . . . .	75
B.2 HID Reader Manager release limitations summary . . . . .	76
B.2.1 HID Reader Manager app 1.0. . . . .	76
B.2.2 HID Reader Manager Portal 5.1.0. . . . .	77

This page is intentionally left blank.



# Section 1

## 1 Introduction

---

### 1.1 Document purpose

This document provides an overview of the HID® Reader Manager™ solution and provides information and procedures for HID 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 in the HID Reader Manager Portal
- Change reader configurations for supported iCLASS SE®/multiCLASS SE® readers
- Update reader firmware for supported iCLASS SE/multiCLASS SE readers
- Upgrade supported 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 Portal 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 Reader Manager app
  - Self-registration within the Reader Manager app
  - Linking the Reader Manager app to the Reader Manager Portal via an issued invitation code
  - Performing reader configuration changes and firmware upgrades
  - Reader configuration update testing

### 1.3 HID Reader Manager solution overview

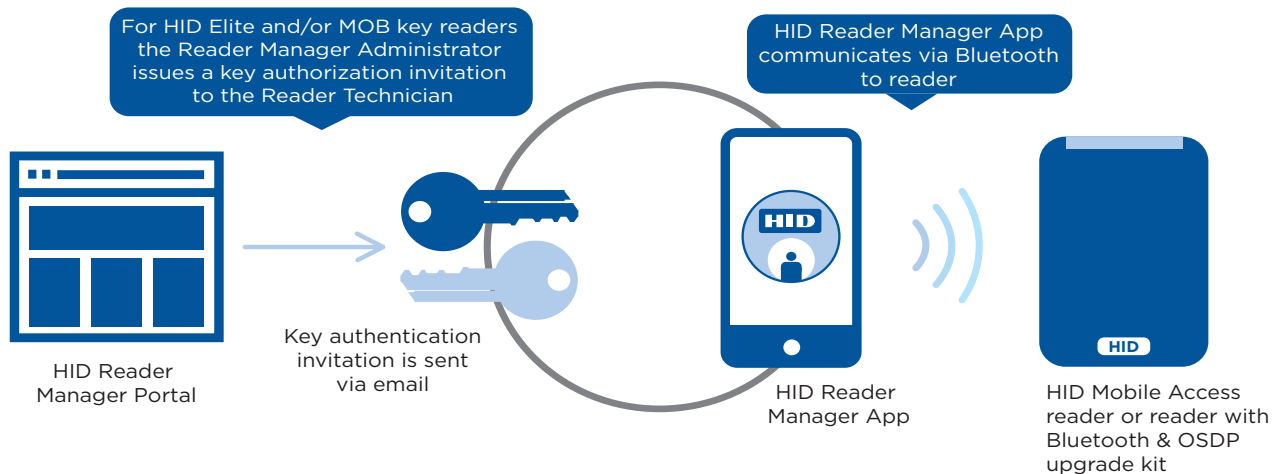
The HID Reader Manager solution streamlines management of BLE capable readers in the field. Administrators can easily adjust certain configuration settings (for example audio/visual settings, read range settings), upgrade firmware, inspect connected reader status and extend functionality on supported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

The main components of the HID Reader Manager solution are:

- **HID Reader Manager Mobile Application:** Mobile app which connects, via Bluetooth, to a reader for configuration changes, firmware upgrades and reader inspections by Reader Technicians.
- **HID Reader Manager Portal:** Web Portal which facilitates Reader Technicians to use the HID Reader Manager Mobile Application with readers that have HID Elite™ and/or MOB keys. The portal 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 Mobile Application can be used with Standard Key readers for OSDP field upgrade or audio/visual setting configuration. However the Reader Manager Portal 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 Mobile Application to upgrade readers to support Bluetooth and/or Open Supervised Device Protocol (OSDP). This module can also be temporarily connected to readers without Bluetooth that do not permanently require Bluetooth support. This enables HID Reader Manager App support for the reader while the plug-in module is connected. For more information, see *Appendix A - Reader upgrade*.



### 1.3.1 Key authorization

HID Reader Manager uses key authorization to:

- Securely connect and control access by the mobile app to iCLASS SE and 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 iCLASS SE and multiCLASS SE, Rev E readers. 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”, with the list of compatible readers at:

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

For details on supported firmware versions, see *Appendix B - HID Reader Manager app 1.0*.

### 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>

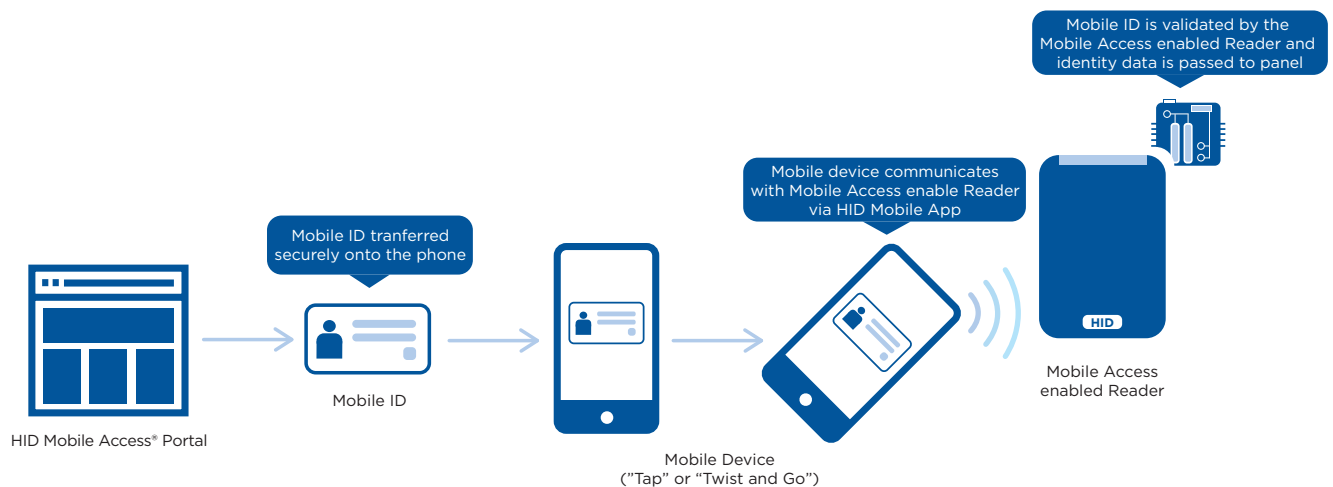
## 1.5 Related Products and Services

### 1.5.1 HID Mobile Access solution overview

HID Mobile Access complements an existing access control solution. As an alternative to using cards or fobs, the HID Mobile Access service enables company personnel to securely access locations using their Android and iOS mobile devices. To support HID Mobile Access the HID Reader Manger Solution allows supported iCLASS SE and multiCLASS SE readers to be upgraded in the field.

HID Mobile Access is powered by Seos® and consists of the following components:

- **HID Mobile Access Portal:** The management portal that allows administrators to manage users and securely issue or revoke Mobile IDs to user mobile devices
- **HID Mobile Access Application:** The app for Android and iOS devices
- **Mobile IDs:** The Mobile IDs with integrated Seos technology for management of trusted identities
- **Mobile Access enabled readers:** iCLASS SE or multiCLASS SE readers



For more detailed information on the HID Mobile Access solution, refer to [HID Mobile Access Solutions](#).



# Section 2

## 2 HID Reader Manager mobile application

---

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.

### 2.1 Mobile application setup

#### 2.1.1 HID Reader Manager app setup prerequisites

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

- A HID Mobile Access® Portal instance has been setup for the Organization.
- A HID Reader Manager Portal instance has been setup for the Organization. See *HID Mobile Access Portal – HID Reader Manager Portal Change Form* located at:  
<https://www.hidglobal.com/documents>
- A Reader Manager Administrator has been setup and enabled within the Organizations Reader Manager Portal instance.

#### 2.1.2 Setup process overview

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

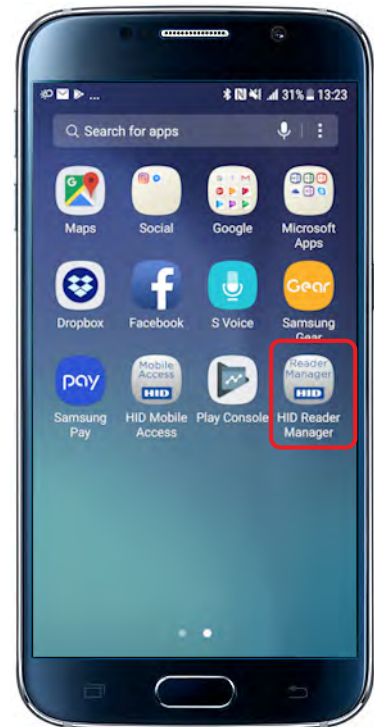
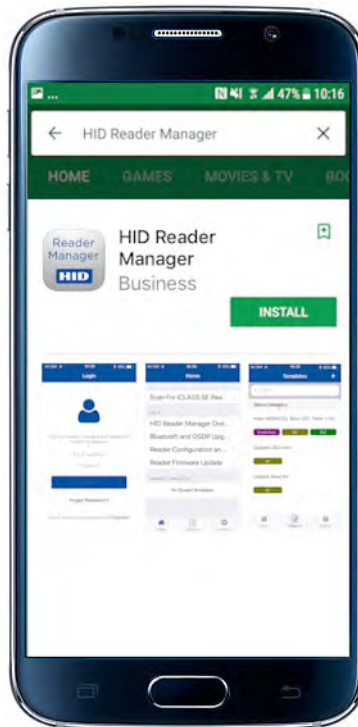
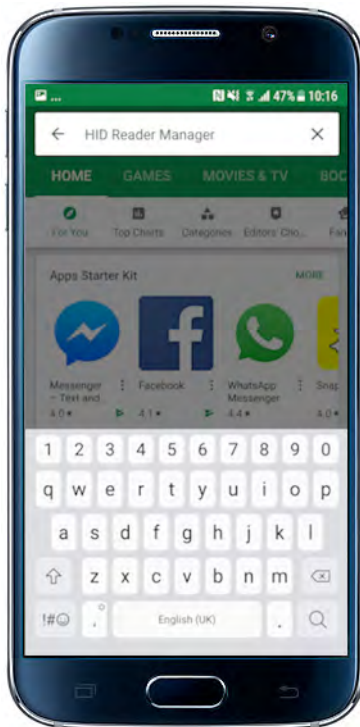
1. The Reader Technician downloads and installs the HID Reader Manager app on a mobile device. See *Section 2.1.3 Download and install the Reader Manager app*.
2. The Reader Technician performs registration with the HID Reader Manager app. See *Section 2.1.4 Register a new Reader Technician within the app*.

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

1. The Reader Manager Administrator enrolls the Reader Technician in the HID Reader Manager Portal and issues an invitation code and key authorization. See *Section 3 HID Reader Manager Portal*.
2. The Reader Technician activates the issued invitation code in the HID Reader Manager app. See *Section 2.1.6 Activate invitation code in the HID Reader Manager app*.
3. The Reader Technician verifies key authorization has been received in the HID Reader Manager app. See *Section 2.1.6 Activate invitation code in the HID Reader Manager app*.

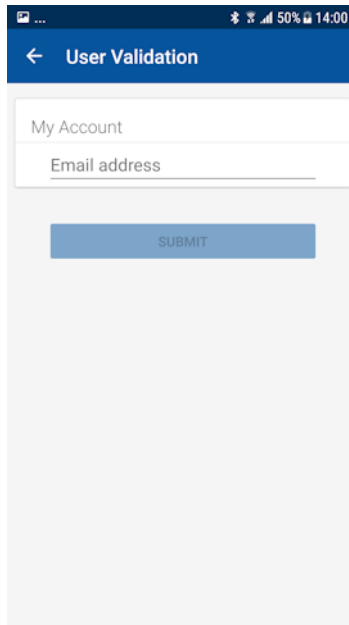
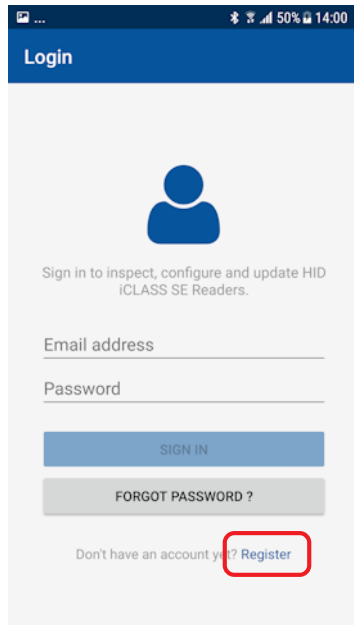
### 2.1.3 Download and install the Reader Manager app

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 Google Play (for Android devices)
3. Search for **HID Reader Manager**
4. Download and install the app on your mobile device.

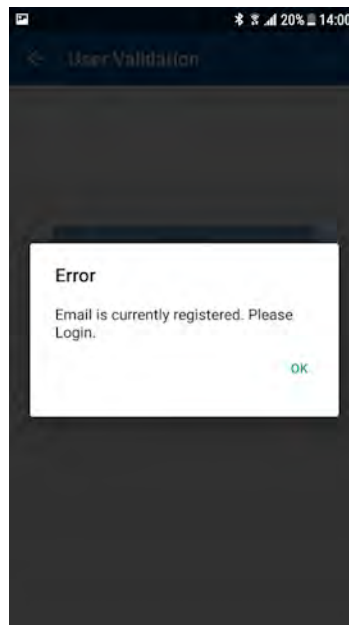
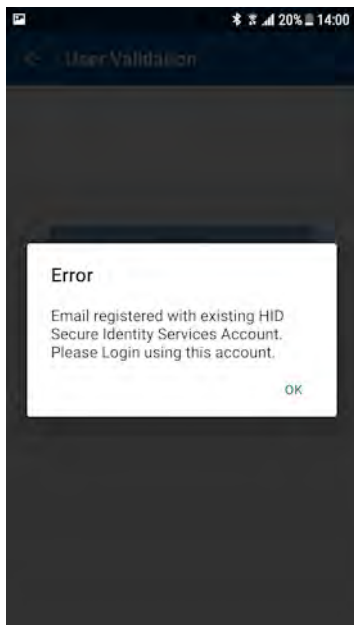


## 2.1.4 Register an account within the app

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**.



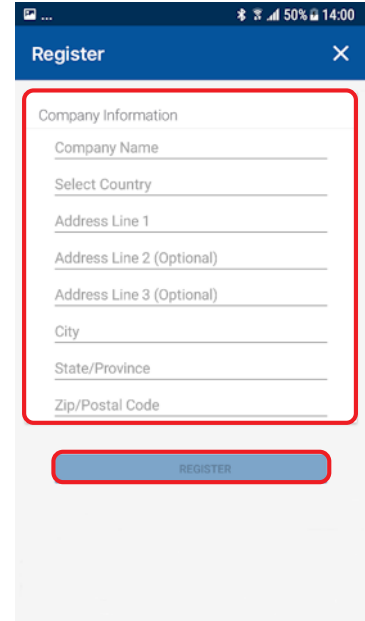
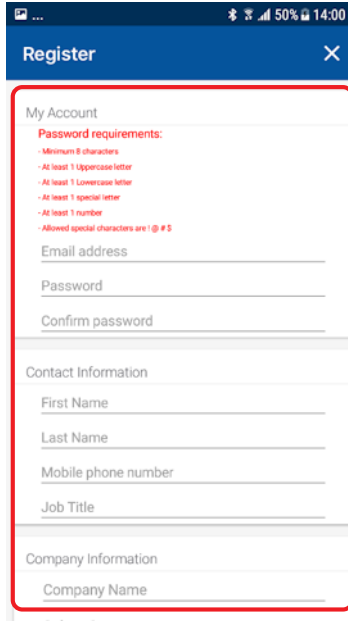
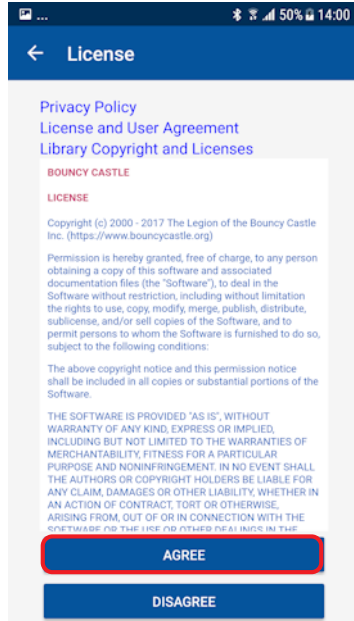
**Note:** If the entered email address is associated with an existing HID Secure Identity Services account or the email address is already registered then the following messages are displayed. Tap **OK** to return the **Login** screen and sign in with your assigned username and password. See *Section 2.1.5 Log into the HID Reader Manager app*



- On the **License** screen, read the privacy policies and license agreements and tap **Agree**.

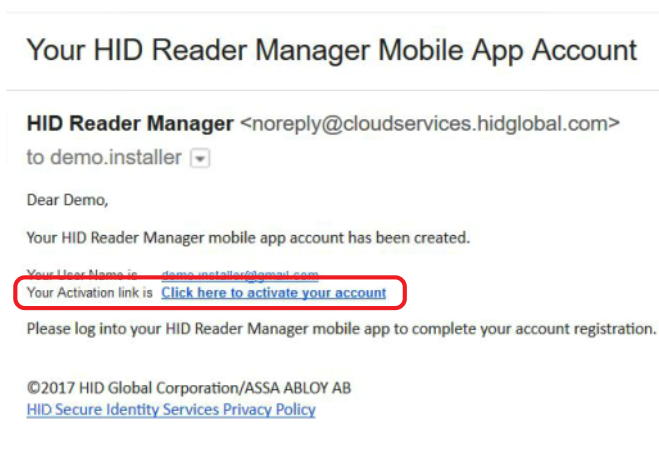
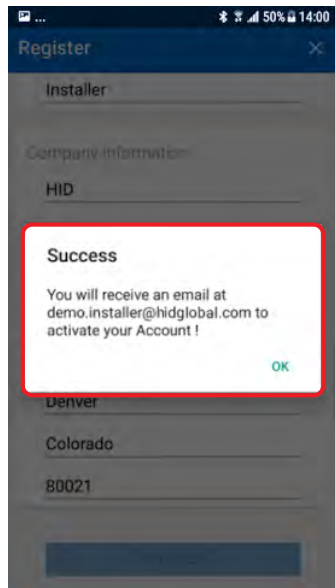
**Note:** Tapping **Disagree** will return you to the **User Validation** screen.

- Enter your registration details (optional fields are indicated) and tap **Register**.



- After receiving a **Success** prompt, tap **OK**.
- Check your registered email account for an email containing an activation link. Click the activation link in the email. A successful activation message will appear in a new browser.

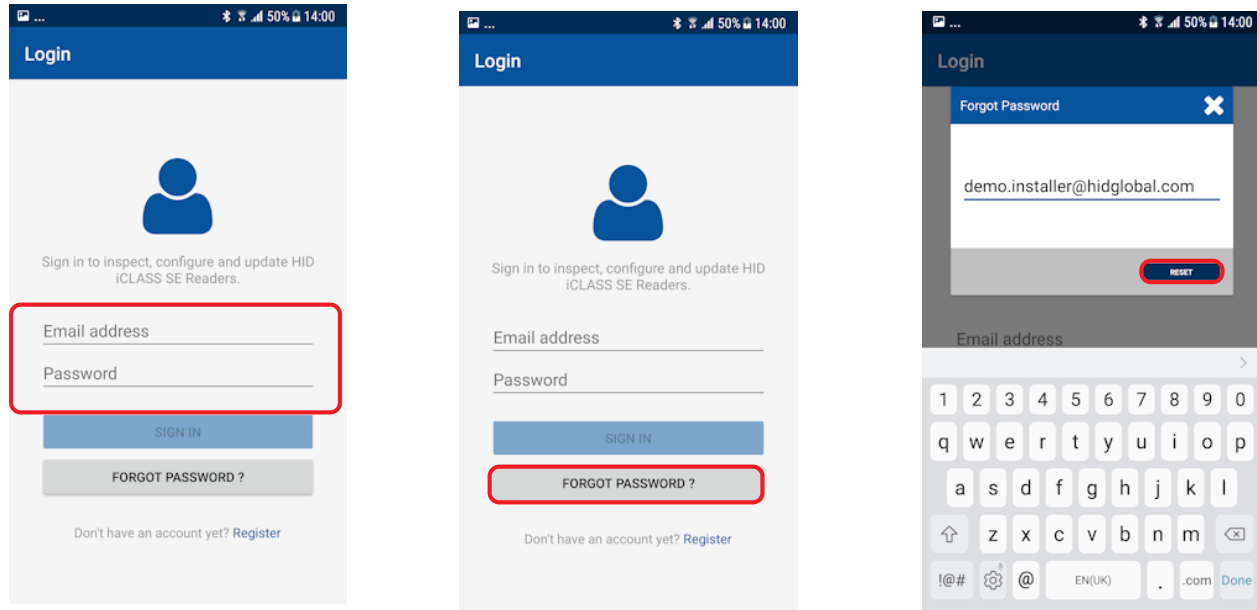
You can now log into the HID Reader Manager app using the registered email address and password.



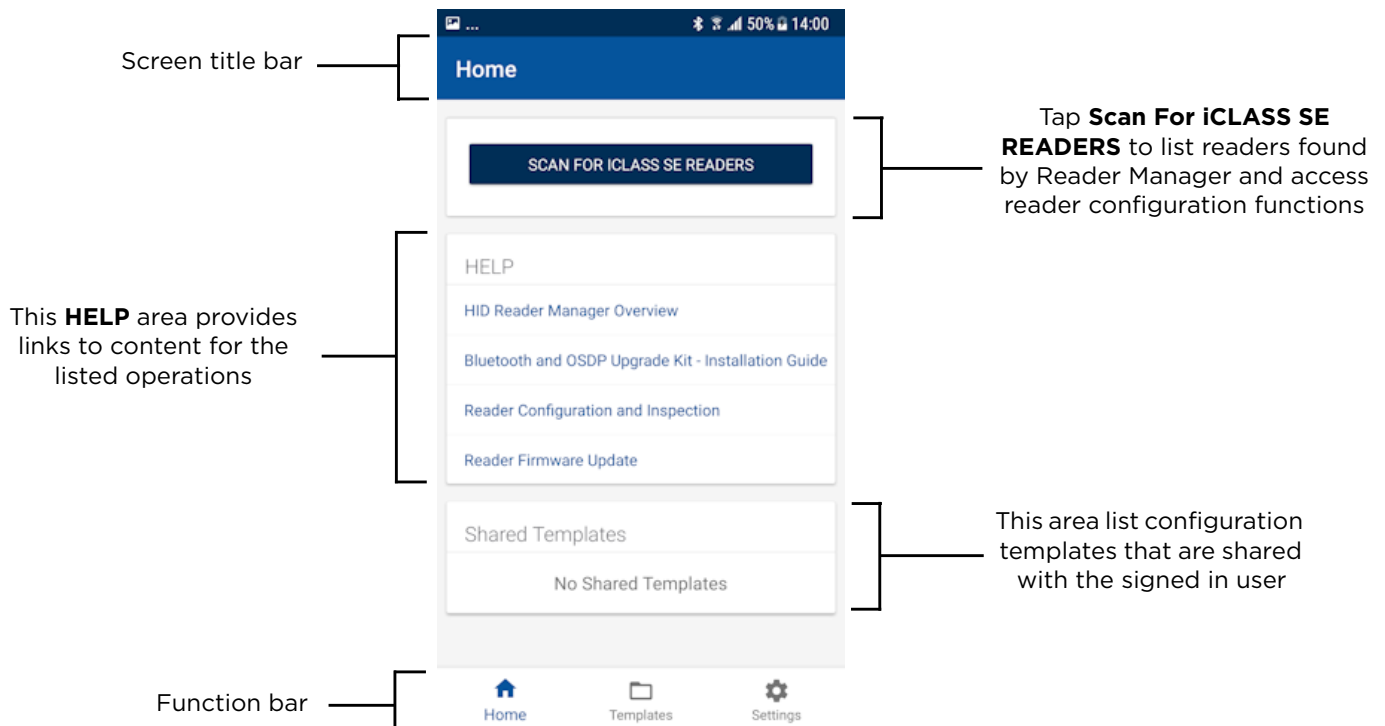
## 2.1.5 Log into the HID Reader Manager app

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.

**Note:** If you have forgotten your login password, tap **Forgot Password?**. Enter your email address and tap **Reset**. Check your registered email account for a password reset email and follow the instructions in the email to reset your password.



Home screen layout:



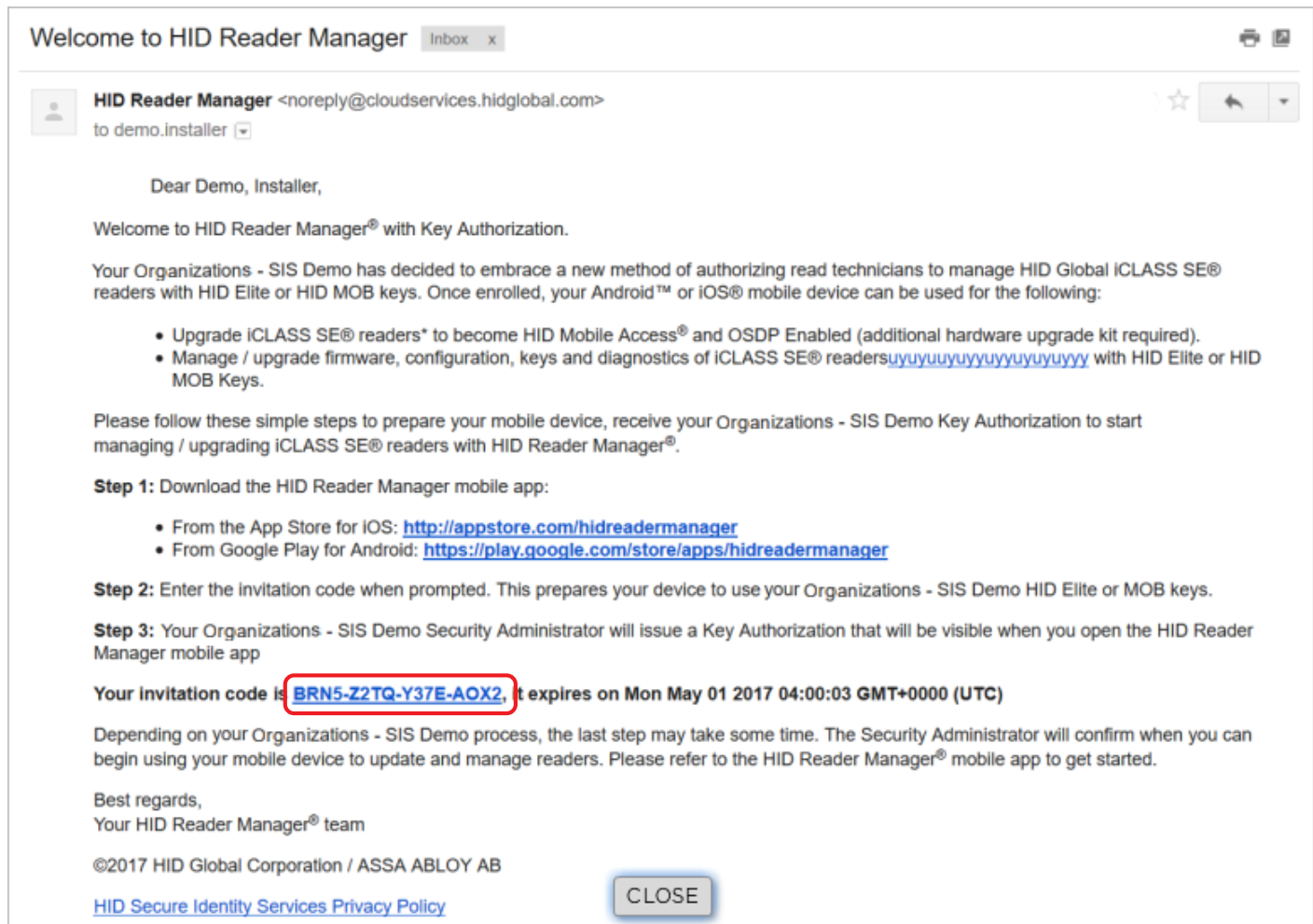
### 2.1.6 Activate invitation code in the HID Reader Manager app

**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 has to enroll the Reader Technician within the HID Reader Manager Portal. See *Section 3.3 Enroll a Reader Technician*.

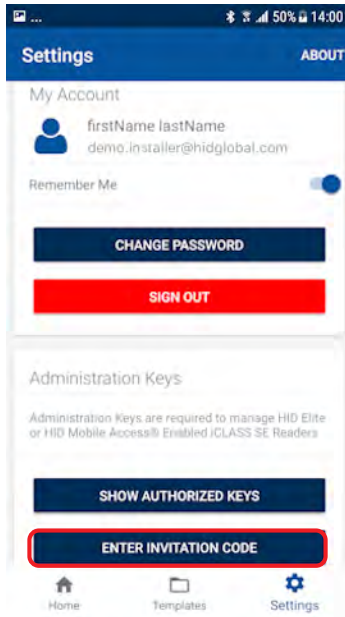
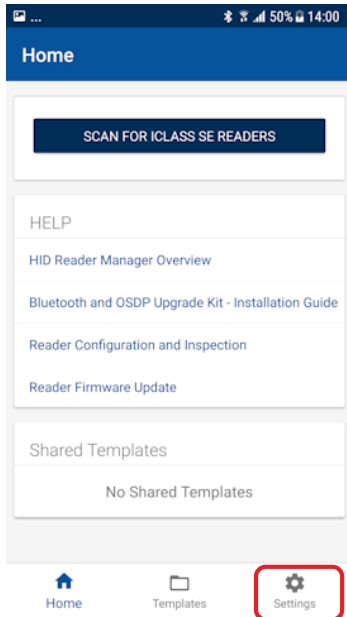
When the Reader Manager Administrator enrolls a Reader Technician within the HID Reader Manager portal an invitation email will be sent to the Technician's registered email address containing an invitation code.

### Sample invitation email



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

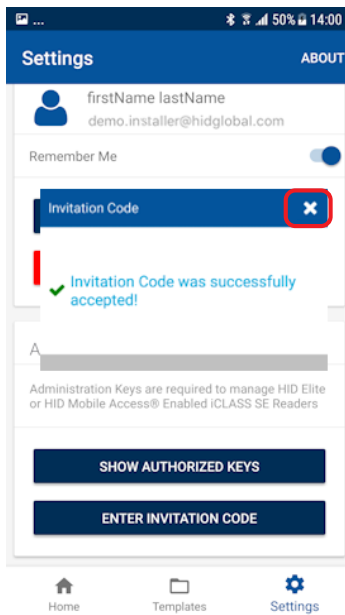
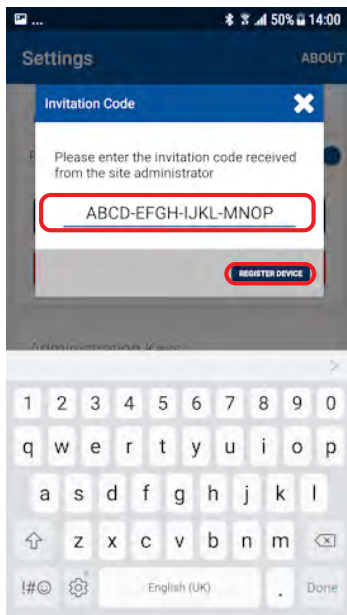
1. Log into the HID Reader Manager app using your registered email and password.
2. Tap the **Settings** icon on the **Home** screen.
3. Tap **ENTER INVITATION CODE**.



4. Enter the invitation code received in the invitation email and click **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.



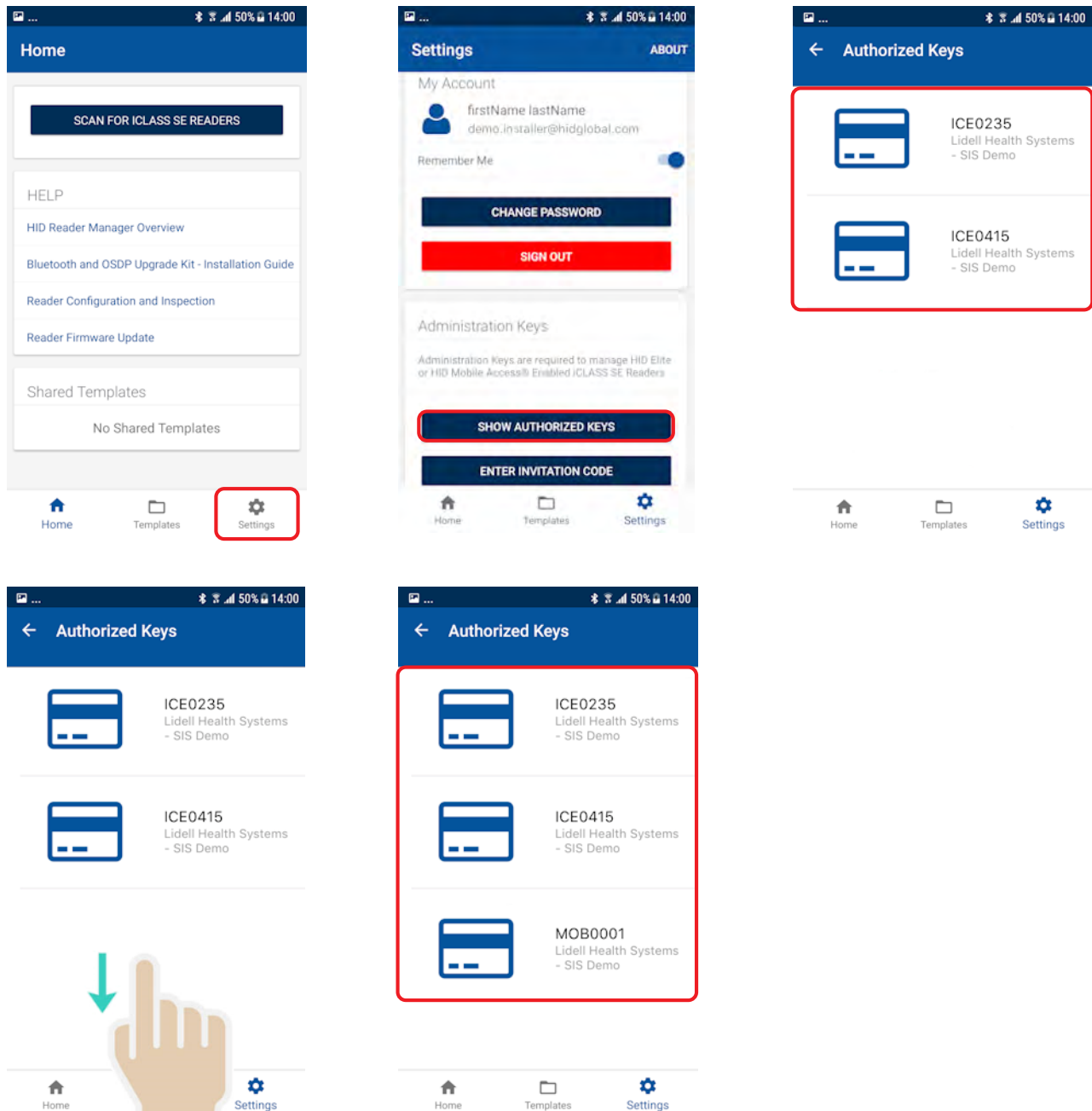
### 2.1.6.1 Display authorized keys

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

Authorization keys issued via the Reader Manager portal can be viewed in the Reader Manager app:

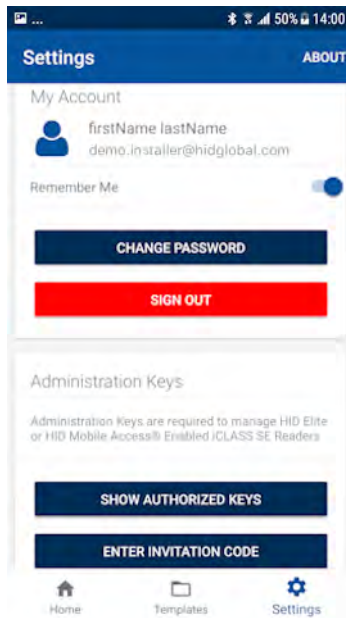
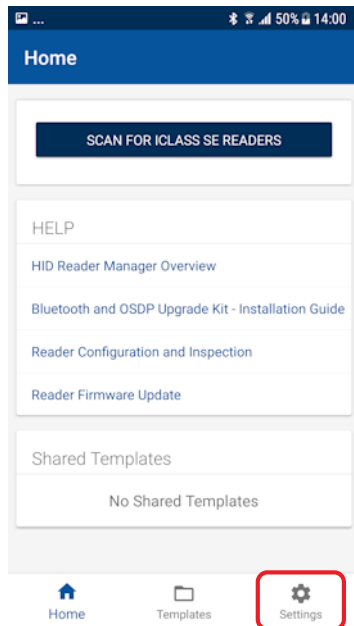
1. Tap the **Settings** icon on the **Home** screen.
2. Tap **Show Authorized Keys**.
3. Verify that issued authorization keys are displayed.

**Note:** If a received issued authorization key is not displayed swipe down to refresh the screen.



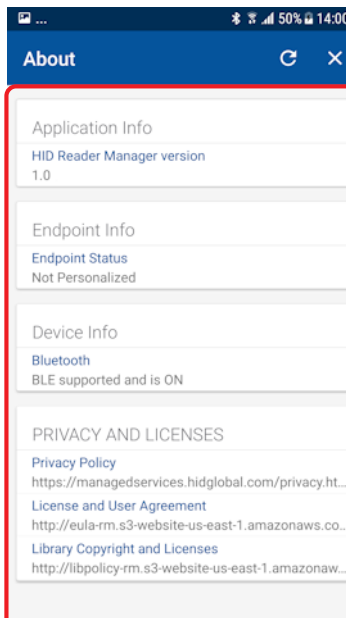
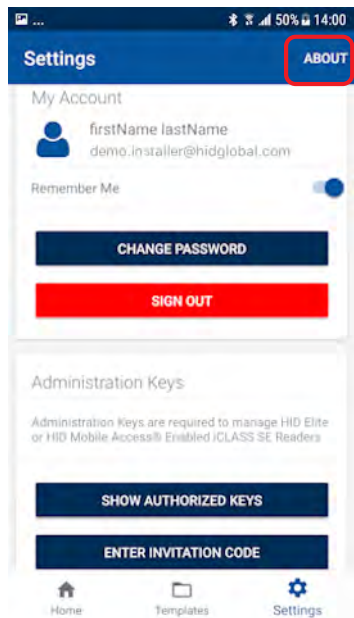
## 2.1.7 HID Reader Manager app settings

Tap the **Settings** icon, on the **Home** screen, to access HID Reader Manager app settings.



### 2.1.7.1 About HID Reader Manager

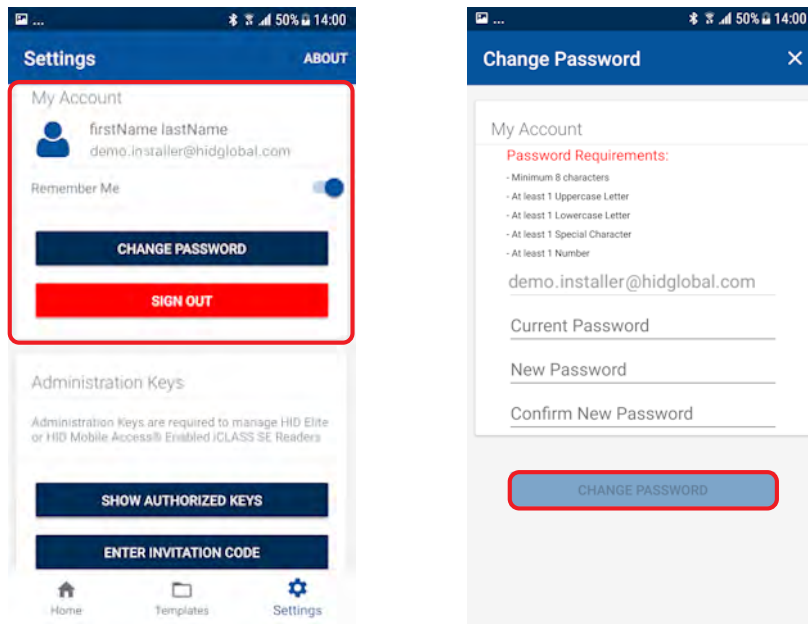
Tap **ABOUT**, on the **Settings** screen, to display Application, Endpoint, and Device information as well as Privacy and License agreements.



### 2.1.7.2 MY ACCOUNT

On the **Settings** screen the **MY ACCOUNT** area displays user account information and provides the following options:

- **Remember Me:** toggle the **Remember Me** option to enable the system to remember your account information.
- **Change Password:** tap **CHANGE PASSWORD** to access the **Change Password** screen. Enter a new login password (refer to the on screen password requirements) and tap **CHANGE PASSWORD**.
- **Sign Out:** tap **SIGN OUT** to exit the app.



### 2.1.7.3 Administration keys

On the **Settings** screen the **Administration Keys** area provides the following functions:

- **SHOW AUTHORIZED KEYS:** displays a list of the issued Authorized Keys.
- **ENTER INVITATION CODE:** allows you to activate the issued invitation code in the HID Reader Manager app.

## 2.2 Reader configuration

The HID Reader Manager solution is only compatible with select iCLASS SE® and multiCLASS SE® reader models. To see the complete list visit:

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

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 *Section 2.3.5 Update reader firmware*.
2. The Reader Technician creates a configuration template to simplify programming the reader. See *Section 2.3.1 Create a new template*.
3. The Reader Technician applies the created configuration template to the reader. See *Section 2.3.7 Apply configuration changes*.

### 2.2.1 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 check valid access is granted and BLE operations perform as configured.
- If you have loaded any HID Elite keys (ICE####), ensure that all physical Elite credentials work at the reader.

## 2.3 Basic app functionality

### 2.3.1 Create a new template

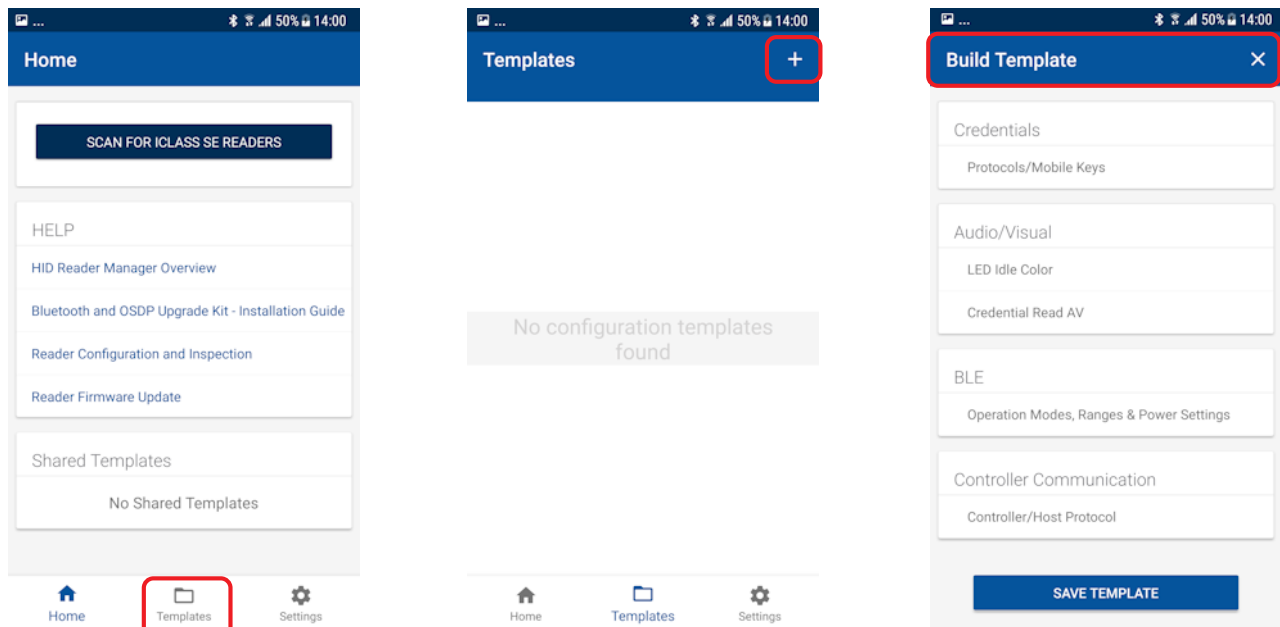
Templates store reader settings. When a template is created it can be applied to multiple readers that require the same configuration or shared with other Technicians to speed up the configuration of multiple readers.

**Note:** Templates only need to include the reader configuration settings that are required to be changed.

To create a new template:

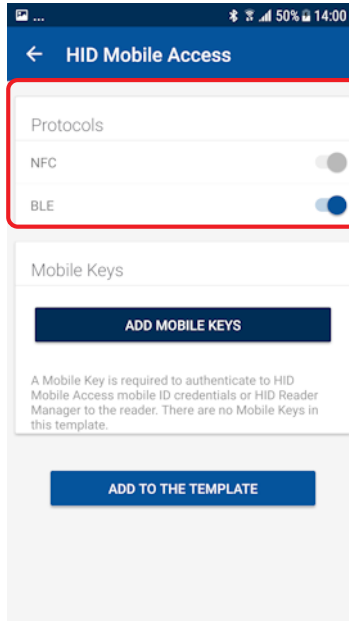
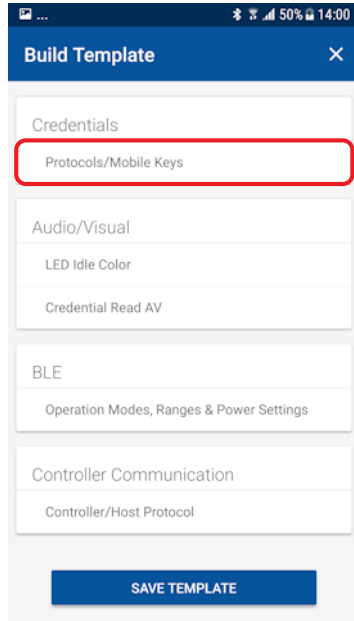
1. Tap the **Templates** icon on the **Home** screen.
2. Tap the plus icon [+] to access the **Build Template** screen.

From the **Build Template** screen you can configure and add settings to a template. These template settings are described in the following sections.

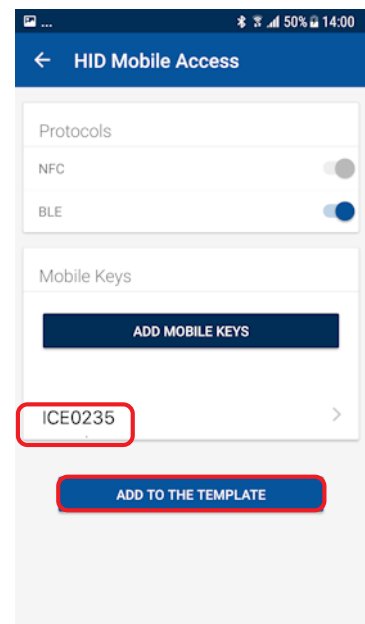
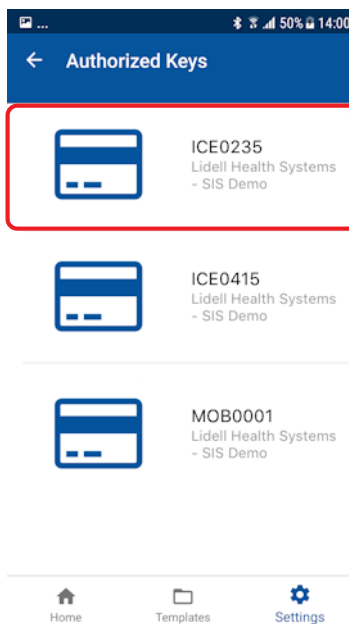
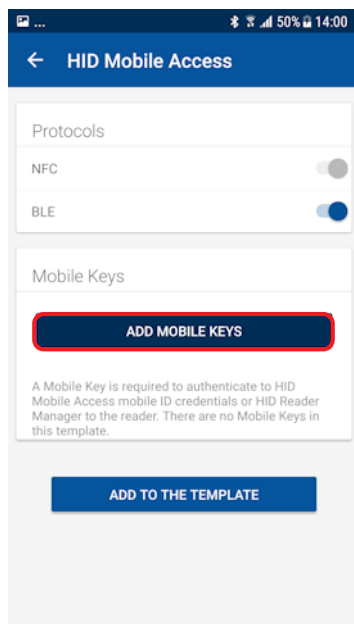


### 2.3.1.1 Credential settings

1. Select **Protocols/Mobile Keys**, from the **Credentials** section.
2. In the **Protocols** section, enable the required credential protocol option.

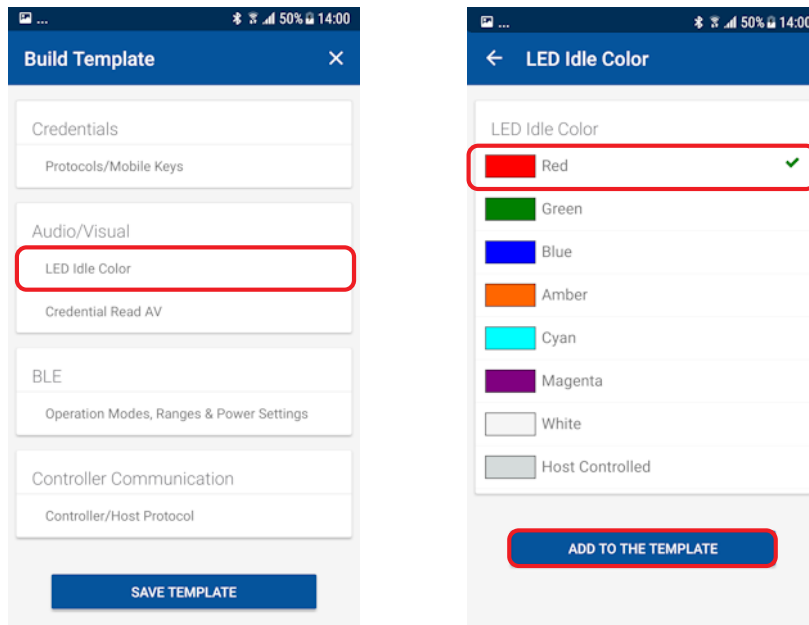


3. Tap **ADD MOBILE KEYS**, in the **Mobile Keys** section, and select the required authorization key to be loaded onto the reader. The selected authorization key will be displayed on the screen.
4. Tap **ADD TO THE TEMPLATE** to save.

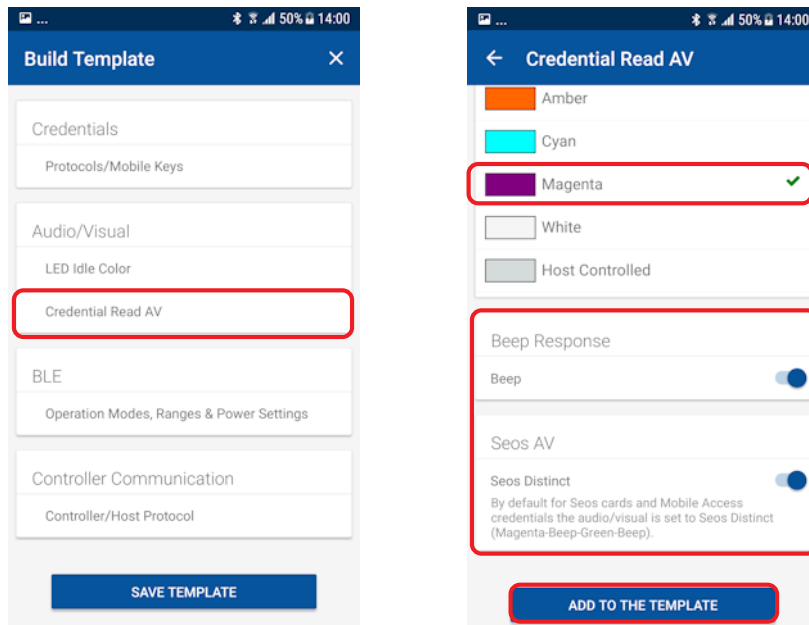


### 2.3.1.2 Audio/Visual settings

1. Select **LED Idle Color** in the **Audio/Visual** section. Select a color and tap **ADD TO THE TEMPLATE**.

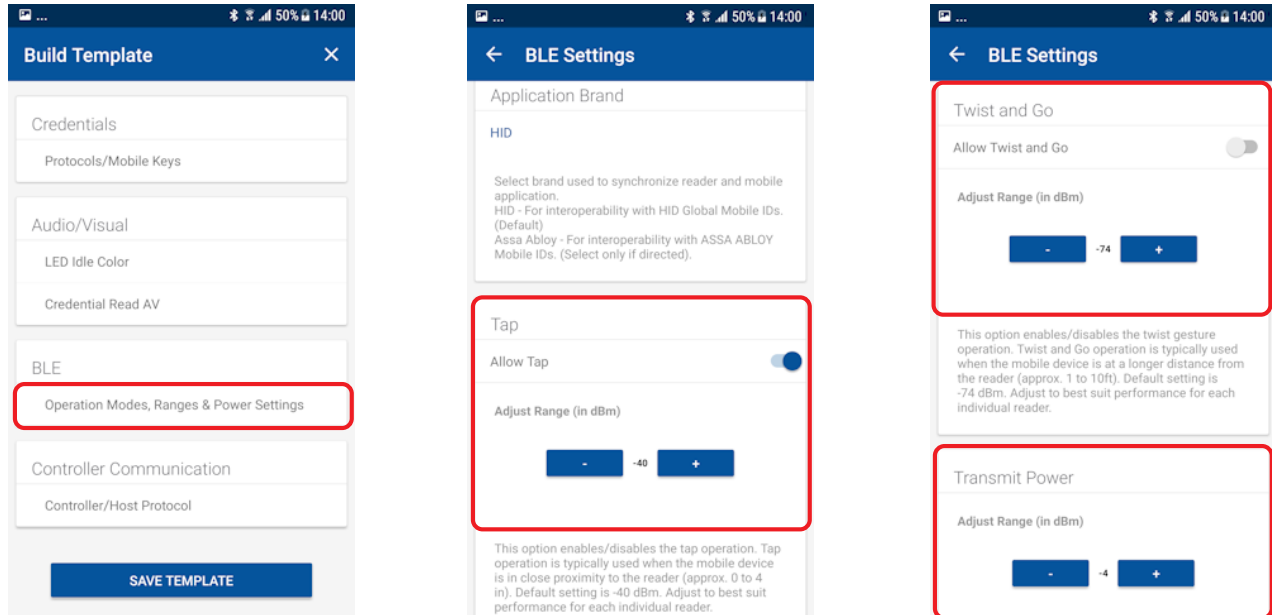


2. Select **Credential Read AV** in the **Audio/Visual** section.
3. Select a color and enable/disable the **Beep Response** and **Seos AV** settings using the options.
4. Tap **ADD TO THE TEMPLATE** to save.



### 2.3.1.3 BLE settings

1. Select **Operation Modes, Ranges & Power Settings** in the **BLE** section.
2. On the **BLE Settings** screen select the required settings for **TAP**, **TWIST AND GO**, and **TRANSMIT POWER**. Tap **ADD TO THE TEMPLATE** to save.



### Recommended Range values

Due to the fact that the range and performance of mobile devices may vary, it is advised that the appropriate settings are selected based on a representative cross-section of mobile device types to be used. For most doors (office environment) the following opening ranges are recommended:

- 15cm to 20cm with **Tap**
- 0.5m to 1m with **Twist and Go**

**Note:** Usually you will want less opening ranges for elevators and other small areas where multiple readers may exist.

Opening ranges will deviate between different mobile devices, therefore you will still want to test and fine tune the settings for a specific site, however the Read Range settings listed below provide a starting point for some common locations:

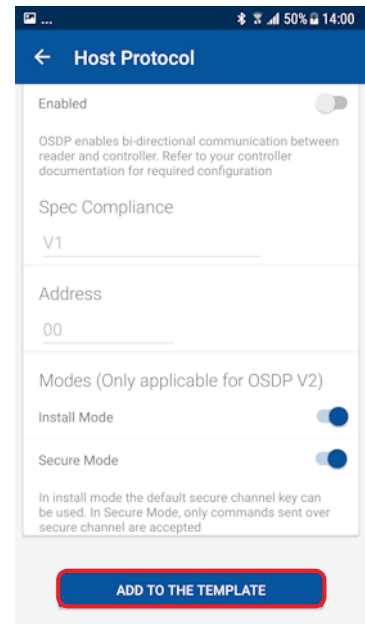
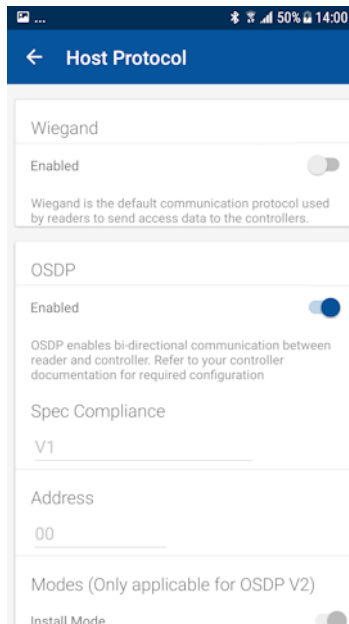
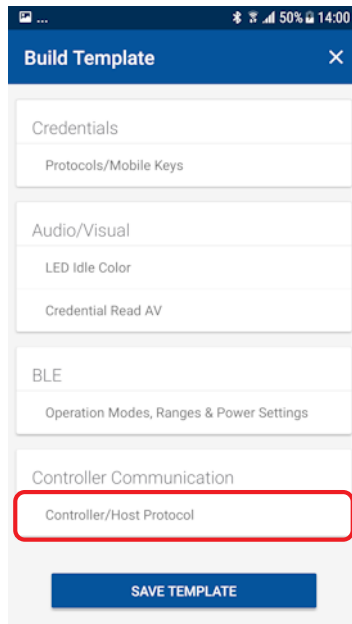
Location	Tap	Twist and Go
Office environment	-48 dBm	-67 dBm
Elevators	-40 dBm	-57 dBm
Outdoor entrances	-48 dBm	-67 dBm
Garage (user inside vehicle)	-53 dBm	-74 dBm

In certain installations a higher or lower **Transmit Power** may be required, however this setting should only be adjusted if the Read Range settings do not result in the desired read range.

**Note:** It is recommended that the default **Transmit Power** setting (-4 dBm) is not exceeded unless absolutely necessary.

### 2.3.1.4 Controller Communication settings

1. Select **Controller/Host Protocol** in the **Controller Communication** section.
2. Enable the required communication protocol. This can be set as **Wiegand** or **OSDP** (not both). Tap **ADD TO THE TEMPLATE** to save.



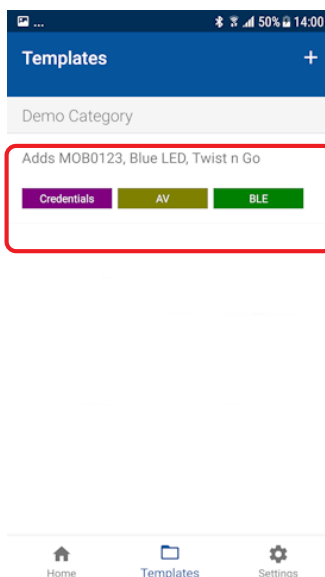
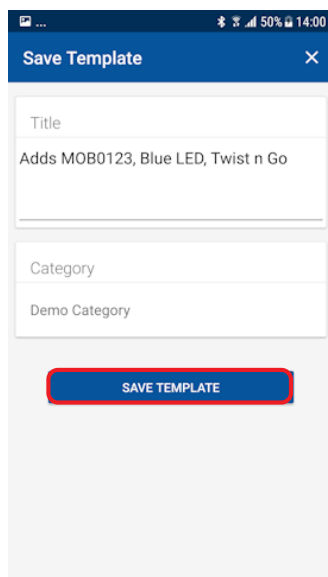
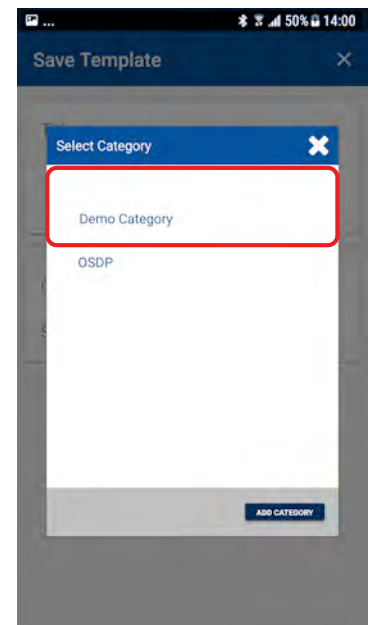
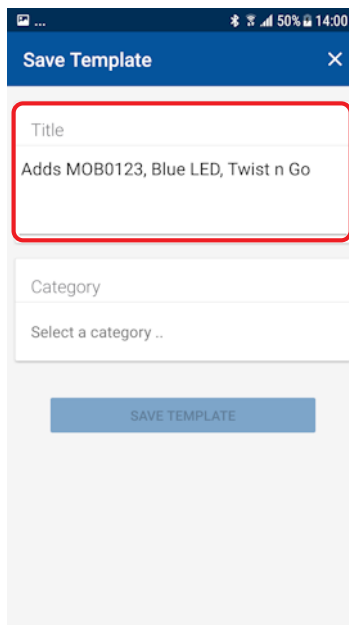
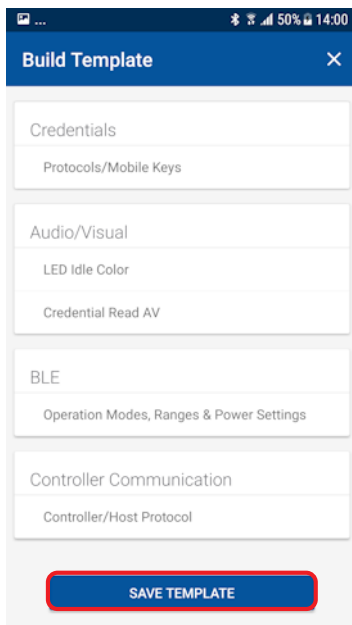
## 2.3.2 Manage templates

### 2.3.2.1 Save a new template

1. When configuration settings have been selected and added to the template, tap **Save Template**.
2. Tap in the **Title** area and enter a title for the template.
3. Tap in the **CATEGORY** area and tap **Select a 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.

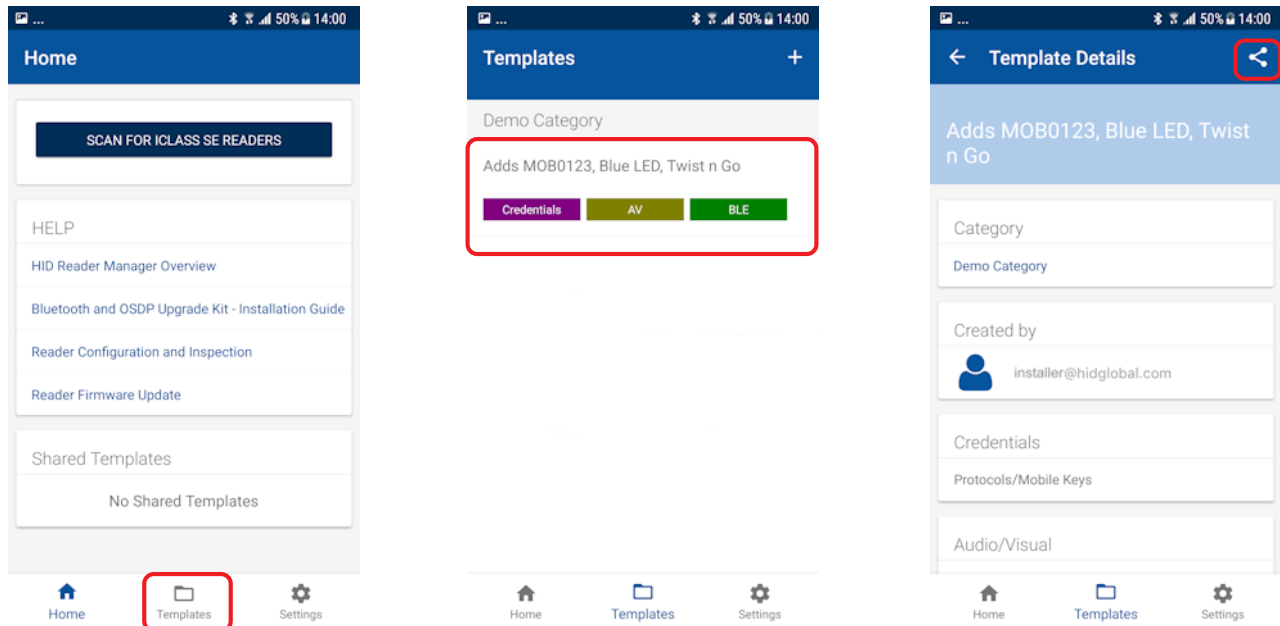
The new template is displayed on the **Templates** screen with indicators for the configuration types within the template



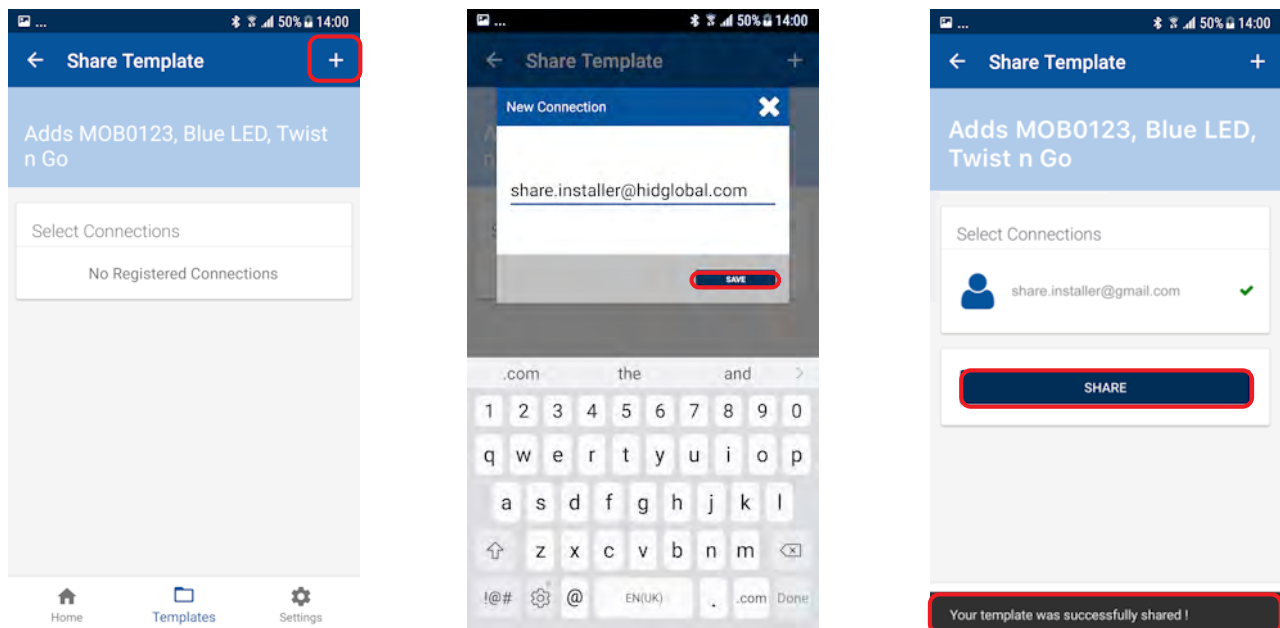
### 2.3.2.2 Share a template

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

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

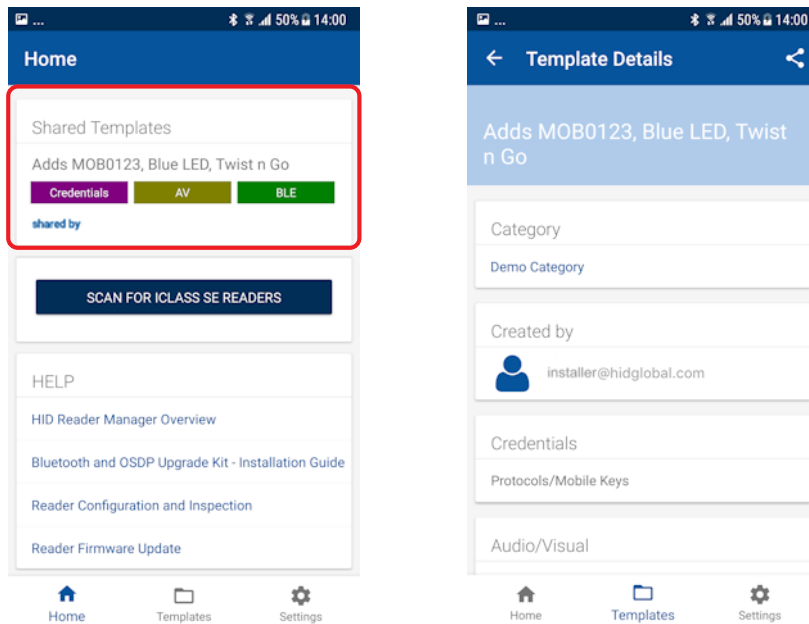


2. Tap the plus icon [⊕] and in the **New Connection** box, enter the email address of another Technician (this can be any Technician that is already registered). Tap **SAVE**.
3. When the connection has been made, tap **SHARE**. A message will appear at the bottom of the screen to indicate success.

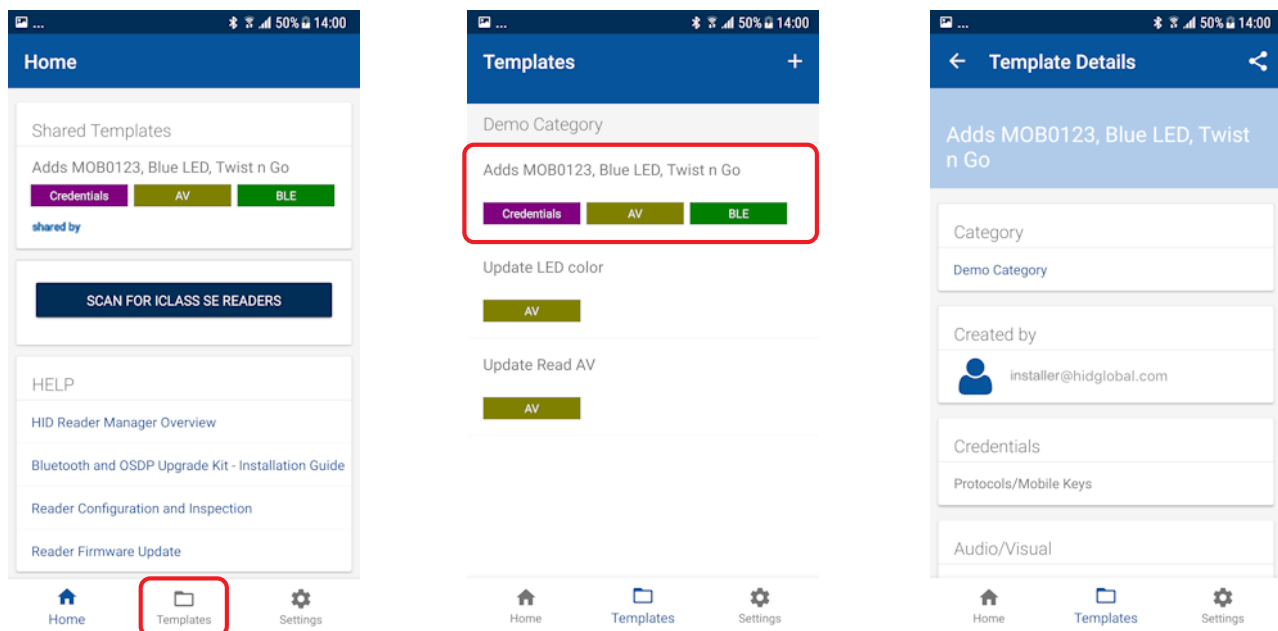


### 2.3.2.3 Display template details

Configuration templates that have been shared with the Reader Technician 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.



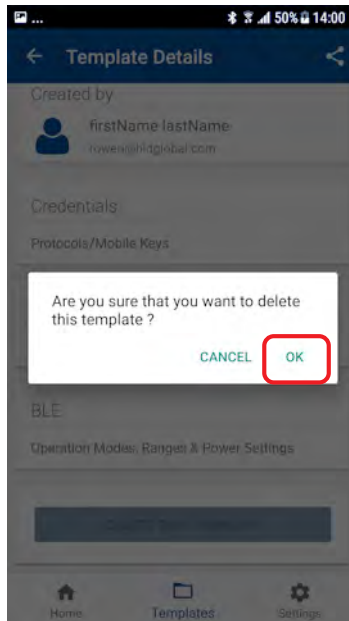
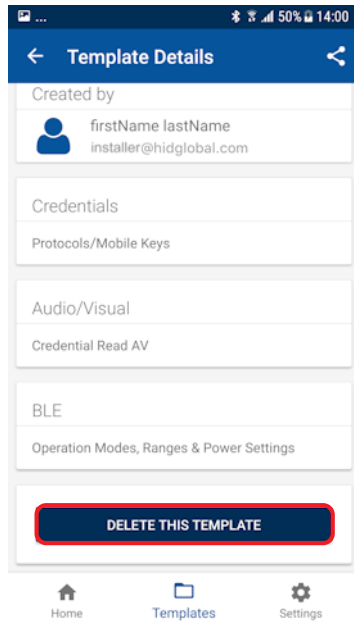
To view the list of created templates tap the **Templates** icon on the HID Reader Manager **Home** screen. Existing created templates are listed on the **Templates** screen. Tap on a displayed template to view the template details.



### 2.3.2.4 Delete a template

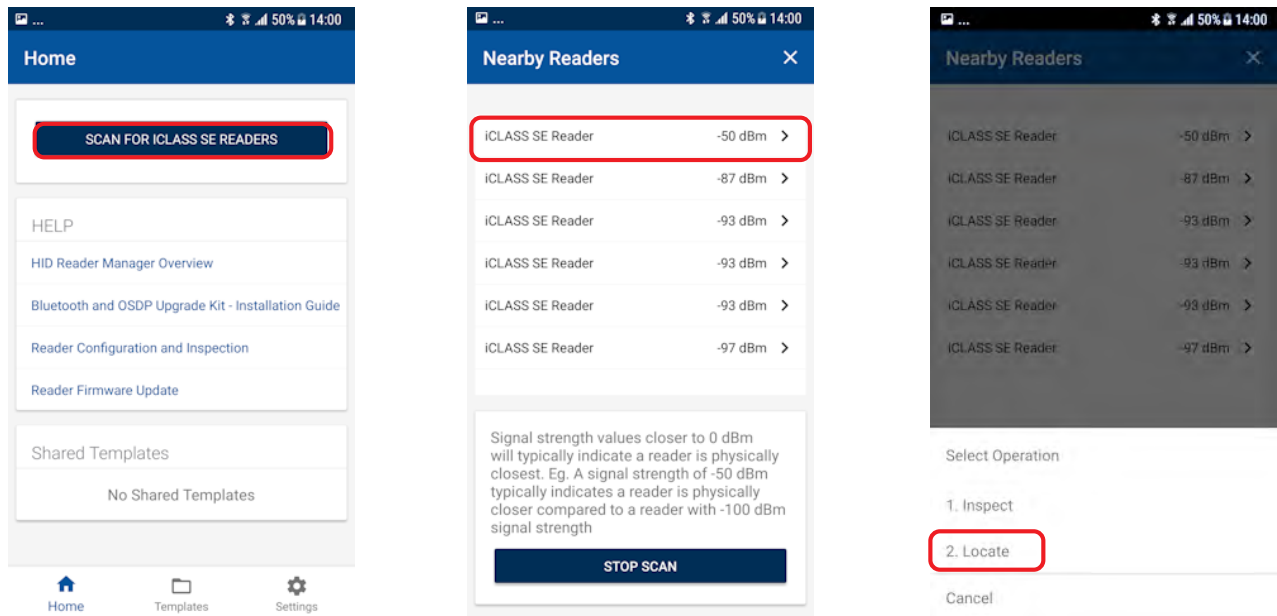
When template details are displayed, the template can be deleted:

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



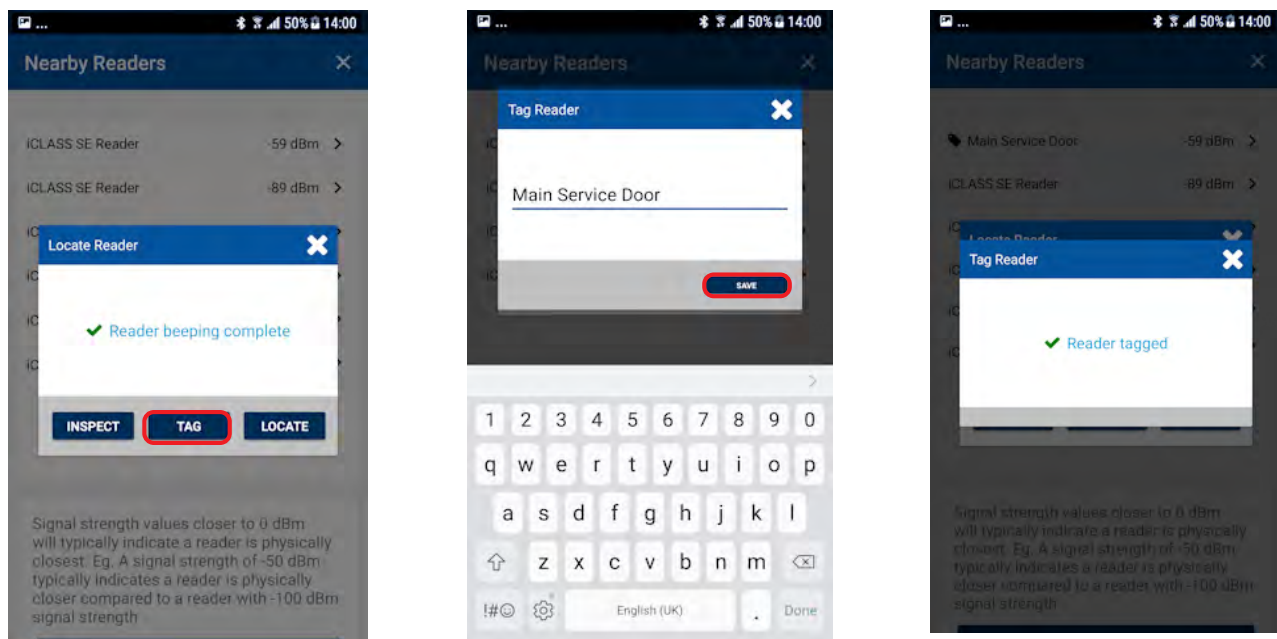
### 2.3.3 Connect to a reader

1. Tap **SCAN FOR ICLASS SE READERS** on the HID Reader Manager **Home** screen. This will scan for nearby Mobile Access® readers (i.e. readers with the BLE Communication module installed).
2. Select a displayed reader from the **Nearby Readers** screen and tap **Locate** from the **Select Operation** menu to ensure the correct reader is selected. The reader will beep for about eight seconds.

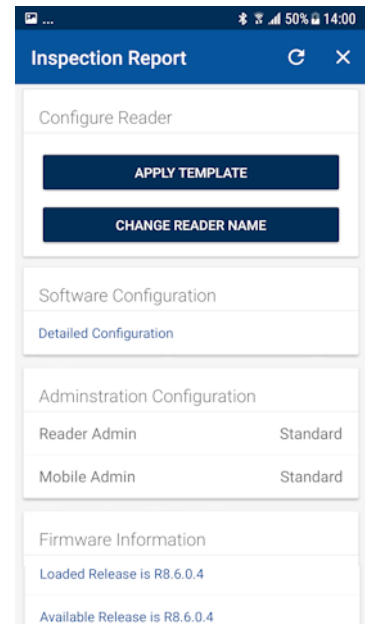
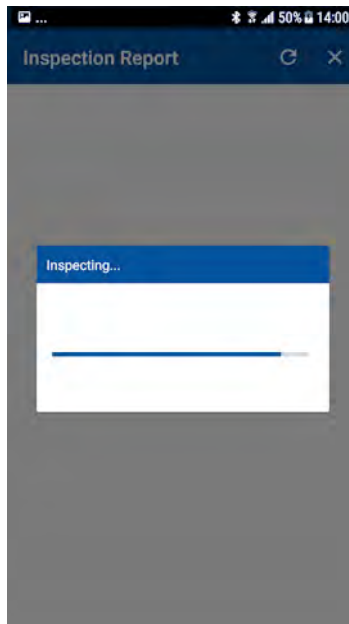
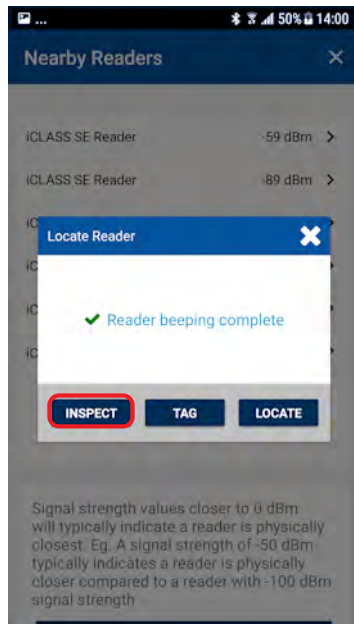


3. If you wish to name the reader for easier identification you can "Tag" it. Tap **TAG**, enter a name (for example, the reader location), and tap **SAVE**.

**Note:** The tagged reader name is only visible on your mobile device.



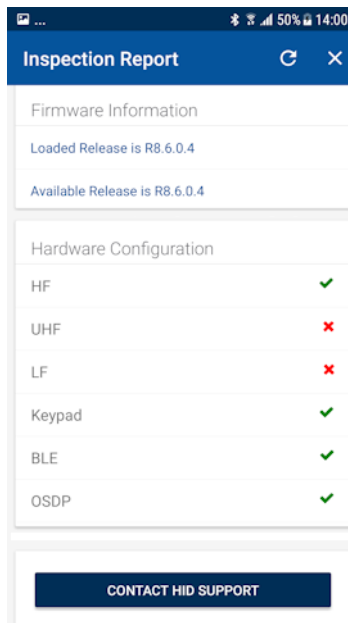
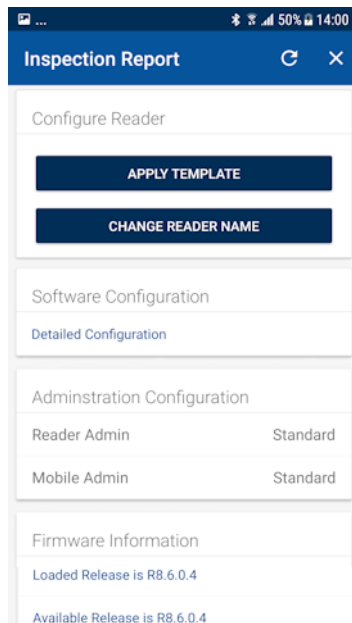
4. Tap **INSPECT**. The reader is now connected and reader information is displayed on the **Inspection Report** screen, see *Section 2.3.4 Reader inspection report*.



## 2.3.4 Reader inspection report

The **Inspection Report** screen displays hardware and configuration details for a connected reader and allows you to carry out the following operations:

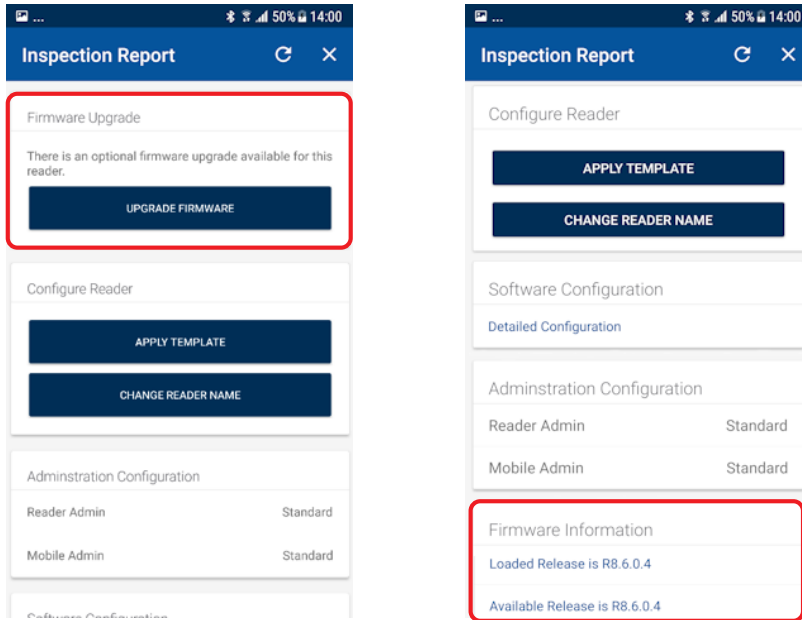
- View reader **Firmware Information** and, if necessary, perform a reader **Firmware Upgrade**. See *Section 2.3.5 Update reader firmware*.
- Tap **Detailed Configuration** to access detailed reader settings, modify settings and directly apply them to the reader. See *Section 2.3.6 View detailed reader configuration*.
- Configure the reader:
  - Tap **APPLY TEMPLATE** to select and apply template configuration settings to the reader. See *Section 2.3.7 Apply configuration changes*.
  - Tap **CHANGE READER NAME** to change the name of the reader. See *Section 2.3.8 Change reader name*.
- Tap **CONTACT HID SUPPORT** if you experience an issue while using the application. You will be provided with contact details for HID Support and an incident number for HID Support to be able to look up limited information regarding the affected reader. For additional information, see *Section 4.2 Contact HID Technical Support*.



### 2.3.5 Update reader firmware

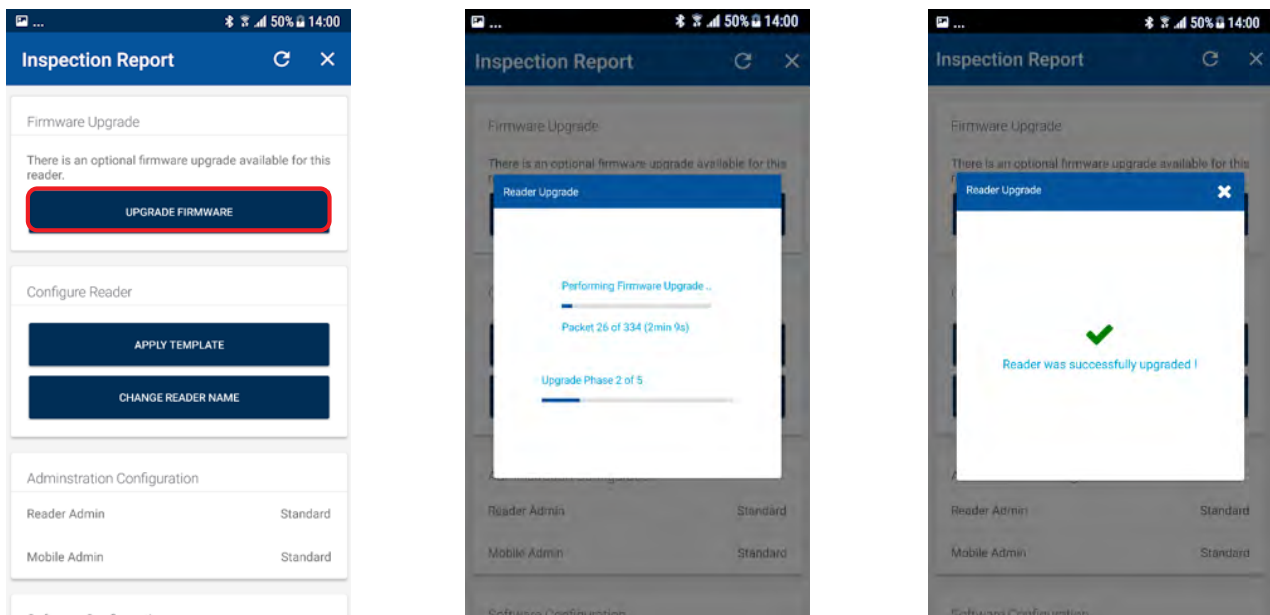
When connected to a reader, on the **Inspection Report** screen, if a newer version of firmware is available, you will be notified about the update in the **Firmware Upgrade** section.

**Note:** If the firmware is already at the latest release or the currently loaded firmware is not supported then the **UPGRADE FIRMWARE** option will not be available.



If a firmware upgrade is available, tap **UPGRADE FIRMWARE** to begin the firmware update process. This will take several minutes.

**Note:** If connection between the HID Reader Manager app and reader is lost during the firmware update process then reconnect the app to the reader and the upgrade process will resume.



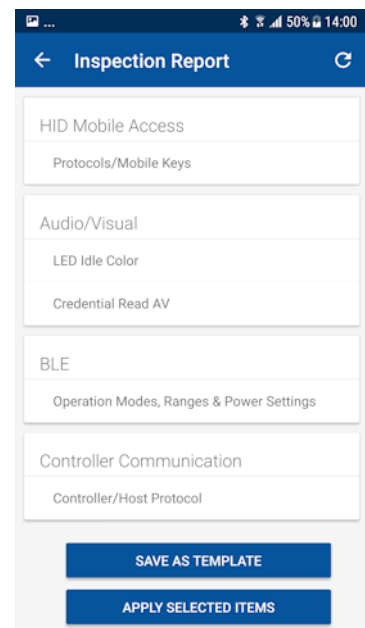
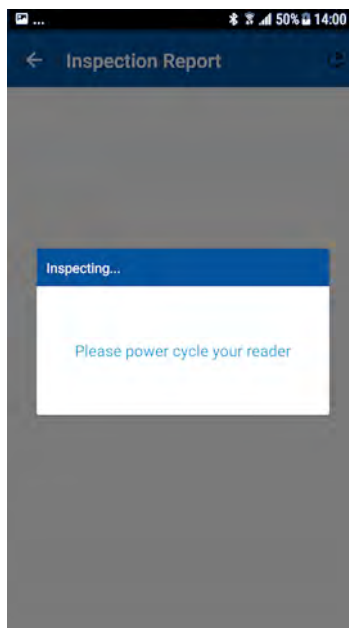
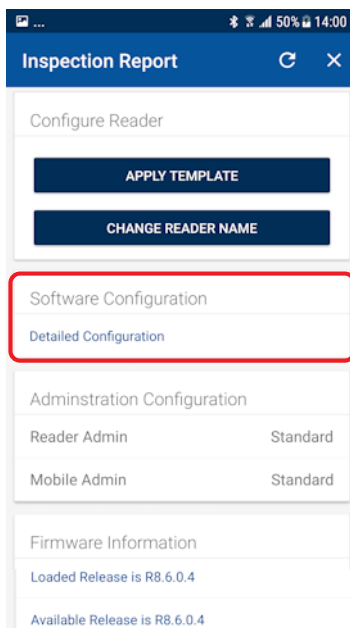
## 2.3.6 View detailed reader configuration

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

**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.

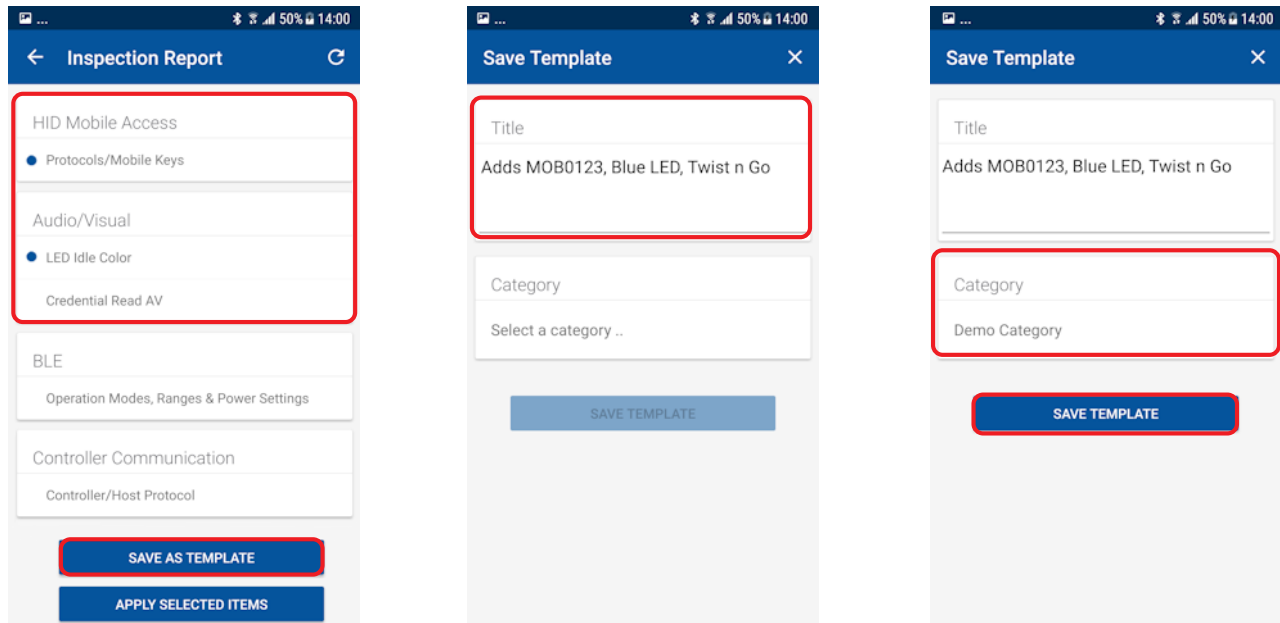
2. From the detailed **Inspection Report** screen you can directly configure reader settings:

- **HID Mobile Access** settings. See *Section 2.3.1.1 Credential settings*.
- **Audio/Visual** settings. See *Section 2.3.1.2 Audio/Visual settings*.
- **BLE** settings. See *Section 2.3.1.3 BLE settings*.
- **Controller Communication** settings. See *Section 2.3.1.4 Controller Communication settings*.



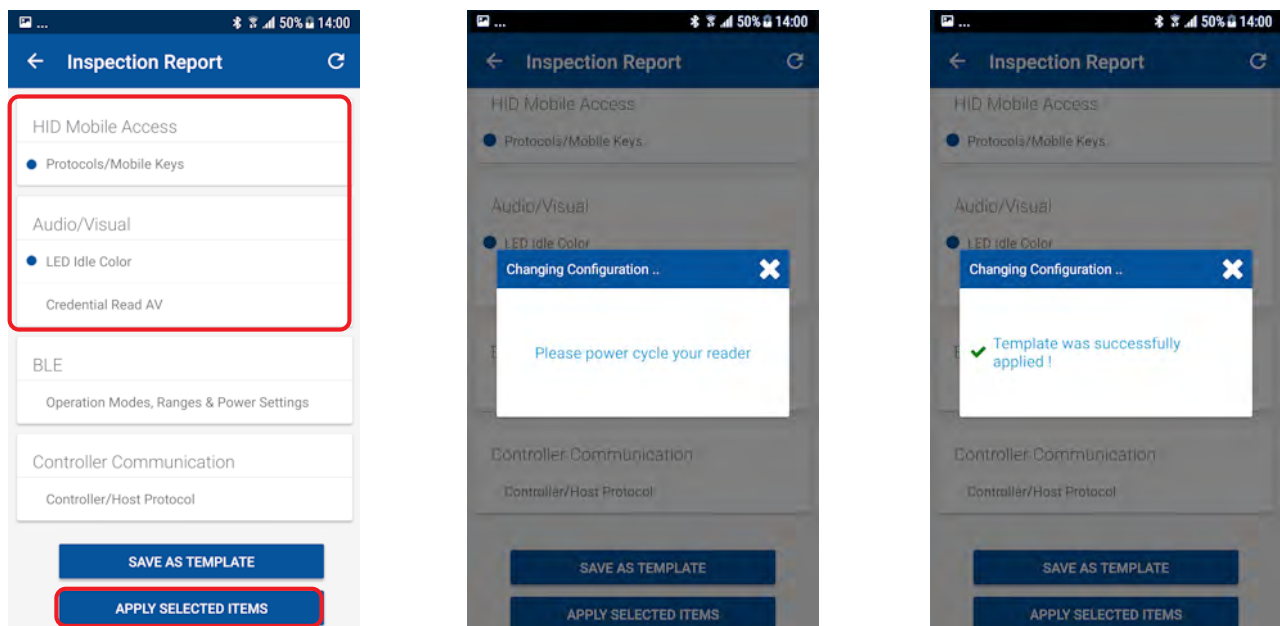
3. Any changed configuration settings are indicated with a blue circle. Changed configuration settings can be:

- Saved as a template: tap **SAVE AS TEMPLATE**, enter a template title and category and tap **SAVE TEMPLATE**.



- Tap **APPLY SELECTED ITEMS** to directly apply settings to the connected 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.

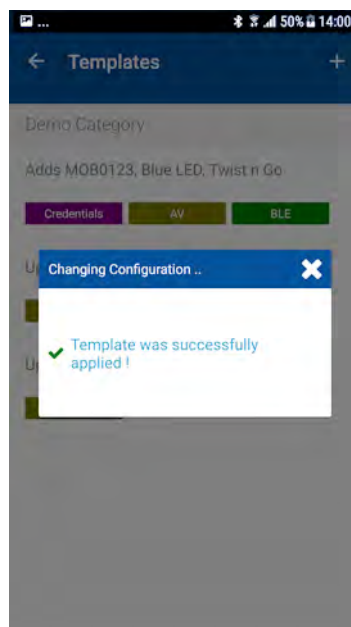
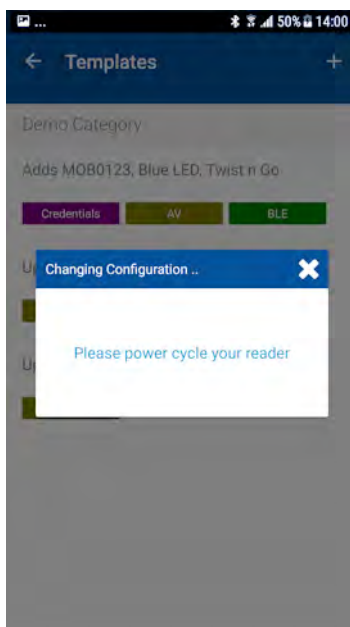
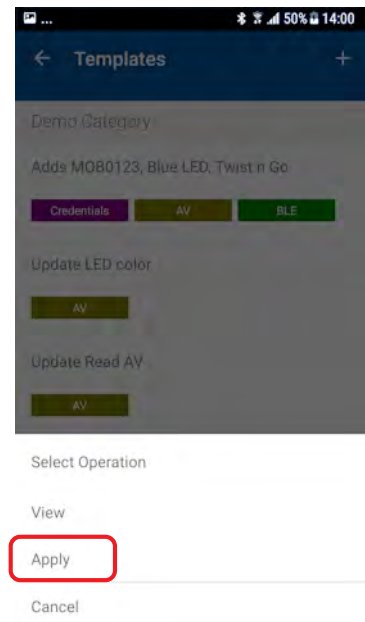
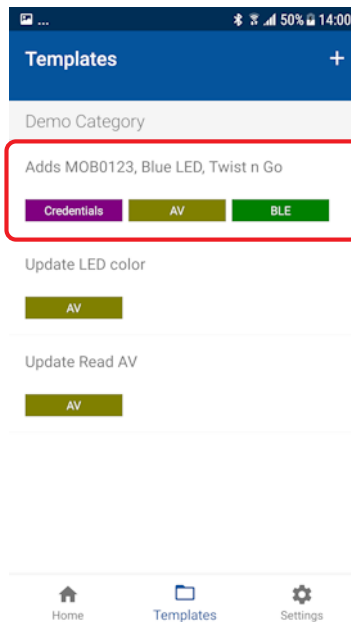
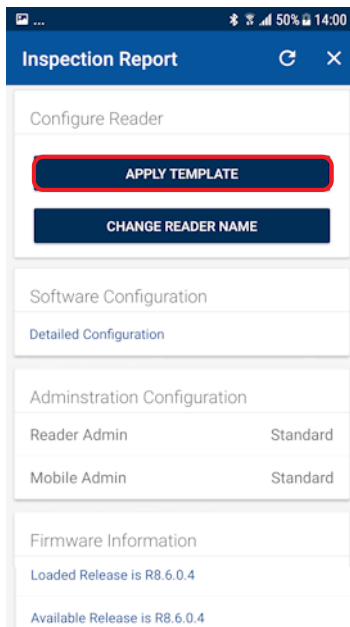


### 2.3.7 Apply configuration changes

When viewing a reader **Inspection Report**:

1. Tap **APPLY TEMPLATE**.
2. Select a displayed template from the **Templates** screen. Tap **Apply** from the **Select Operation** menu.

**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.

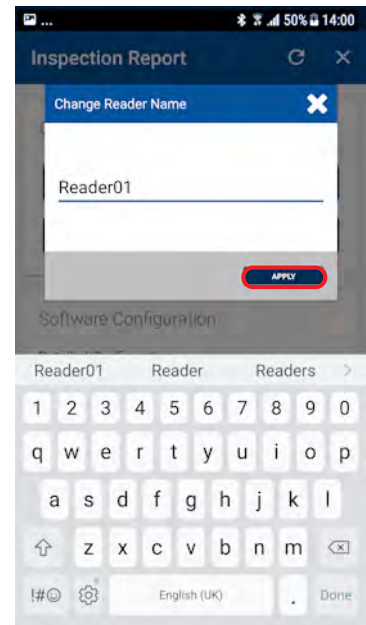
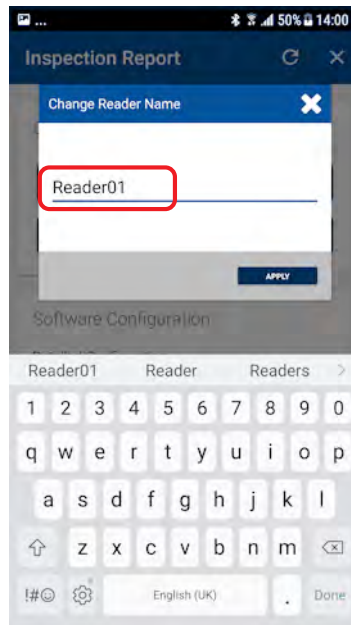
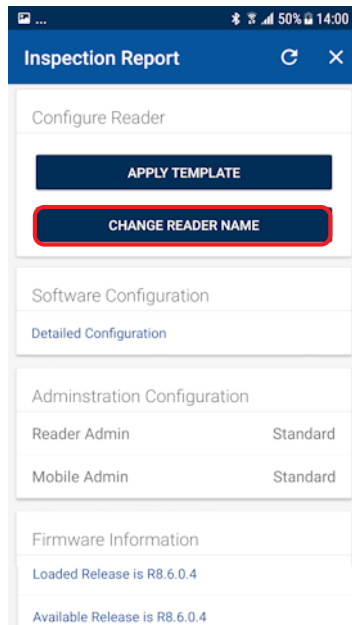


## 2.3.8 Change reader name

When viewing a reader **Inspection Report** the reader name can be changed.

**Note:** 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.

1. Tap **Change Reader Name**.
2. Enter a new reader name.
3. Tap **Apply**.





# Section 3

## 3 HID Reader Manager Portal

---

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

**Note:** The HID® Reader Manager™ Portal is not required for Standard Key readers as these do not use HID Elite™ and/or MOB keys.

### 3.1 Portal setup overview

The HID Mobile Access® Portal provides iCLASS Elite™ and Mobile Key end users with the option to enable/disable the HID Reader Manager Portal. Adding or removing the HID Reader Manager Portal for an organization must be completed by HID.

To setup the HID Reader Manager Portal, refer to the *HID Mobile Access Portal - HID Reader Manager Portal Change Form* located at:

<https://www.hidglobal.com/documents>

A HID Mobile Access Portal is required to enable/disable HID Reader Manager. If this has not been setup for a organization, please follow this process:

- **Mobile (MOB) Key Users:** Follow the steps provided at:

<https://managedservices.hidglobal.com/faces/maUserOnBoardingStart>

Then complete and return the *HID Mobile Access® Portal - HID Reader Manager Portal Change Form*.

- **iCLASS Elite Key Users:** Complete and return the *iCLASS Elite Program™ - New HID Mobile Access® Portal Request Form*. The HID Reader Manager Portal is enabled/disabled with this form.

**Note:**

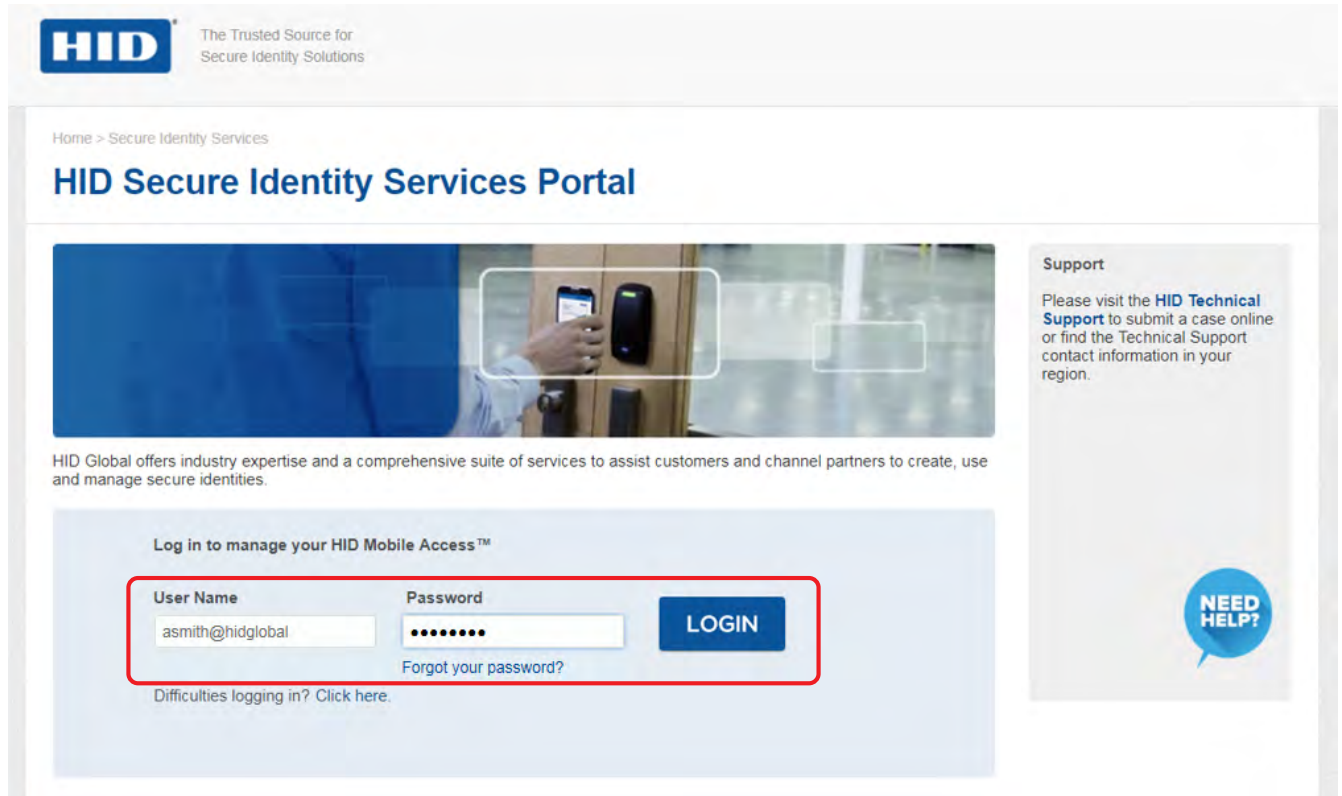
- A HID Mobile Access Portal is required to enable the HID Reader Manager Portal.
- When the HID Reader Manager Portal is enabled/disabled, the HID Reader Manager Portal Admin role will be granted/revoked from all active HID Mobile Access Org Admins.

## 3.2 Access the HID Reader Manager Portal

The HID Reader Manager Portal is a hosted service available to registered Reader Manager Administrators. To access the portal:

1. Log into the HID Secure Identity Services (SIS) Portal.

**Note:** This is the same login page and login credentials used for the Mobile Access Portal.



**HID** The Trusted Source for Secure Identity Solutions

Home > Secure Identity Services

## HID Secure Identity Services Portal

HID Global offers industry expertise and a comprehensive suite of services to assist customers and channel partners to create, use and manage secure identities.

Log in to manage your HID Mobile Access™

User Name Password LOGIN

asmith@hidglobal

Forgot your password?

Difficulties logging in? Click here.

Support

Please visit the **HID Technical Support** to submit a case online or find the Technical Support contact information in your region.

NEED HELP?

2. Select the **HID Reader Manager** link on the main **HID Secure Identity Services Portal** page.

[Home](#) > [Secure Identity Services](#)

## HID Secure Identity Services Portal



HID Global offers industry expertise and a comprehensive suite of services to assist customers and channel partners to create, use and manage secure identities.



### Card Services

Our Card Services application offers easy-to-use online tools to personalize and produce ID card badges – whether you are looking to outsource the daily flow of requests or faced with the daunting task of re-badging thousands of employees.



### HID Mobile Access®

Our HID Mobile Access application allows you to easily issue and manage Mobile IDs for smart devices. The HID Mobile Access solution allows you to provision and revoke access rights over-the-air through this robust application.



### Online Order Status and RMA Requests

Our Order Status and RMA Request tool makes it possible for HID Direct Customers to check order status and request a Return Material Authorization (RMA) through an easy-to-use and secure online system.

HID SIS Administration

**Last Successful Login**

Sep 17, 2018 14:47:16 (GMT)

[My Account](#) | [Log Out](#)

[HID Mobile Access](#)

[HID Reader Manager](#)

Administration

### RELATED DOCUMENTS

The agreements below are accepted during App installation:

[HID Mobile Access end user license agreement \(Android\)](#)

[HID Mobile Access end user license agreement \(iOS\)](#)

[Privacy Policy for HID Mobile Access](#)

### RELATED LINKS

[Frequently Asked Questions](#)

3. Click **YES** to be redirected to your organizations instance of the HID Reader Manager Portal.

### Redirecting to HID Reader Manager Portal

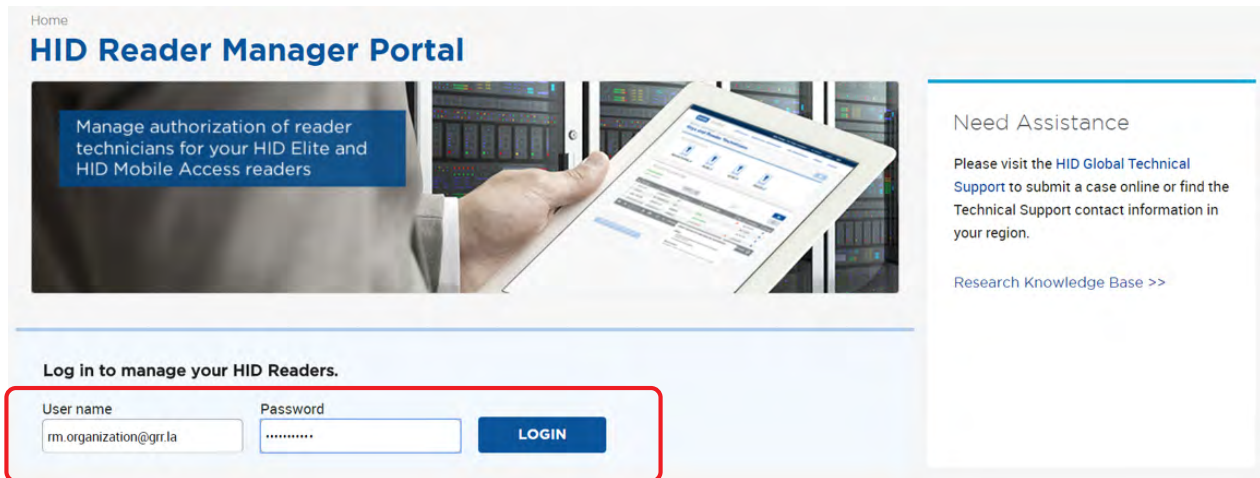
You will be transferred to the HID Reader Manager Portal in a new tab. You will be required to log in using your Secure Identity Services Portal account.

Do you want to continue?

[NO](#)

[YES](#)

4. Login as Reader Manager Administrator using the User name and Password setup in the HID Secure Identity Services Portal.



Home

## HID Reader Manager Portal

Manage authorization of reader technicians for your HID Elite and HID Mobile Access readers

**Need Assistance**

Please visit the [HID Global Technical Support](#) to submit a case online or find the Technical Support contact information in your region.

[Research Knowledge Base >>](#)

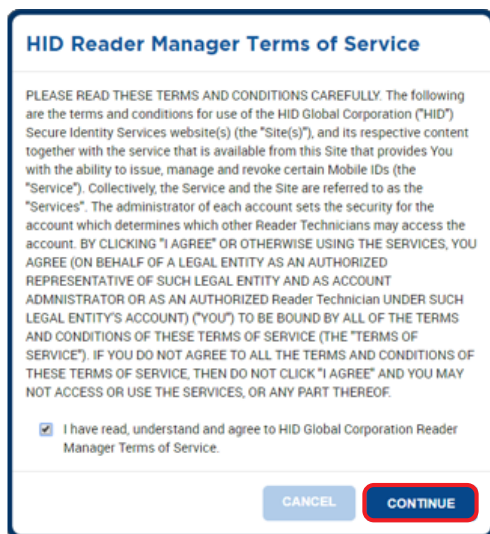
**Log in to manage your HID Readers.**

User name: rm.organization@grt.la

Password: \*\*\*\*\*

**LOGIN**

**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**.



### HID Reader Manager Terms of Service

PLEASE READ THESE TERMS AND CONDITIONS CAREFULLY. The following are the terms and conditions for use of the HID Global Corporation ("HID") Secure Identity Services website(s) (the "Site(s)"), and its respective content together with the service that is available from this Site that provides You with the ability to issue, manage and revoke certain Mobile IDs (the "Service"). Collectively, the Service and the Site are referred to as the "Services". The administrator of each account sets the security for the account which determines which other Reader Technicians may access the account. BY CLICKING "I AGREE" OR OTHERWISE USING THE SERVICES, YOU AGREE (ON BEHALF OF A LEGAL ENTITY AS AN AUTHORIZED REPRESENTATIVE OF SUCH LEGAL ENTITY AND AS ACCOUNT ADMINISTRATOR OR AS AN AUTHORIZED Reader Technician UNDER SUCH LEGAL ENTITY'S ACCOUNT) ("YOU") TO BE BOUND BY ALL OF THE TERMS AND CONDITIONS OF THESE TERMS OF SERVICE (THE "TERMS OF SERVICE"). IF YOU DO NOT AGREE TO ALL THE TERMS AND CONDITIONS OF THESE TERMS OF SERVICE, THEN DO NOT CLICK "I AGREE" AND YOU MAY NOT ACCESS OR USE THE SERVICES, OR ANY PART THEREOF.


☒ I have read, understand and agree to HID Global Corporation Reader Manager Terms of Service.

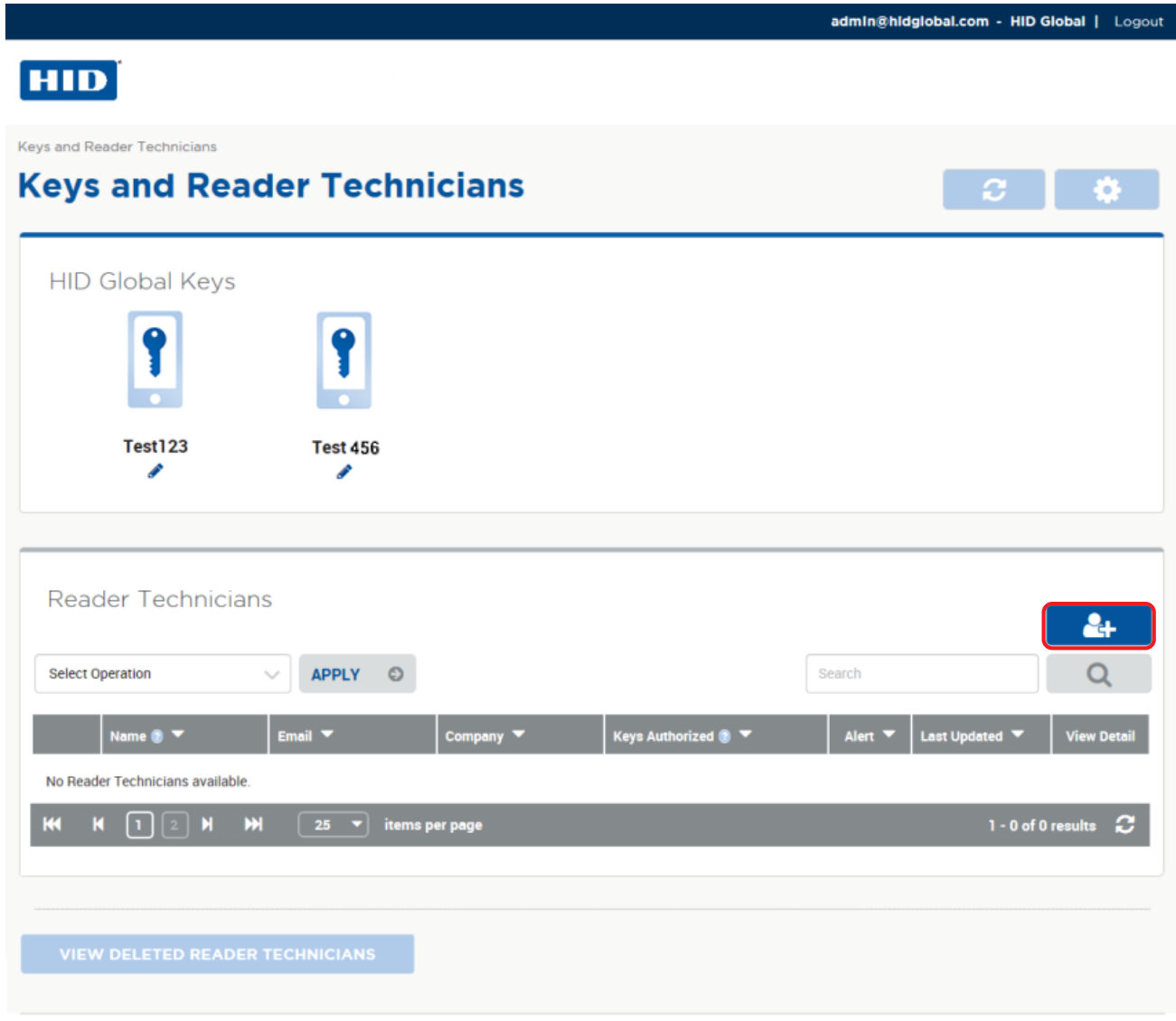
**CANCEL** **CONTINUE**

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

### 3.3 Enroll a Reader Technician

To enroll a Reader Technician in the HID Reader Manager Portal:

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



admin@hidglobal.com - HID Global | Logout

## Keys and Reader Technicians

HID Global Keys

Test123 Test 456

### Reader Technicians

Select Operation  Search


Name	Email	Company	Keys Authorized	Alert	Last Updated	View Detail
No Reader Technicians available.						

1 - 0 of 0 results

[VIEW DELETED READER TECHNICIANS](#)

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

admin@hidglobal.com - HID Global | Logout


HID Administration

Keys and Reader Technicians > Enroll Reader Technician

## Enroll Reader Technician

Reader Technician Information

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

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

Invitation & Key Authorization

**How do you want to proceed?**

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


☐ Send invitation and Key Authorization(s) to Reader Technician.

CANCEL

ENROLL

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

admin@hidglobal.com - HID Global | Logout




Keys and Reader Technicians

## Keys and Reader Technicians


↺
⚙️

### HID Global Keys



**Test123**

✎



**Test 456**

✎

### Reader Technicians

Select Operation ▼

APPLY

Search

🔍

+ User

<input type="checkbox"/>	Name ▼	Email ▼	Company ▼	Keys Authorized ▼	Alert ▼	Last Updated ▼	View Detail
<input type="checkbox"/>	Demo Installer	demo.installer@hidglobal.com	HID Global	-		Feb 02, 2018	▶

⏮
⏪

1

2

⏩
⏭

25

 items per page

1 - 1 of 1 results
 ↺


VIEW DELETED READER TECHNICIANS

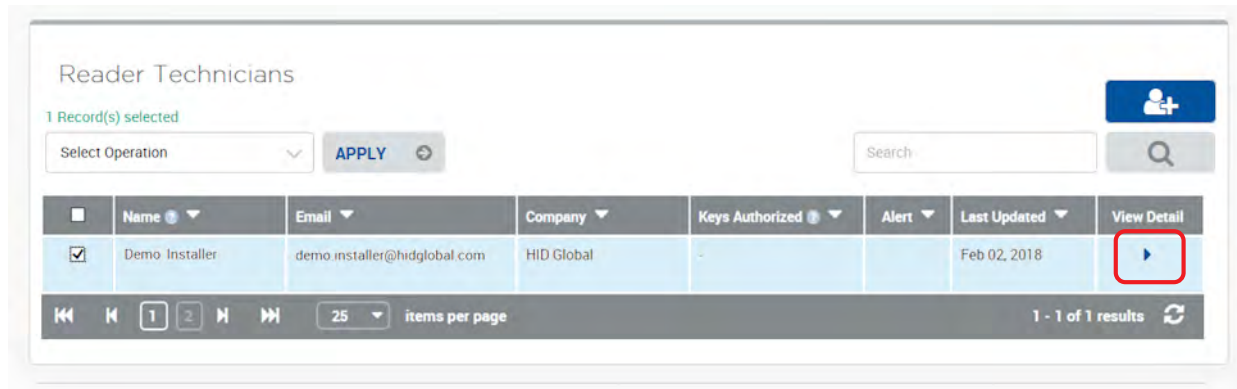
The enrolled Reader Technician will receive a Reader Manager invitation email in their registered email inbox containing an invitation code for activating the HID Reader Manager app. See *Section 2.1.6 Activate invitation code in the HID Reader Manager app.*

When the Reader Manager app is activated the administrator can issue key authorization. See *Section 3.4 Issue authorization keys.*

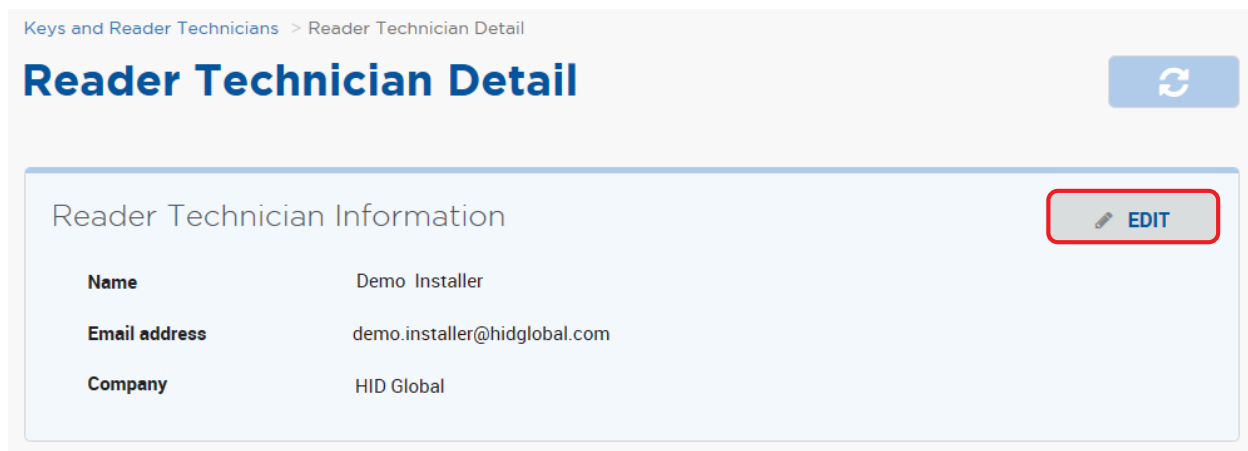
### 3.3.1 Edit Reader Technician information

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** Demo Installer

**Email address** demo.installer@hidglobal.com

**Company** HID Global

 **SAVE** Cancel

### 3.3.2 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.

Reader Technicians

1 Record(s) selected

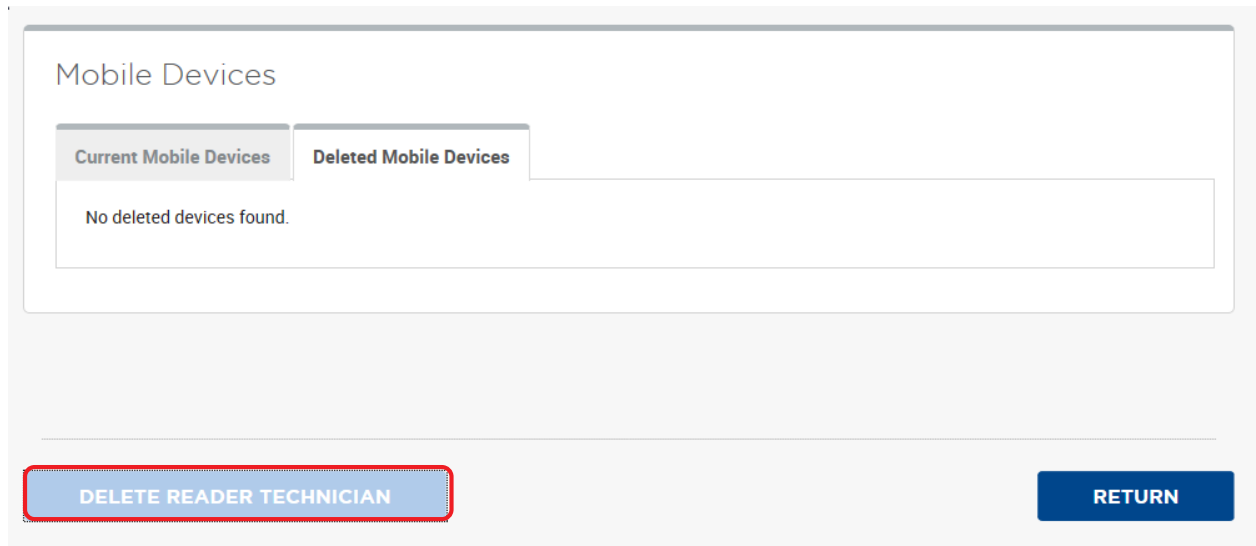
Select Operation **APPLY**

Search

<input type="checkbox"/>	Name	Email	Company	Keys Authorized	Alert	Last Updated	View Detail
<input checked="" type="checkbox"/>	Demo Installer	demo.installer@hidglobal.com	HID Global	-		Feb 02, 2018	

25 items per page 1 - 1 of 1 results

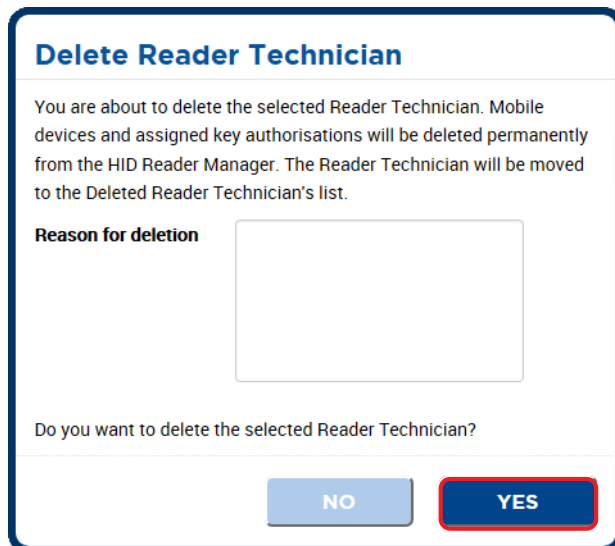
3. Scroll to the bottom of the **Reader Technician Detail** page and click **DELETE READER TECHNICIAN**.



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 *Section 3.4.5 Configure Delete Threshold*), has elapsed the system automatically completes the delete operation and places the key authorization in a revoked state.



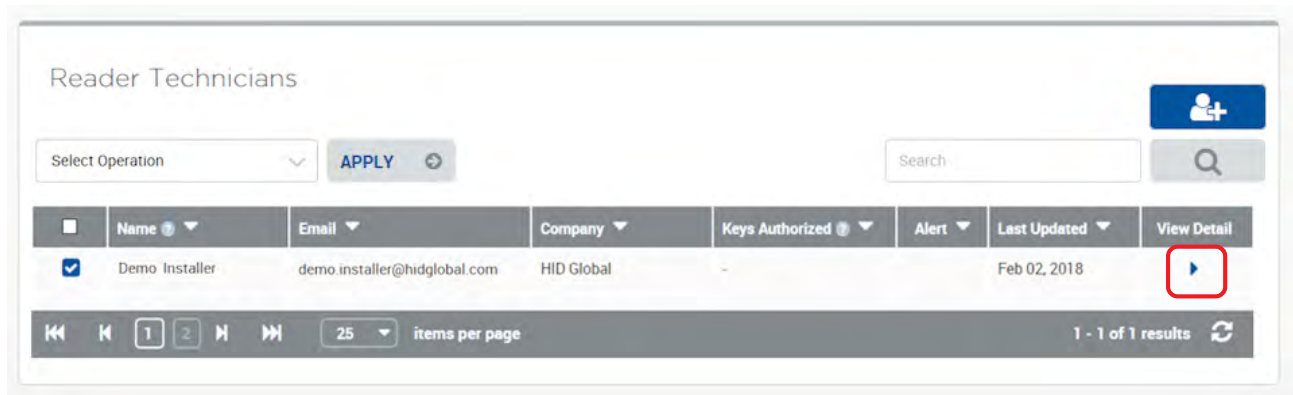
The deleted Reader Technician appears in the list of **Deleted Reader Technicians**.

### 3.4 Issue authorization keys

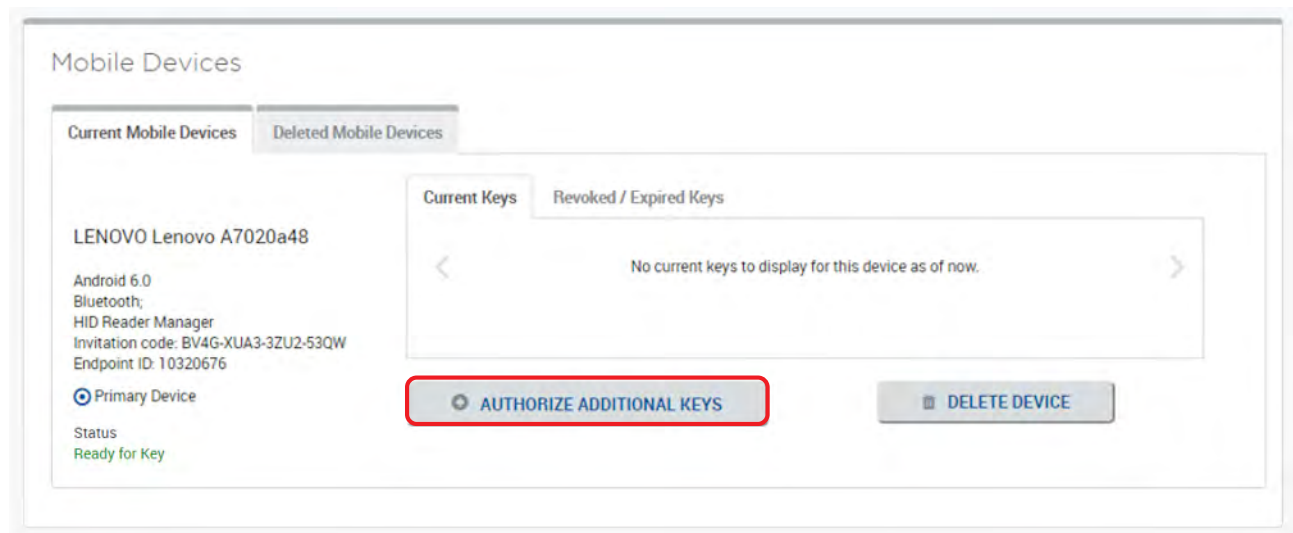
Reader Manager uses authorization keys to securely connect and control access by the mobile app.

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**.

admin@hidglobal.com - HID Global | Logout



Keys and Reader Technicians > Reader Technician Detail > Authorize Additional Keys

## Authorize Additional Keys



Available RM Testing Organization Keys

**LENOVO Lenovo A7020a48**

Android 6.0  
Bluetooth;  
HID Reader Manager  
Invitation Code: BV4G-XUA3-3ZU2-53QW  
Endpoint ID: 10320676

Primary Device

Status  
Ready for Key

**Key**

Validity period for authorization (Optional)

MOB0001

▼

2

Years

▼

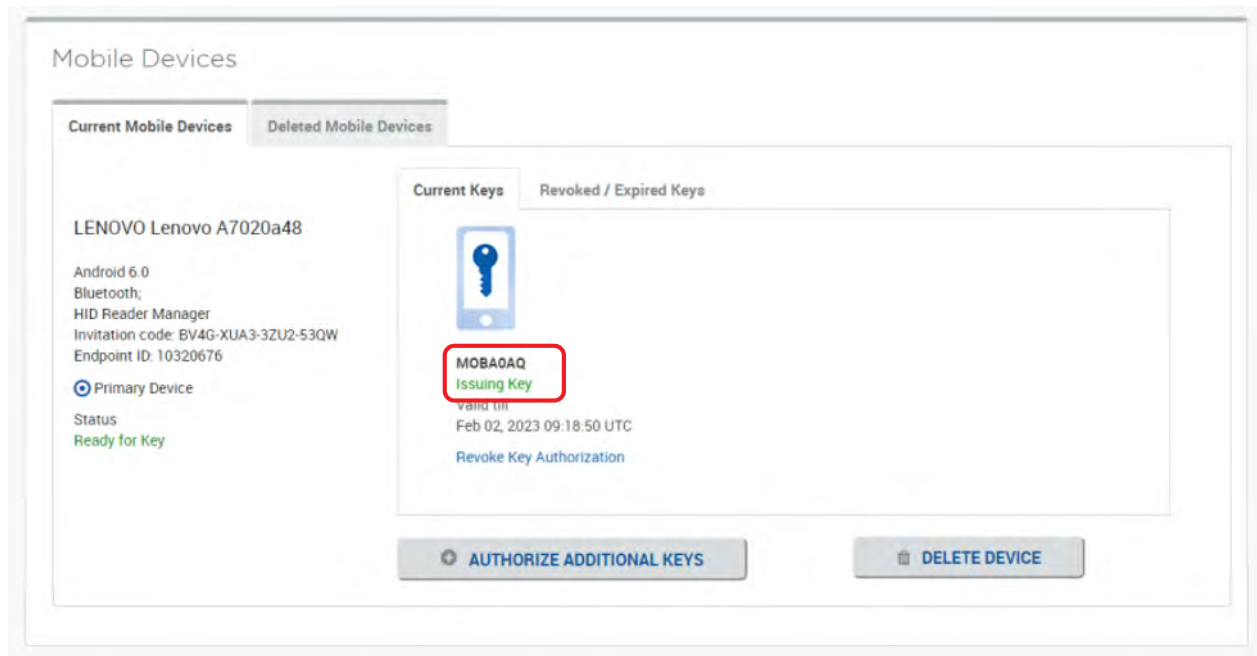
CANCEL

SAVE

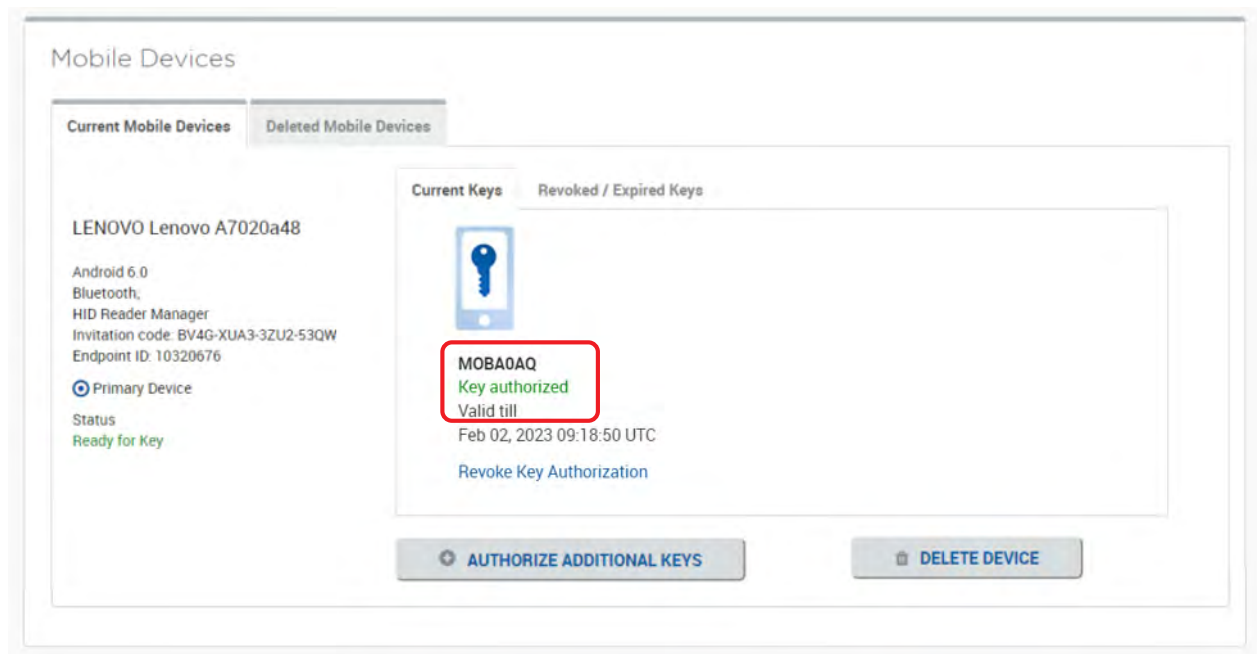
50

September 2018

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




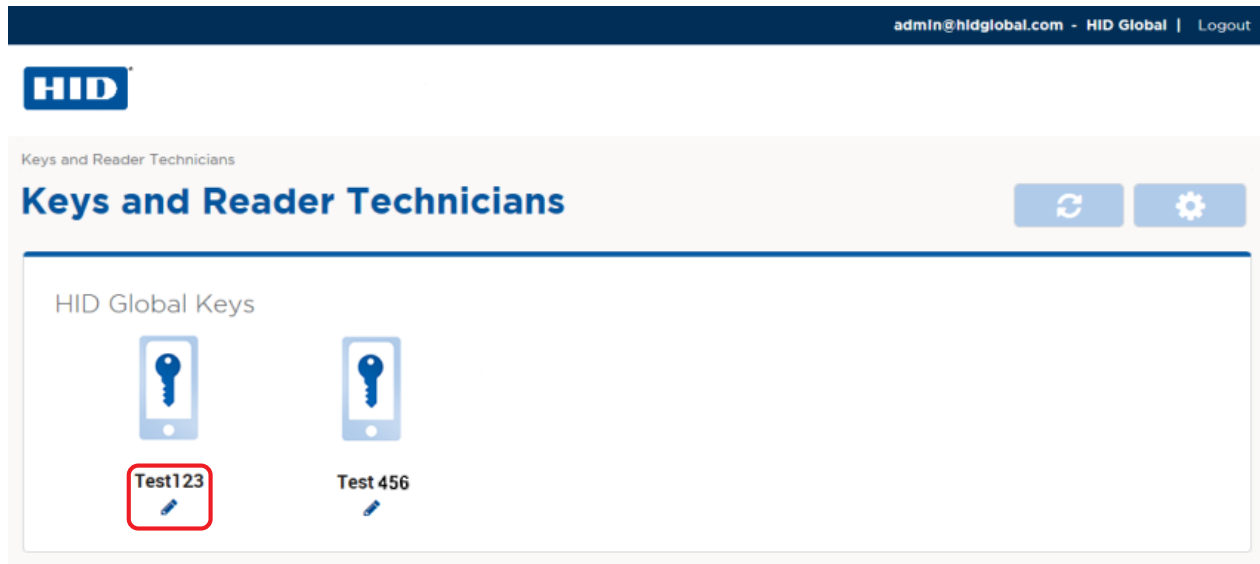
7. Check with the Reader Technician that the authorization key has been issued to the Reader Manager app. See *Section 2.1.7 Display authorized keys*.
8. Refresh the **Reader Technician Detail** page and verify that the key status is changed to **Key authorized**.



### 3.4.1 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**.

#### Edit Key Details

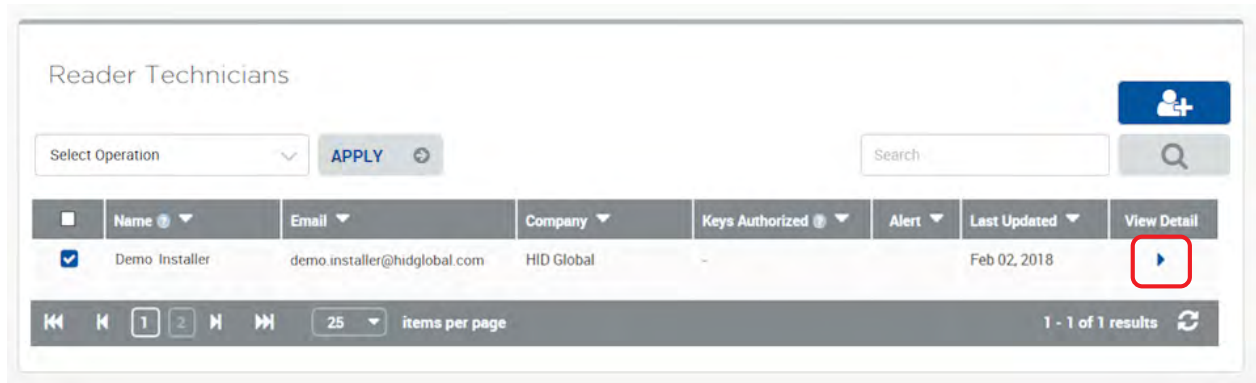
**Key reference**  
ICE65789

**Friendly name of key**

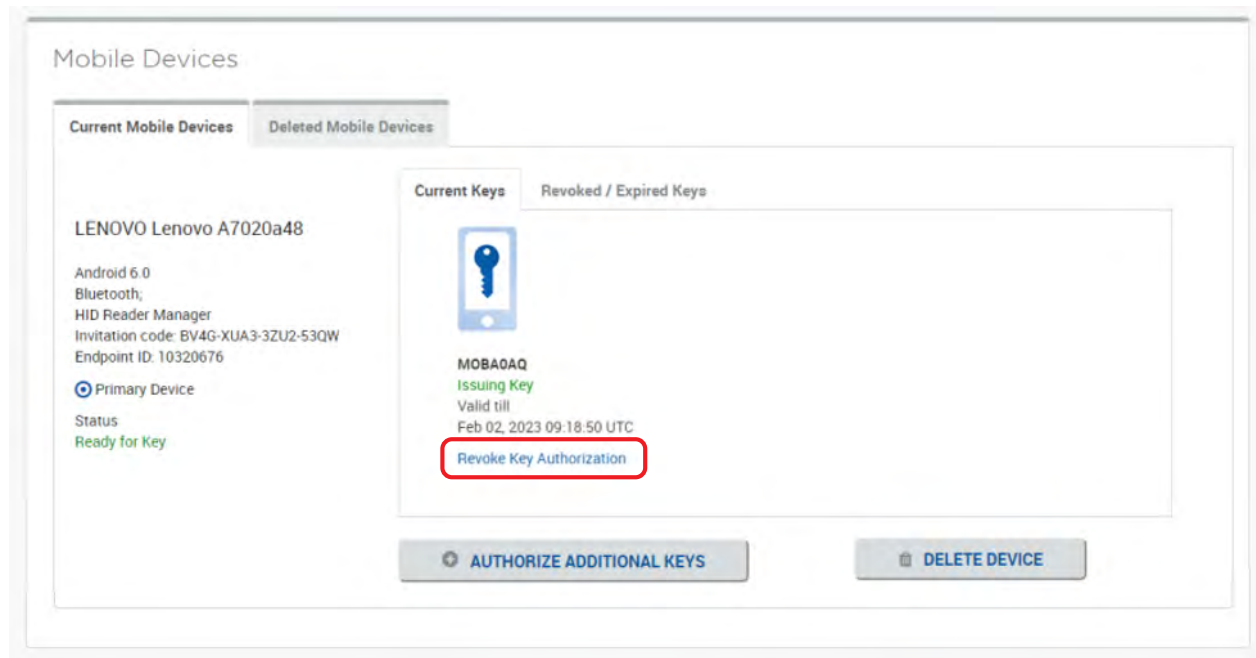
**Description (Optional)**

### 3.4.2 Revoke (delete) key authorization

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.



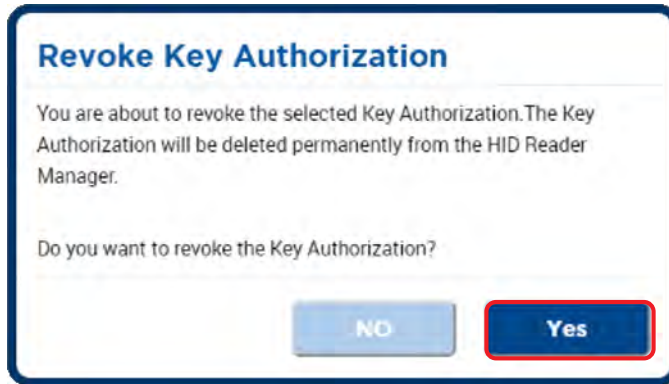
3. Scroll to the **Mobile Devices** section. For the authorization key to revoke, click **Revoke Key Authorization**.



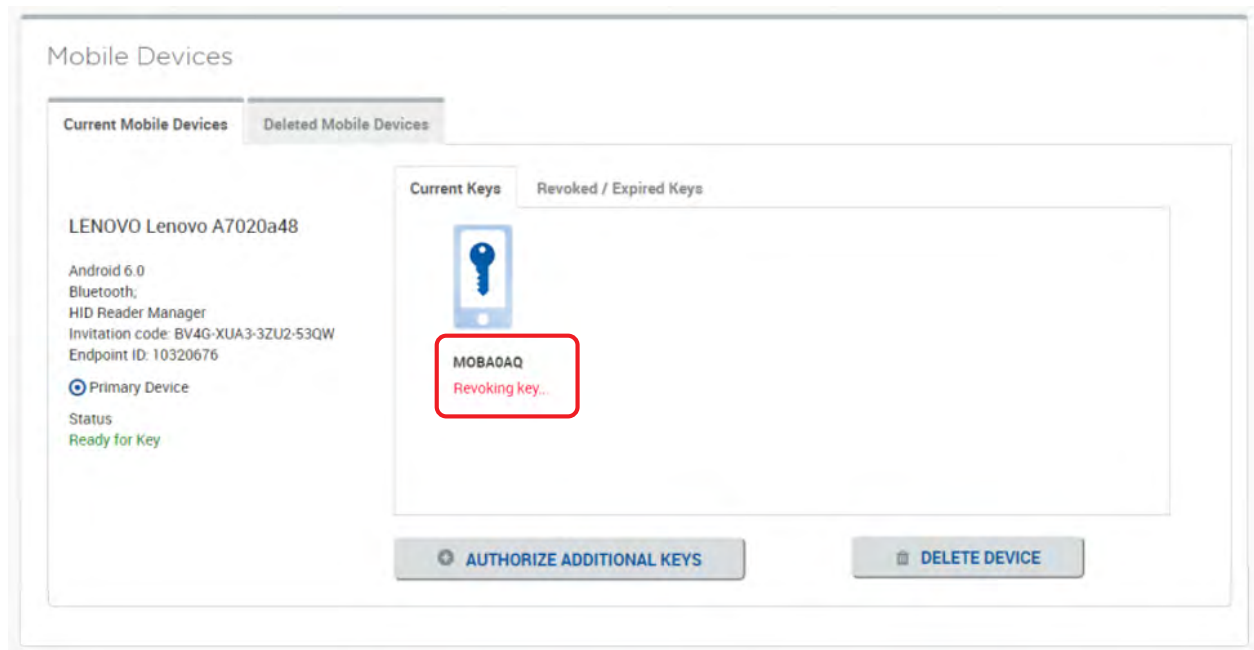
4. Click **YES** to revoke the selected key authorization from the HID Reader Manager.

**Note:** The key authorization 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.

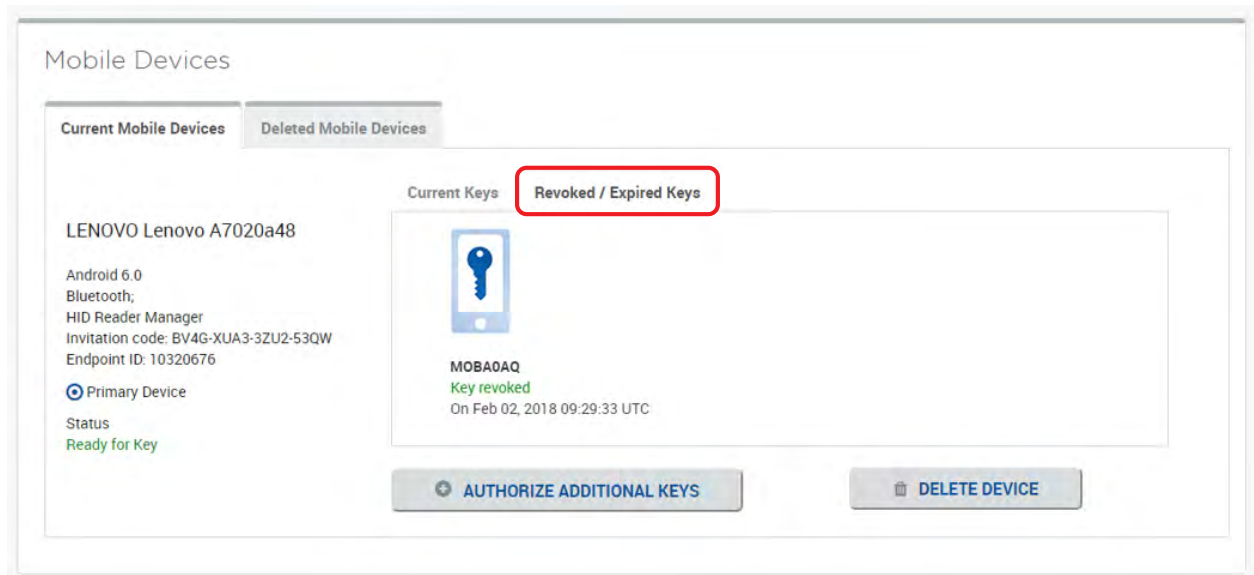
When the Delete Threshold time (see *Section 3.4.5 Configure Delete Threshold*), has elapsed the system automatically completes the delete operation and places the key authorization in a revoked state.



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




5. Check with the 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.



### 3.3 Configure HID Reader Manager Portal settings

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


admin@hidglobal.com - HID Global | Logout




Keys and Reader Technicians

Keys and Reader Technicians

HID Global Keys



Test123



Test 456

Reader Technicians

Select Operation

APPLY

Search

Name	Email	Company	Keys Authorized	Alert	Last Updated	View Detail
No Reader Technicians available.						

125 items per page

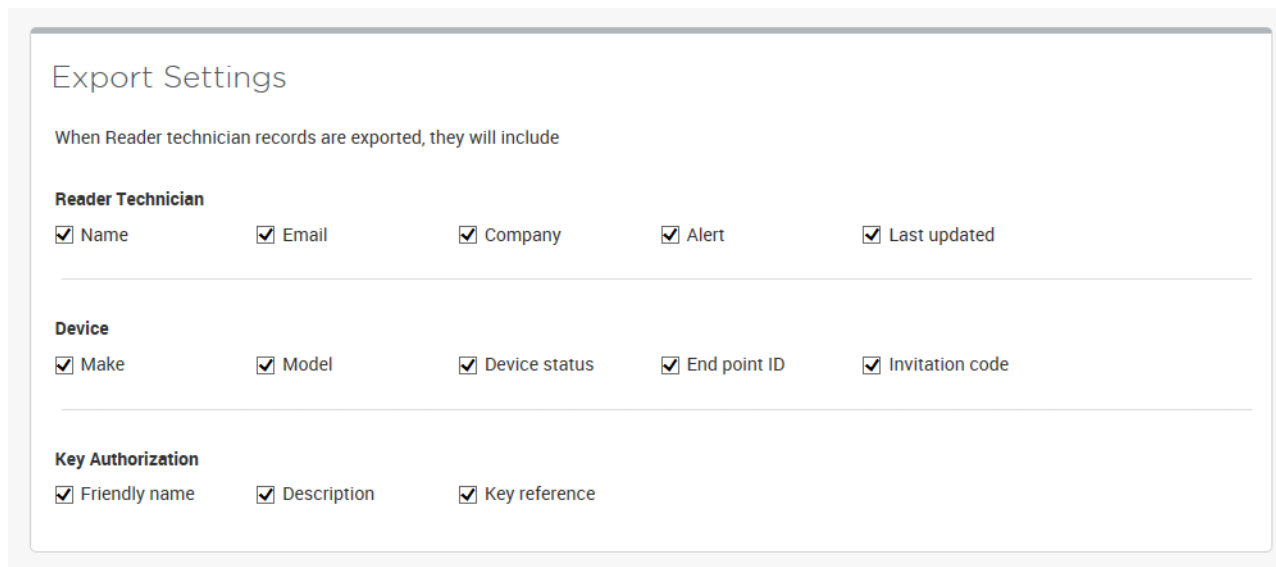
1 - 0 of 0 results

VIEW DELETED READER TECHNICIANS

### 3.4.3 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.



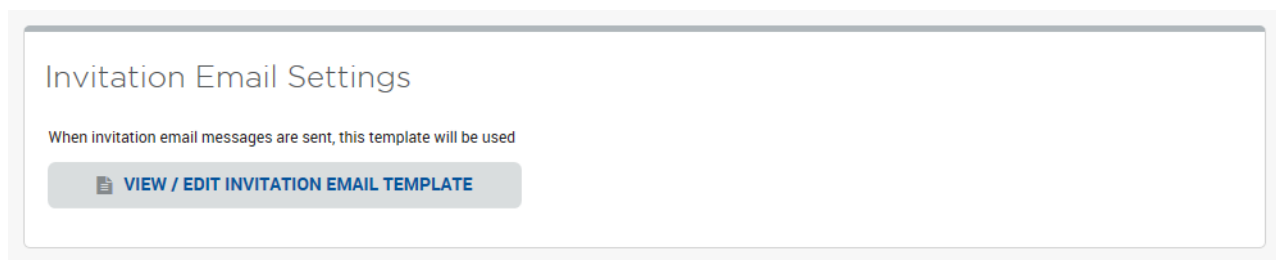
The screenshot shows the 'Export Settings' form. It has a title 'Export Settings' and a subtitle 'When Reader technician records are exported, they will include'. Below this, there are three sections: 'Reader Technician', 'Device', and 'Key Authorization'. Each section contains a list of fields with checkboxes. In the 'Reader Technician' section, 'Name', 'Email', 'Company', 'Alert', and 'Last updated' are all checked. In the 'Device' section, 'Make', 'Model', 'Device status', 'End point ID', and 'Invitation code' are all checked. In the 'Key Authorization' section, 'Friendly name', 'Description', and 'Key reference' are all checked.

Section	Field	Selected
Reader Technician	Name	Yes
	Email	Yes
	Company	Yes
	Alert	Yes
	Last updated	Yes
Device	Make	Yes
	Model	Yes
	Device status	Yes
	End point ID	Yes
	Invitation code	Yes
Key Authorization	Friendly name	Yes
	Description	Yes
	Key reference	Yes

### 3.4.4 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' form. It has a title 'Invitation Email Settings' and a subtitle 'When invitation email messages are sent, this template will be used'. Below this, there is a single button labeled 'VIEW / EDIT INVITATION EMAIL TEMPLATE' with a document icon.

Action
<a href="#">VIEW / EDIT INVITATION EMAIL TEMPLATE</a>

### 3.4.5 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.

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.

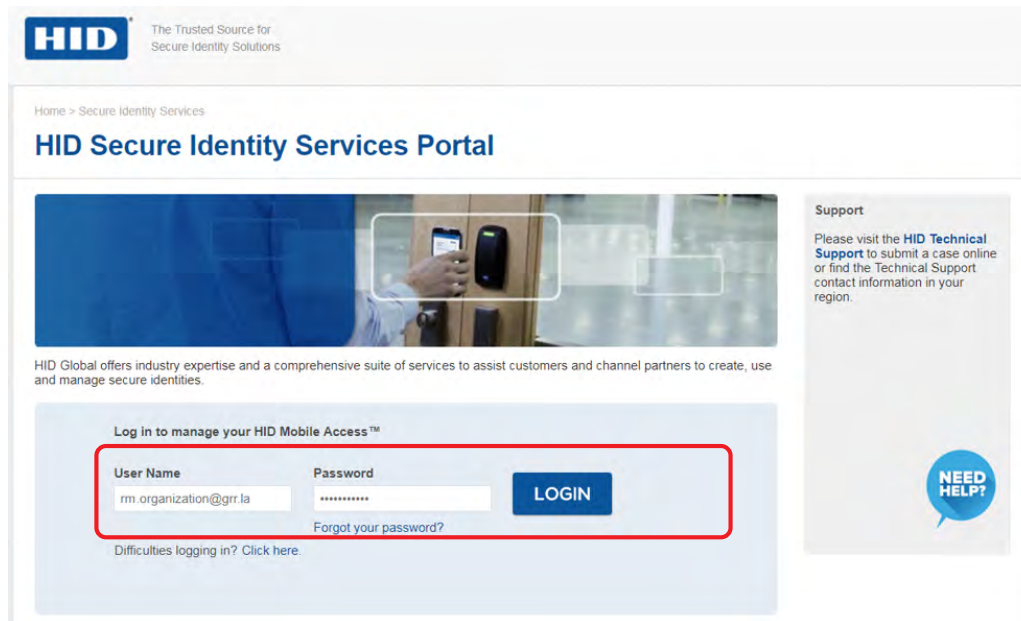
Delete threshold
2

Hours
▼

### 3.5 Enroll additional Reader Manager Admin

When adding a Reader Manager Admin for an Organization, the Organization Administrator must login to the SIS Portal and add the Administrators under the Administration tab.

1. Log into the SIS Portal as Organization Admin.



**HID** The Trusted Source for Secure Identity Solutions

Home > Secure Identity Services

## HID Secure Identity Services Portal

HID Global offers industry expertise and a comprehensive suite of services to assist customers and channel partners to create, use and manage secure identities.

Log in to manage your HID Mobile Access™

User Name: rm.organization@grr.la Password: \*\*\*\*\* LOGIN

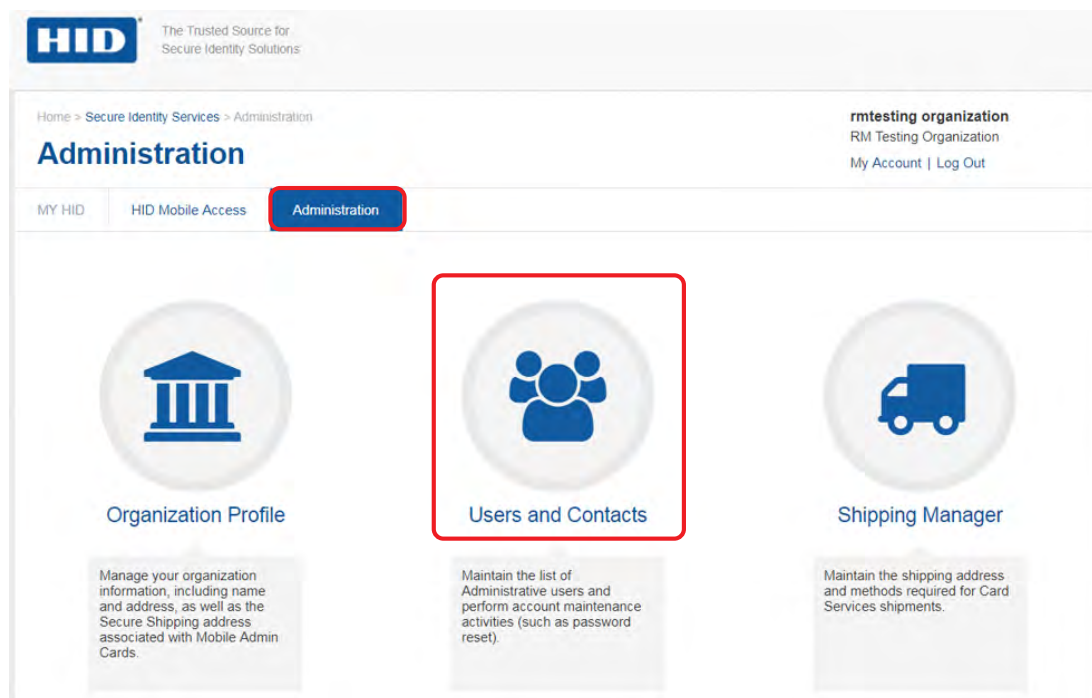
Forgot your password?

Difficulties logging in? Click here.

Support: Please visit the **HID Technical Support** to submit a case online or find the Technical Support contact information in your region.

NEED HELP?

2. Select the **Administration** tab.
3. Select **Users and Contacts**.



**HID** The Trusted Source for Secure Identity Solutions

Home > Secure Identity Services > Administration

## Administration

rmtesting organization  
RM Testing Organization  
My Account | Log Out

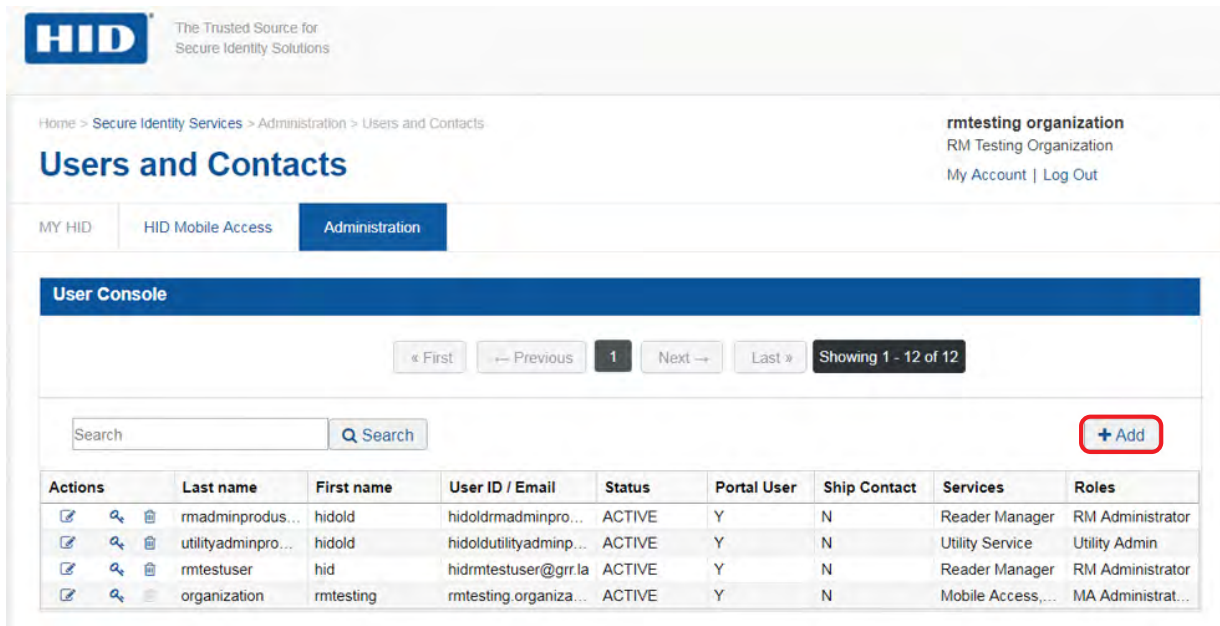
MY HID HID Mobile Access **Administration**

**Organization Profile**  
Manage your organization information, including name and address, as well as the Secure Shipping address associated with Mobile Admin Cards.













**Users and Contacts**  
Maintain the list of Administrative users and perform account maintenance activities (such as password reset).

**Shipping Manager**  
Maintain the shipping address and methods required for Card Services shipments.

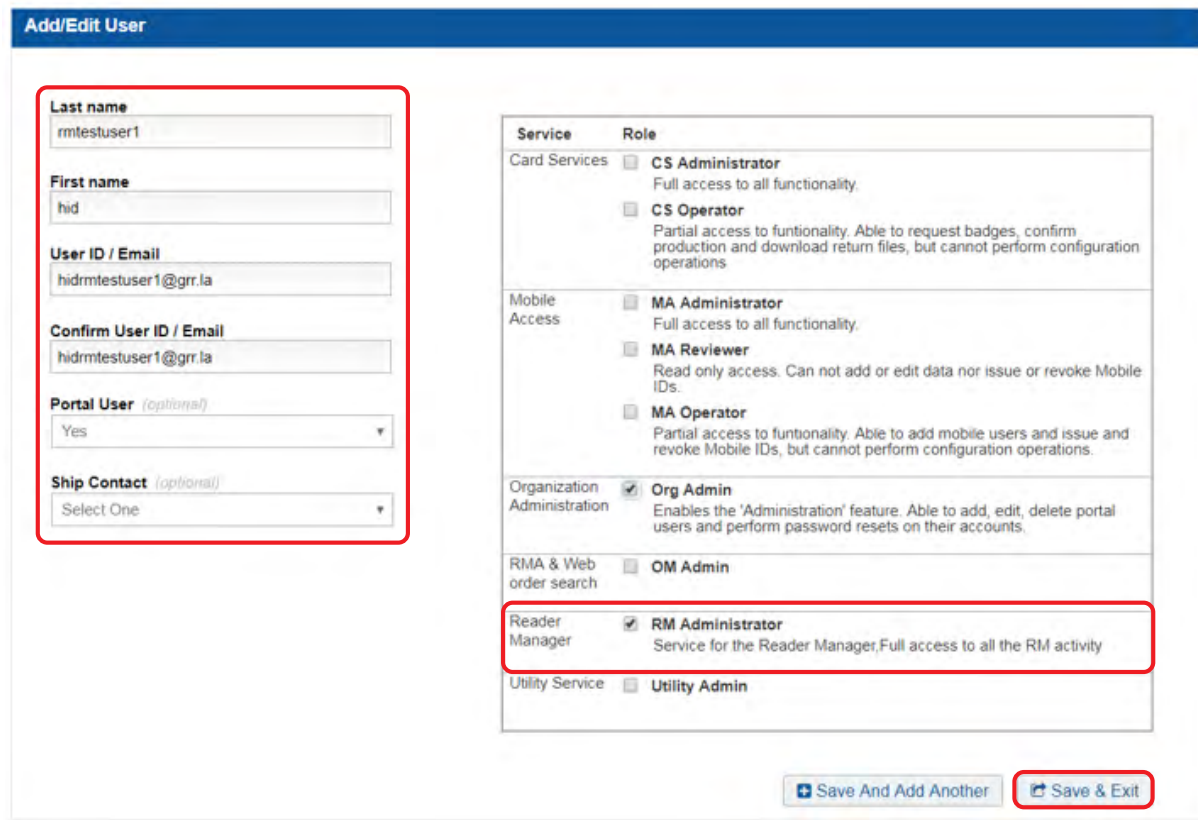
- In the **User Console** section click **Add**.



The screenshot shows the 'Users and Contacts' page in the HID Reader Manager Portal. The page has a navigation bar with 'MY HID', 'HID Mobile Access', and 'Administration'. The 'Administration' tab is selected. Below the navigation bar is the 'User Console' section. It includes a search bar, a '+ Add' button (highlighted with a red box), and a table of users.

Actions	Last name	First name	User ID / Email	Status	Portal User	Ship Contact	Services	Roles
  	rmadminprodus...	hidold	hidoldrmadminpro...	ACTIVE	Y	N	Reader Manager	RM Administrator
  	utilityadminpro...	hidold	hidoldutilityadminp...	ACTIVE	Y	N	Utility Service	Utility Admin
  	rmtestuser	hid	hidrmtestuser@grr.la	ACTIVE	Y	N	Reader Manager	RM Administrator
  	organization	rmtesting	rmtesting.organiza...	ACTIVE	Y	N	Mobile Access,...	MA Administrat...

- In the **Add/Edit User** section, enter the administrator details and select the **RM Administrator** option.
- Click **Save & Exit** and log out of the SIS Portal.



The screenshot shows the 'Add/Edit User' form. The form is divided into two main sections. The left section contains input fields for user details, and the right section contains a list of roles to select. The 'Last name' field is highlighted with a red box. The 'Role' section on the right is also highlighted with a red box, showing the 'RM Administrator' role selected.

**User Details:**

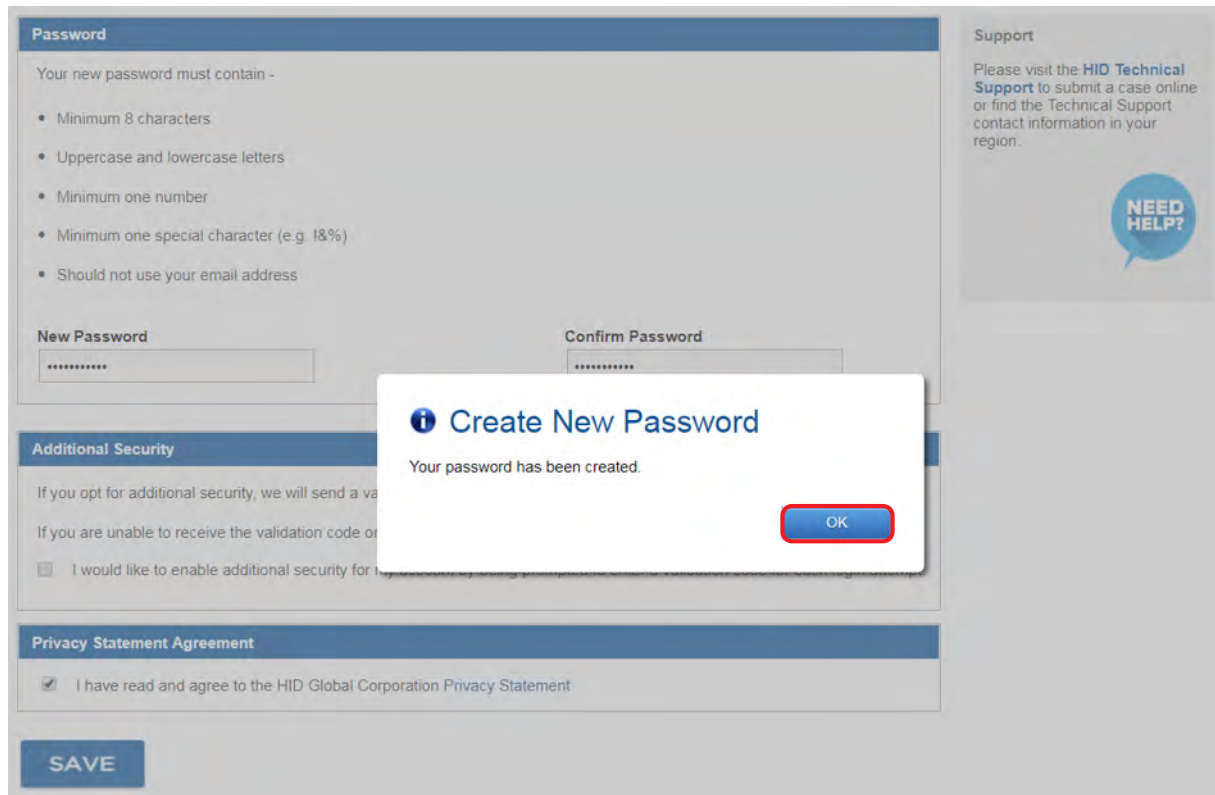
- Last name: rmtestuser1
- First name: hid
- User ID / Email: hidrmtestuser1@grr.la
- Confirm User ID / Email: hidrmtestuser1@grr.la
- Portal User (optional): Yes
- Ship Contact (optional): Select One

**Role Selection:**

Service	Role
Card Services	<input type="checkbox"/> <b>CS Administrator</b> Full access to all functionality.
	<input type="checkbox"/> <b>CS Operator</b> Partial access to functionality. Able to request badges, confirm production and download return files, but cannot perform configuration operations
Mobile Access	<input type="checkbox"/> <b>MA Administrator</b> Full access to all functionality.
	<input type="checkbox"/> <b>MA Reviewer</b> Read only access. Can not add or edit data nor issue or revoke Mobile IDs.
	<input type="checkbox"/> <b>MA Operator</b> Partial access to functionality. Able to add mobile users and issue and revoke Mobile IDs, but cannot perform configuration operations.
Organization Administration	<input checked="" type="checkbox"/> <b>Org Admin</b> Enables the 'Administration' feature. Able to add, edit, delete portal users and perform password resets on their accounts.
RMA & Web order search	<input type="checkbox"/> <b>OM Admin</b>
Reader Manager	<input checked="" type="checkbox"/> <b>RM Administrator</b> Service for the Reader Manager, Full access to all the RM activity
Utility Service	<input type="checkbox"/> <b>Utility Admin</b>

Buttons: **Save And Add Another**, **Save & Exit** (highlighted with a red box).

7. The newly created RM Administrator should check their email inbox for an email containing a username, a temporary password, and a SIS Portal landing page link. Click the **Here** link in the email to be directed to the SIS Portal landing page.
8. Log into the SIS Portal using the login details contained in the email. You are re-directed to the **Create New Password** page.
9. On the **Create New Password** 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 **OK** to log out of the SIS Portal.



**Password**

Your new password must contain -

- Minimum 8 characters
- Uppercase and lowercase letters
- Minimum one number
- Minimum one special character (e.g. !&%)
- Should not use your email address

New Password

Confirm Password

**Additional Security**

If you opt for additional security, we will send a validation code to your email address.

If you are unable to receive the validation code or you are unable to enter the validation code, you can contact Technical Support for assistance.

☐ I would like to enable additional security for my account.

**Privacy Statement Agreement**

☒ I have read and agree to the HID Global Corporation Privacy Statement

**SAVE**

**Support**

Please visit the **HID Technical Support** to submit a case online or find the Technical Support contact information in your region.

**NEED HELP?**


10. The RM Administrator can now log back into the SIS Portal using their new password. In the SIS Portal select the **HID Reader Manager** link.

Home > Secure Identity Services

## HID Secure Identity Services Portal




HID Global offers industry expertise and a comprehensive suite of services to assist customers and channel partners to create, use and manage secure identities.




### Card Services

Our Card Services application offers easy-to-use online tools to personalize and produce ID card badges -- whether you are looking to outsource the daily flow of requests or faced with the daunting task of re-badging thousands of employees.



### HID Mobile Access®

Our HID Mobile Access application allows you to easily issue and manage Mobile IDs for smart devices. The HID Mobile Access solution allows you to provision and revoke access rights over-the-air through this robust application.



### Online Order Status and RMA Requests

Our Order Status and RMA Request tool makes it possible for HID Direct Customers to check order status and request a Return Material Authorization (RMA) through an easy-to-use and secure online system.

HID SIS Administration

**Last Successful Login**  
Sep 17, 2018 14:47:16 (GMT)

[My Account](#) | [Log Out](#)

**HID Mobile Access**

[HID Reader Manager Administration](#)

#### RELATED DOCUMENTS

The agreements below are accepted during App installation:

- [HID Mobile Access end user license agreement \(Android\)](#)
- [HID Mobile Access end user license agreement \(iOS\)](#)
- [Privacy Policy for HID Mobile Access](#)

#### RELATED LINKS

[Frequently Asked Questions](#)

11. Click **YES** to be redirected to your organizations instance of the HID Reader Manager Portal.

### Redirecting to HID Reader Manager Portal

You will be transferred to the HID Reader Manager Portal in a new tab. You will be required to log in using your Secure Identity Services Portal account.

Do you want to continue?

NO

**YES**

12. Login as Reader Manager Administrator using the User name and new Password setup in the HID Secure Identity Services Portal.

Home

## HID Reader Manager Portal

Manage authorization of reader technicians for your HID Elite and HID Mobile Access readers

Need Assistance

Please visit the [HID Global Technical Support](#) to submit a case online or find the Technical Support contact information in your region.

[Research Knowledge Base >>](#)

Log in to manage your HID Readers.

User name	Password	LOGIN
<input type="text" value="rm.organization@grr.la"/>	<input type="password" value="*****"/>	

This page is intentionally left blank.

# Section 4

## 4 Troubleshooting

### 4.1 Reader Manager app messages

#### 4.1.1 Error 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 service. Please check mobile device Internet connection.
<i>"Issues at HID Servers, please try again."</i>	HID Reader Manager services are down. Please periodically try again and check your email for any service distribution notification.
<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 service is 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 Portal Administrator.
<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 Manager Portal 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. Please try again with the mobile device closer to the reader.

Message	Description and next step to attempt resolution
<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.
<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 Portal Administrator.
<i>"An unknown error has occurred."</i>	A general non-specific error has occurred. Please try again.

#### 4.1.2 Warning messages

Message	Description and next step to attempt resolution
<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 reenale, 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 OSDP and Bluetooth upgrade kit. See <i>Appendix A - iCLASS SE and multiCLASS SE Upgrade Kits</i>
<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.

### 4.1.3 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>"Invitation Code was successfully accepted"</i>	The entered invitation code is valid and the invitation is successfully redeemed by the user.
<i>"No reader found"</i>	No readers nearby reader found during Scan for iCLASS SE® Readers. 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 inspected.
<i>"Reader was successfully upgraded"</i>	Reader firmware upgrade has successfully completed.
<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.

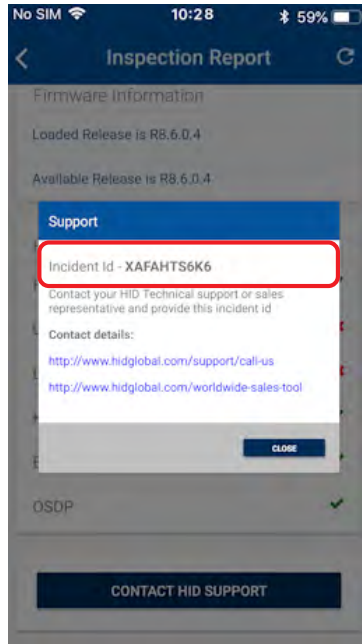
### 4.1.4 Validation messages

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 &amp; 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. The **Inspection Report** screen, tap **CONTACT HID SUPPORT**.
2. Take a note of the displayed **Incident Id** number and contact your HID Technical Support or Sales Representative.



# Appendix A

## A Reader upgrade

### A.1 iCLASS SE and multiCLASS SE Bluetooth and OSDP Upgrade Kit

The iCLASS SE® and multiCLASS SE® Bluetooth and OSDP Upgrade Kit allows for readers which do not currently support Bluetooth or OSDP to be upgraded to support these technologies.

#### A.1.1 Verify reader compatibility

The HID Reader Manager solution is only compatible with iCLASS SE and multiCLASS SE, Rev E readers. 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 already “Mobile-ready” or “Mobile-enabled”, with the list of compatible readers at:

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

#### A.1.2 iCLASS SE and multiCLASS SE Upgrade Kits

If your reader does not already have bluetooth capability you will need to upgrade the reader using the iCLASS SE and multiCLASS SE Bluetooth and OSDP upgrade kit. Depending on the reader model the following upgrade kits are available.

**Note:** These cannot be used on pivCLASS or Rev. A iCLASS SE/multiCLASS SE readers.

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

### A.1.3 iCLASS SE and multiCLASS SE Bluetooth and 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 module as it will be replaced.

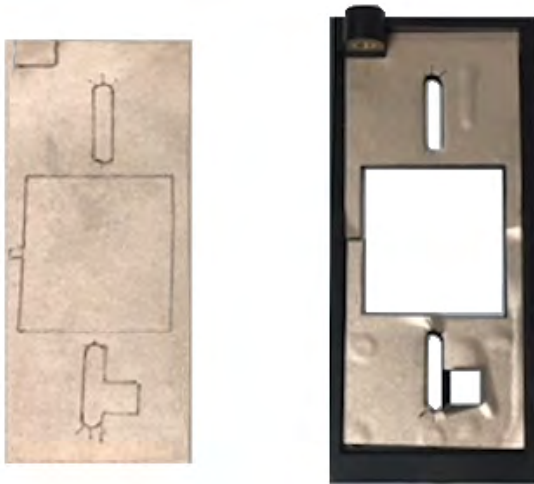


4. Insert the upgrade module into the expansion slot. Take care not to touch the expansion slot with anything apart from the module as this could remove the colorless anti-corrosive compound.



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.

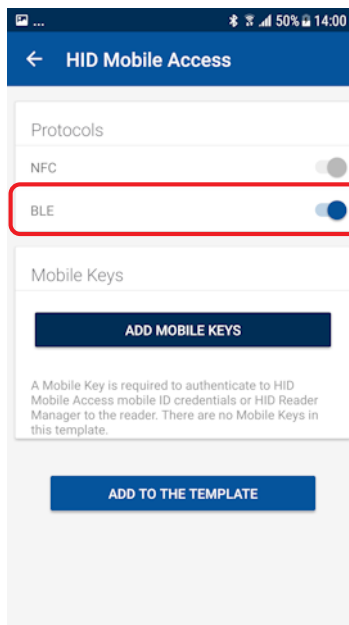
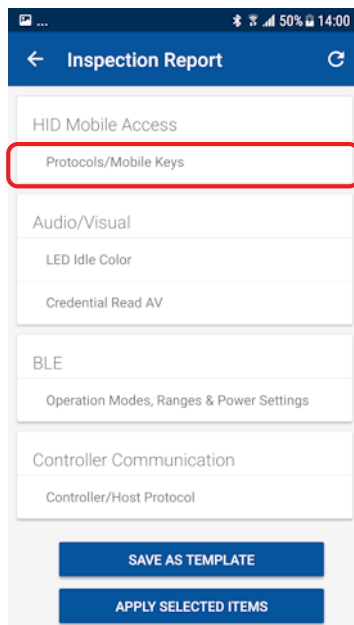
**Note:** Different conductors are used for wiegand vs OSDP communication.

### A.1.3.1 Configure reader in HID Reader Manager

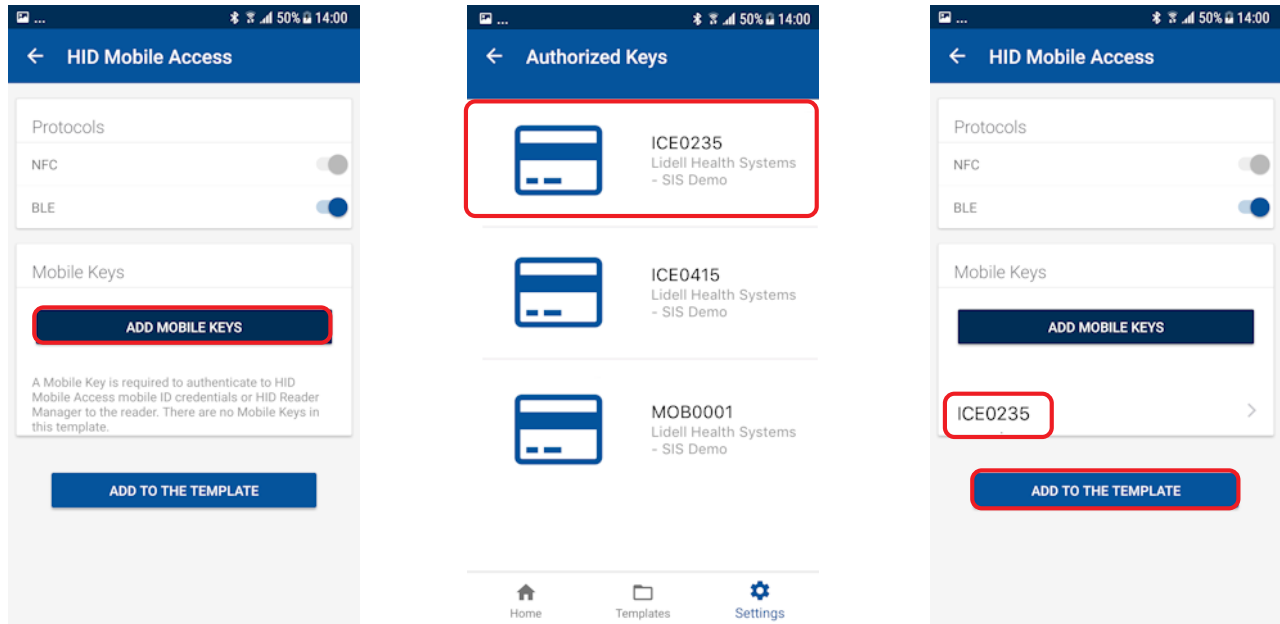
If the reader is ready to be configured use the following procedure to configure the reader to support Bluetooth for HID Mobile Access and/or OSDP controller communication.

**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 Portal. See *Section 2 HID Reader Manager mobile application*.

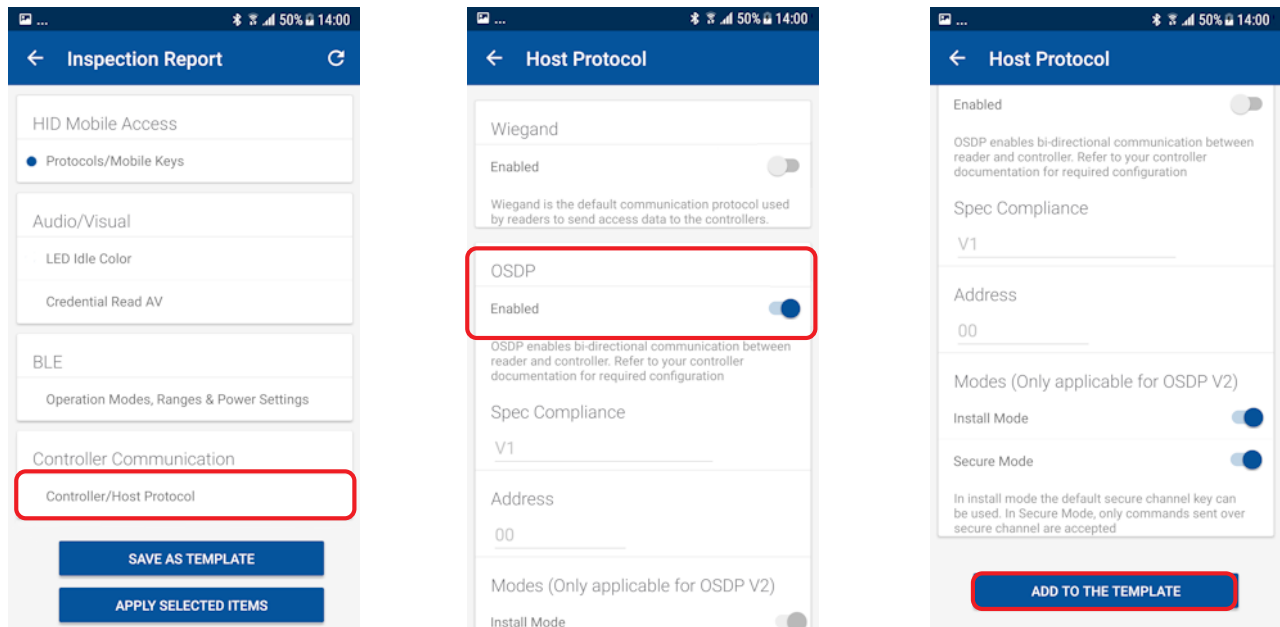
1. Log into the HID Reader Manager app.
2. Connect the HID Reader Manager app to the reader. See *Section 2.3.3 Connect to a reader*.
3. In the HID Reader Manager app inspect the reader configuration and, if indicated, upgrade the reader firmware. See *Section 2.3.4 Reader inspection report*.
4. To configure the reader to support Bluetooth for HID Mobile Access and/or OSDP controller communication, on the **Inspection Report** screen tap **Inspect Detailed Configuration**.
5. Tap **Protocols/Mobile Keys** in the **HID Mobile Access** section.
6. Enable the **BLE** option in the **Protocols** section.



7. Tap **ADD MOBILE KEYS** and select the required authorization key to be loaded onto the reader. The selected authorization key will be listed on the screen.
8. Tap **ADD TO THE TEMPLATE** to save.

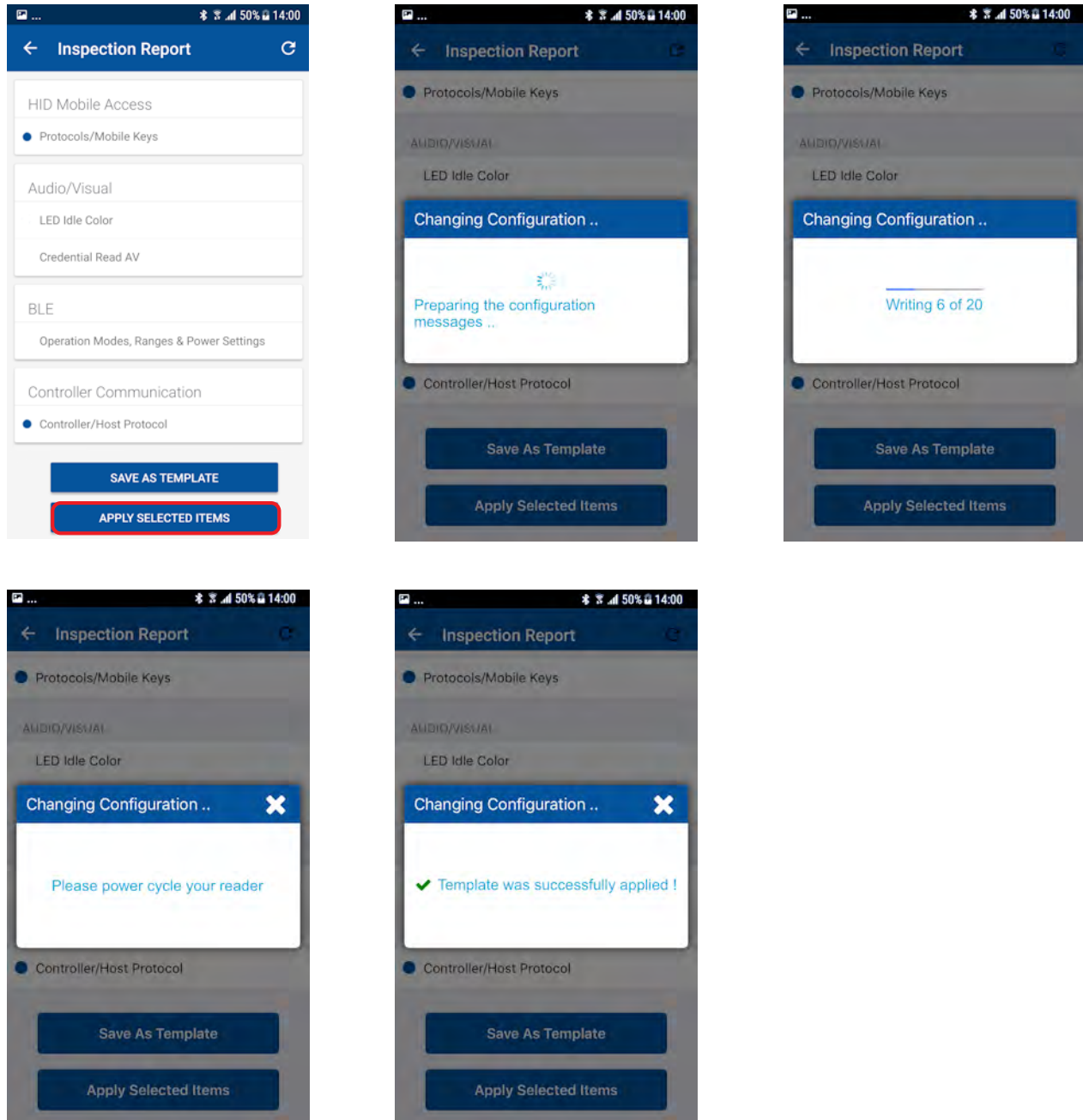


9. To configure the reader for OSDP controller communication (optional) tap **Controller/Host Protocol**, in the **Controller Communication** section.
10. Enable the **OSDP** option and tap **ADD TO THE TEMPLATE** to save.



11. Tap **APPLY SELECTED ITEMS** on the **Inspection Report** screen. 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.



12. Test configuration changes, see *Section 2.2.1 Test configuration changes*.

## B Release notes

---

### B.1 HID Reader Manager release feature summary

The HID Reader Manager application intends to deliver a solution that will enable select iCLASS SE® and multiCLASS SE® readers to be upgraded in the field via BLE communication with a mobile device. This solution aims to deliver an enhanced user experience to the current method of using multiple configuration cards with only Reader LED status providing feedback on the status. Additionally, the solution will provide inspection, configuration and BLE tuning functionality. The following sections provide details on features included in this release.

#### B.1.1 HID Reader Manager app 1.0 release items

HID Reader Manager app supports the following functionality:

- Locating - able to scan and locate reader for communication
- Inspection - able to inspect reader hardware, firmware, and configuration details
- Configuration changes - able to apply reader configuration changes
- Firmware Upgrade - able to upgrade reader firmware

#### B.1.2 HID Reader Manager Portal release items

HID Reader Manager Portal supports the following functionality:

- Enroll a Reader Technician in the Portal for an organization
- Send only Invitation to the registered Reader Technician
- Send Invitation and Key at once to the Reader Technician
- Revoke key authorization from a mobile device
- Delete a Reader Technician mobile device
- View the list of deleted Reader Technicians
- Select and export the Reader Technicians associated with an organization
- Enable authorization for additional keys with validity period
- View the list of current and deleted mobile devices

## B.2 HID Reader Manager release limitations summary

### B.2.1 HID Reader Manager app 1.0

HID Reader Manager app known release limitations:

- BLE stability. Due to inherent differences in the technology stacks used in mobile devices, not all devices work consistently.
- Readers upgraded from Standard to HID Elite™ or custom reader admin keys (SNMP) using configuration cards are not supported.
- Supported firmware releases:

Reader Firmware	Admin Configuration	Supported?
R8.2.2	ICE	No
R8.3.0	Standard	No
R8.3.0	ICE/MOB	No
R8.3.1.6	Standard	No
R8.3.1.6	ICE/MOB	No
R8.3.2.1	Standard	No
R8.3.2.1	ICE/MOB	No
R8.4.0.6	Standard	Yes
R8.4.0.6	ICE/MOB	Yes
R8.4.1.0	Standard	Yes
R8.4.1.0	ICE/MOB	Yes
R8.4.2.0	Standard	Yes
R8.4.2.1	ICE/MOB	Yes
R8.5.0.9	Standard	Yes
R8.5.0.9	ICE/MOB	Yes
R8.6.0.4	Standard	Yes
R8.6.0.4	ICE/MOB	Yes

For full details of compatibility with the current version of the app, visit:

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

### B.2.2 HID Reader Manager Portal 5.1.0

HID Reader Manager Portal known release limitations:

- HID Reader Manager Portal 5.1.0 has not been tested with the Safari browser (Windows and MacOS). For full details of compatibility with the current version, visit:

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

- A user who has enrolled as a Reader Technician in the mobile application cannot be enrolled as an Administrator in the Reader Manager or Mobile Access Portal with the same email ID.

If access is required for the Reader Manager mobile applications, enroll first in either the Mobile Access or Reader Manager portal and then the Reader Manager Mobile Application.

**Note:** If a user is already enrolled in the Reader Manager mobile application and Reader Manager portal access is required, please contact HID Global technical support.

This page is intentionally left blank.

# 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 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.
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 Secure Identity Services 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.

Term	Description
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 Portal 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.
Tap	The Tap gesture with mobile device for door opening. The Tap operation is typically used when the mobile device is in close proximity to the reader. Approximately 0 inch to 4 inches (0 cm to 10 cm).
Twist an Go	The Twist gesture with mobile device for door opening. The Twist operation is typically used when the mobile device is at a longer distance from the reader. Approximately 1 ft to 10 ft (0.3 m to 3 m).

This page is intentionally left blank.

