HID® Reader Manager™ Solution

User Guide (iOS)

PLT-03683, A.4
May 2020

Powering
Trusted Identities

Copyright

Trademarks

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

MIFARE, MIFARE DESFire, and MIFARE Classic are registered trademarks of NXP Semiconductors N.V. and are used under license.

Contacts

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

Americas and Corporate	**Asia Pacific**
611 Center Ridge Drive Austin, TX 78753 USA Phone: +1 866 607 7339	19/F 625 King's Road North Point, Island East Hong Kong Phone: +852 3160 9833
Europe, Middle East and Africa (EMEA)	**Brazil**
3 Cae Gwyrdd Green Meadow Springs Cardiff CF15 7AB United Kingdom Phone: +44 (0) 2920 528 500	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**.

What's new

The major changes introduced in this reissue of the *HID Reader Manager Solution User Guide (iOS)*, are described below:

Section	Description
All	Updates throughout document for HID Reader Manager 1.4.0.

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

Section 01
Introduction

Powering
Trusted Identities

1.1 Document purpose

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

- Download and install the HID Reader Manager mobile app.
- Register and authenticate the HID Reader Manager app on a mobile device.
- Enroll Reader Technicians and issue Authorization Keys in the HID Reader Manager Portal.
- Change reader configurations for supported iCLASS SE®/multiCLASS SE® readers, the iCLASS SE® Express R10 reader and HID® Signo™ readers.
- Update reader firmware for supported iCLASS SE/multiCLASS SE readers, the iCLASS SE® Express R10 reader, and HID Signo 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 HID Reader Manager app.
  - Self-registration within the HID 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.

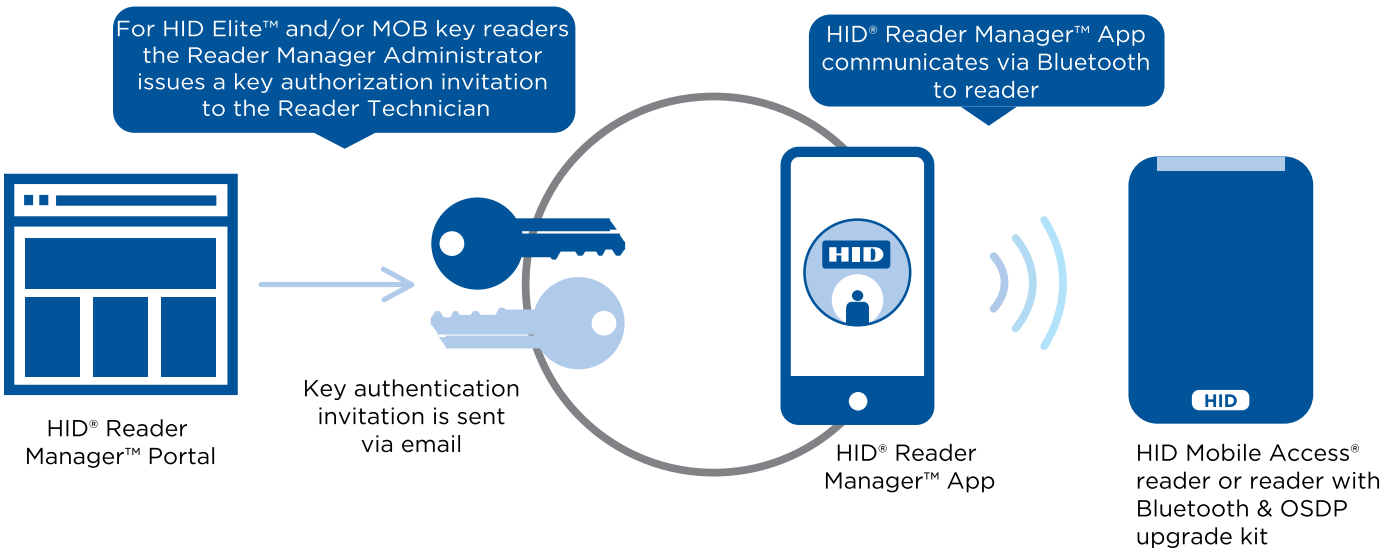
1.3 HID Reader Manager solution overview

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, BLE read range settings), upgrade firmware, inspect connected reader status and extend functionality on supported iCLASS SE/multiCLASS SE readers, the iCLASS SE Express R10 reader and HID Signo readers. The main components of the HID Reader Manager solution are:

- **HID Reader Manager Application:** Mobile app which connects, via Bluetooth, to a reader for configuration changes, firmware upgrades and reader inspections by Reader Technicians.
- **HID Reader Manager Portal:** Web Portal which facilitates Reader Technicians to use the HID Reader Manager App 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 App 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 App to upgrade readers to support Bluetooth and/or Open Supervised Device Protocol (OSDP). For more information, see **Appendix 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/multiCLASS SE readers, the iCLASS SE Express R10 reader and HID Signo 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/multiCLASS SE Rev E readers (with Bluetooth & OSDP module installed), the iCLASS SE Express R10 reader and HID Signo 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”.

For details on supported firmware versions, refer to **Appendix Reader upgrade**.

1.4.2 Mobile devices

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

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

Section 02

HID Reader Manager App

Powering
Trusted Identities

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 overview

2.1.1 Prerequisites

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

- A Mobile Access account is established for the organization through the HID Global onboarding process. See **Mobile Access setup**.
- A HID Reader Manager Portal instance is available for the Organization. See **Reader Manager Portal setup**.
- A Reader Manager Administrator has been setup and enabled for the Organization's Reader Manager Portal instance.

2.1.2 HID Reader Manager setup overview

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

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

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

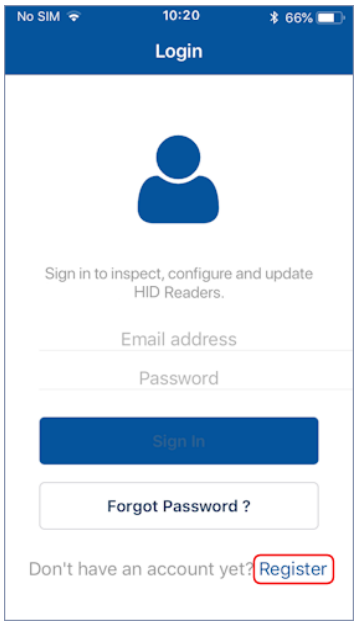
1. The Reader Manager Administrator enrolls the Reader Technician in the HID Reader Manager Portal and issues an invitation code and key authorization. See **HID Reader Manager Portal**.
2. The Reader Technician activates the issued invitation code in the HID Reader Manager app. See **Activate the HID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

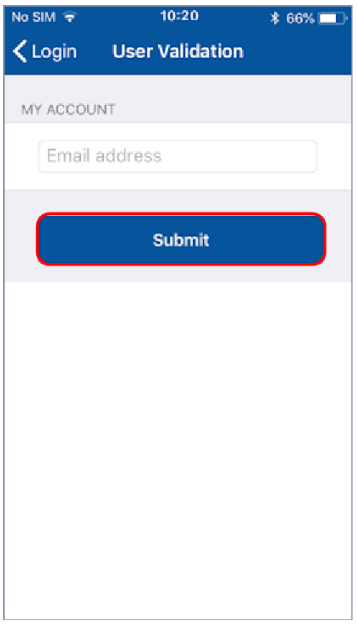
2.1.3 Download and install the Reader Manager app

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

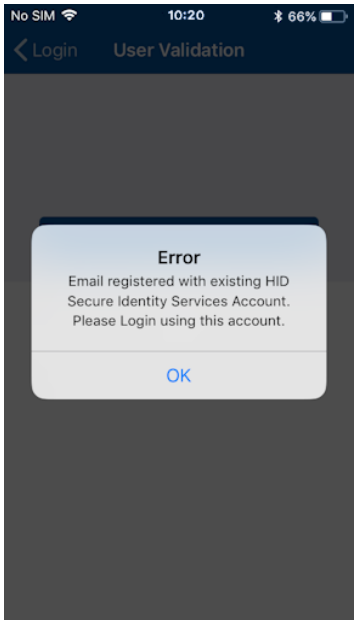
2.1.4 Register a new account within the app

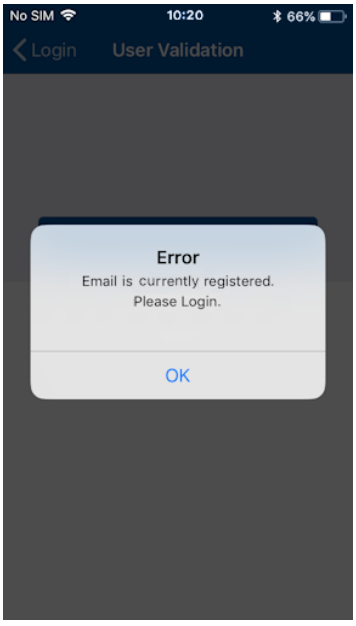
1. Open the HID Reader Manager app on your mobile device.
2. On the **Login** screen, tap the **Register** link.
3. On the **User Validation** screen, enter your email address and tap **Submit**.





Note: If the entered email address is associated with an existing HID Origo™ Management Portal account 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 **Log into the HID Reader Manager app**.

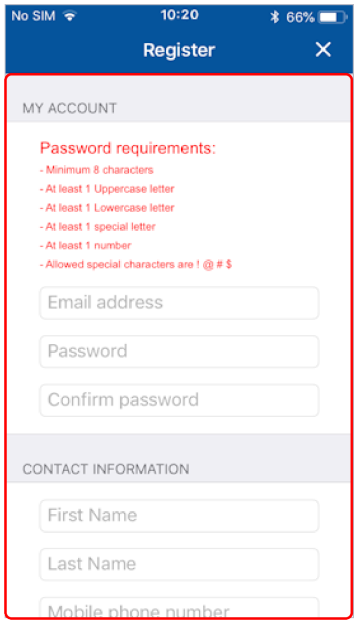


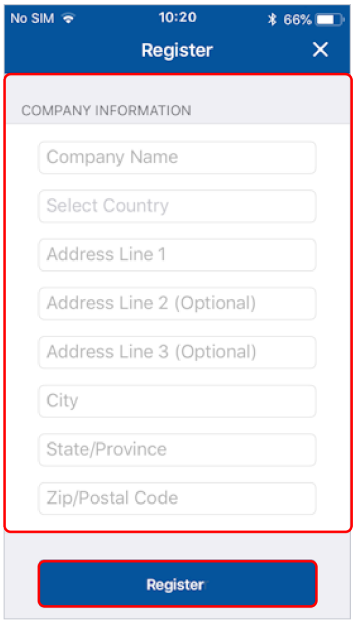


4. On the **License** screen, read the privacy polices and license agreements and tap **AGREE**.

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

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



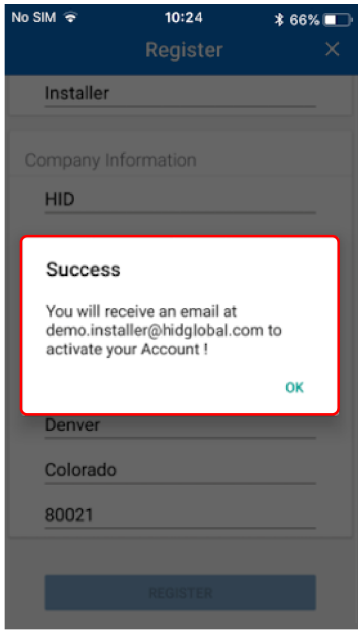


6. After receiving a **Success** prompt, tap **OK**.

7. Check your registered email account for a HID Reader Manager email containing an activation link. Click the activation link in the email.

   Note: The activation link has an expiry date which is indicated in the email.

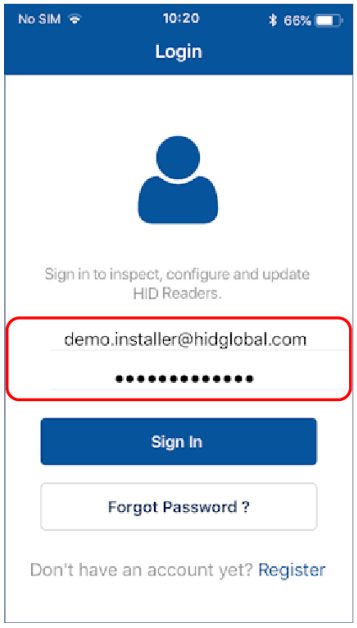
8. A successful activation message will appear in a new browser. You can now log into the HID Reader Manager app using the registered email address and password.

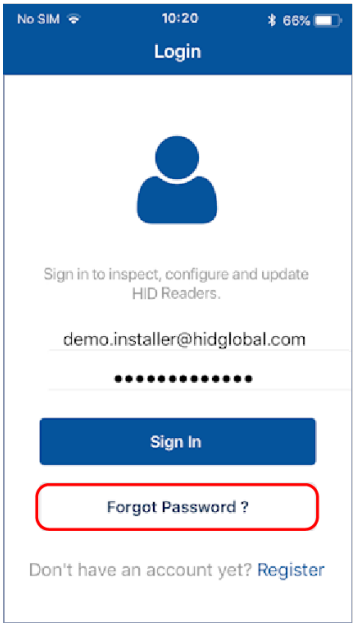


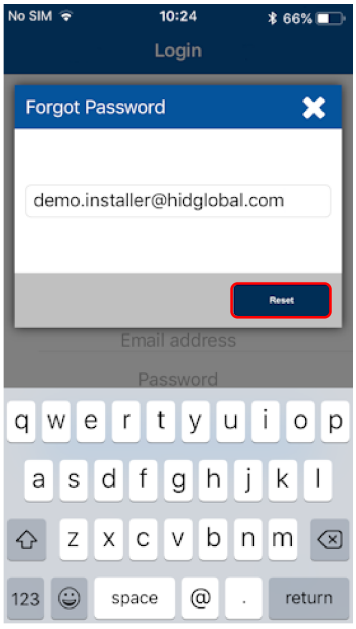
2.1.5 Log into the HID Reader Manager app

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.

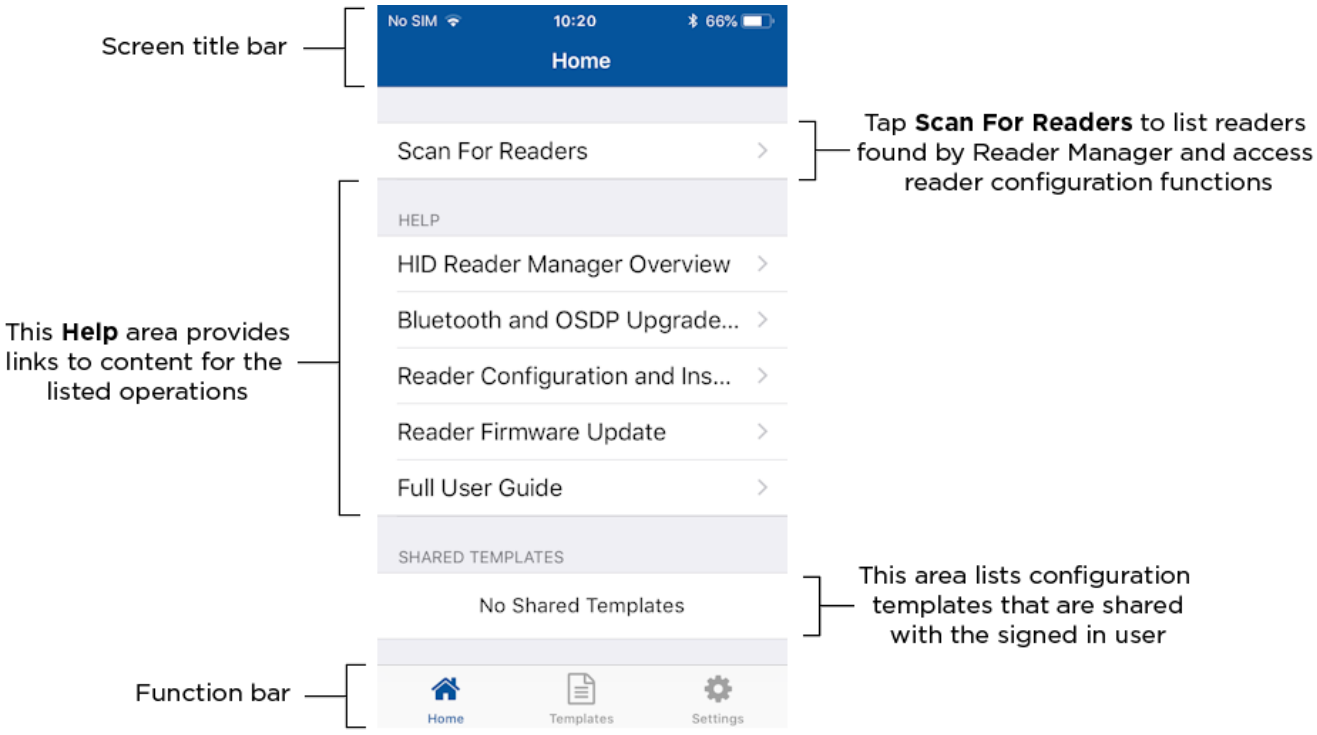
Note: If you have forgotten your login password, tap **Forgot Password?**. Enter your email address and tap **Reset**. Your password will be reset through the management portal therefore check your registered mail account for a password reset notification email.







Home screen layout



2.1.6 Activate the HID Reader Manager app

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

Prior to activating the HID Reader Manager app, the Reader Manager Administrator must enroll the Reader Technician within the HID Reader Manager Portal. See **Enroll a Reader Technician**.

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

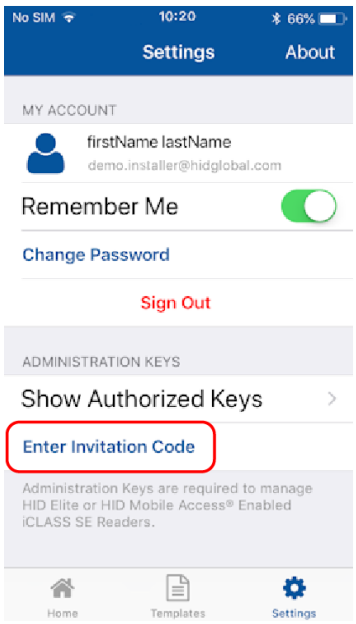
To activate an invitation code in the HID Reader Manager app:

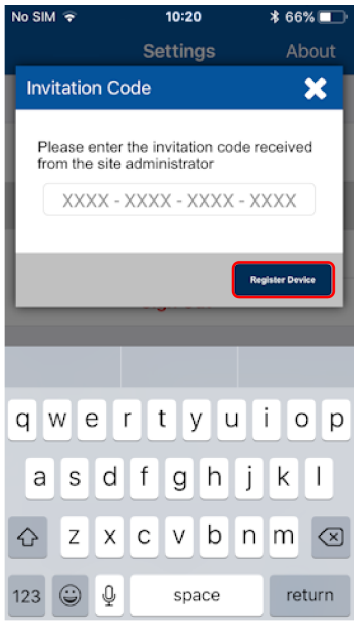
1. Log into the HID Reader Manager app using your registered email and password.
2. On the **Home** screen, tap the **Settings** icon.
3. Open the invitation email on the device and tap the invitation link. The invitation code will be automatically entered in the Reader Manager App.

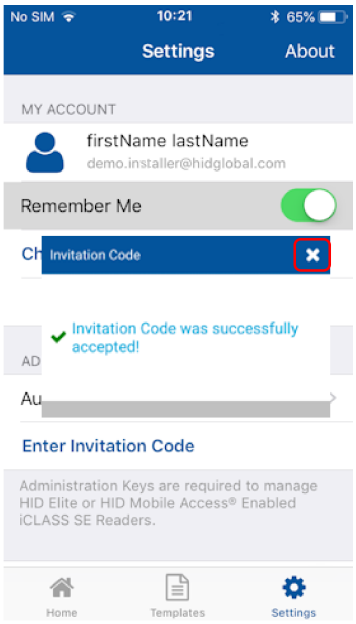
   Alternatively, manually enter the invitation code by tapping **Enter Invitation Code** on the **Settings** screen.
4. Tap **Register Device**.

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

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







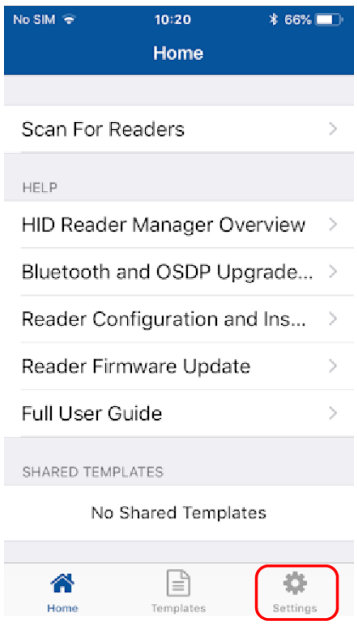
2.1.7 Display authorized keys

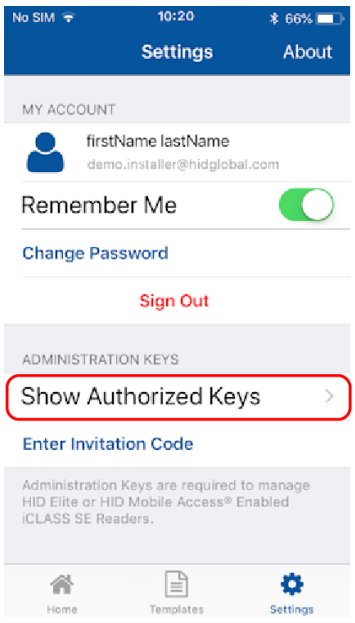
Note: This section does not apply to Standard Key readers as these do not use HID Elite and/or MOB Keys.

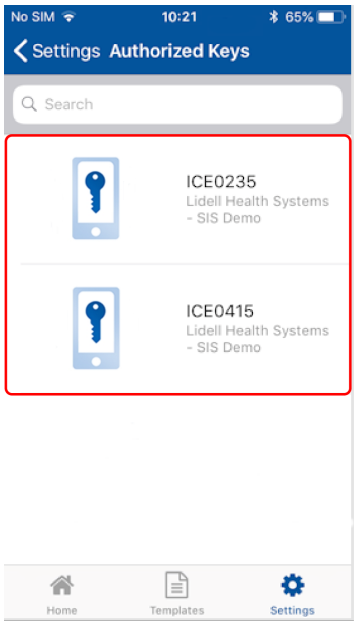
Authorized keys issued via the Reader Manager portal can be viewed in the Reader Manager app:

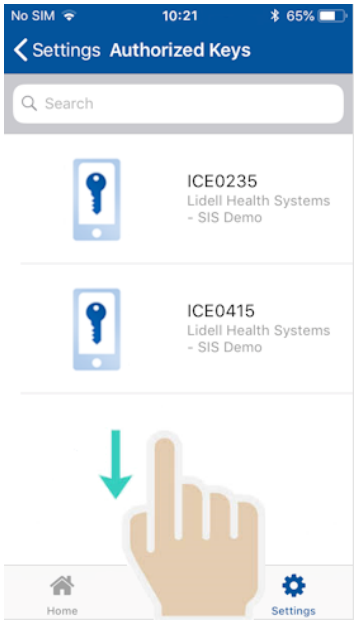
1. On the **Home** screen, tap the **Settings** icon .
2. Tap **Show Authorized Keys** to display authorized keys.

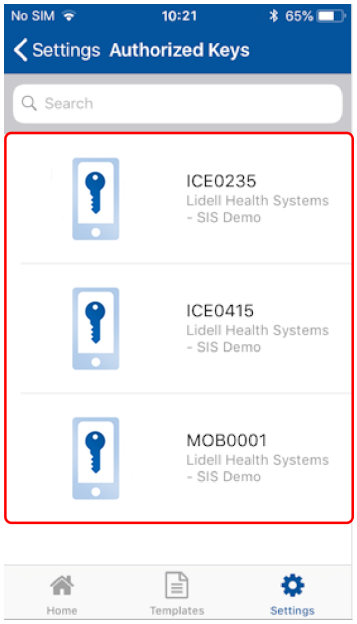
   Note: Authorized keys are added the app memory and will only be visible after a screen refresh. If an authorized key is not displayed swipe down to refresh the screen.





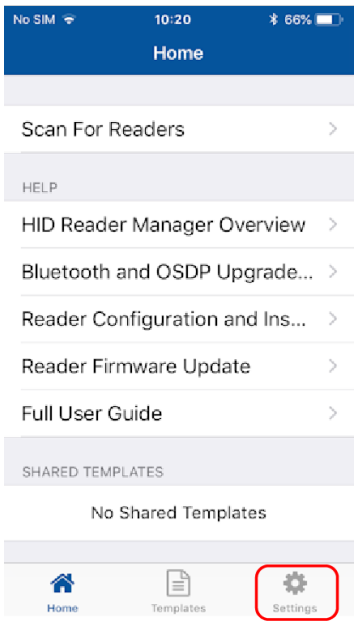


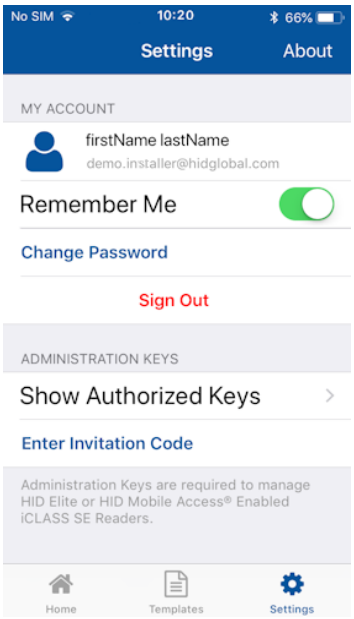




2.1.8 HID Reader Manager app settings

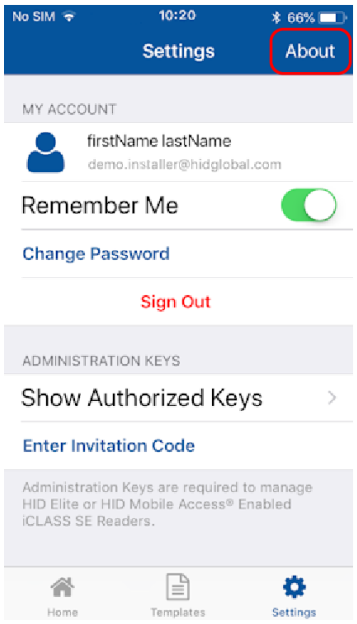
On the **Home** screen, tap the **Settings** icon to access HID Reader Manager app settings.

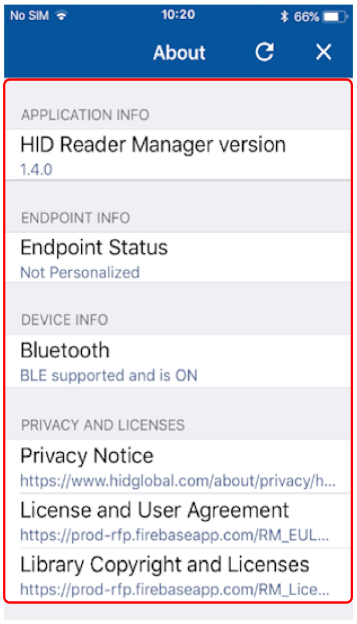




About HID Reader Manager

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

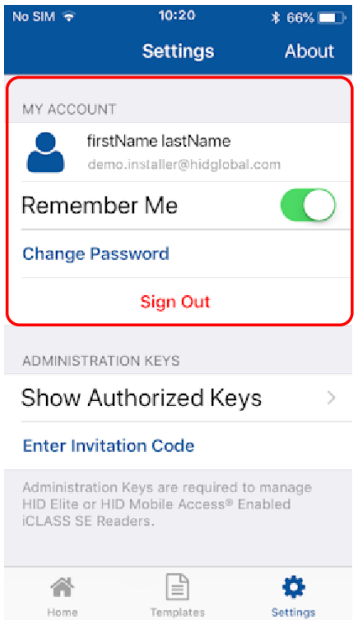


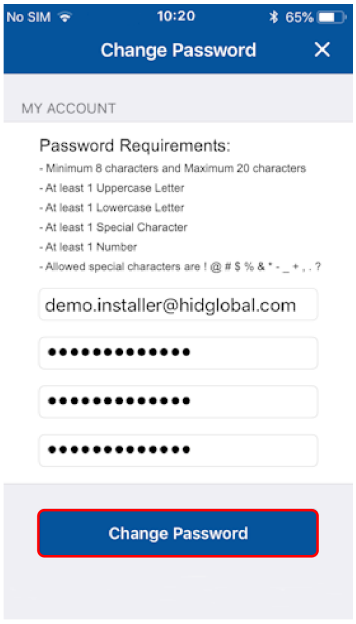


My Account

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 to access the **Change Password** screen. Enter a new app login password (refer to the on screen password requirements) and tap **Change Password**.
- **Sign Out:** tap to exit the app.





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 enter and activate the issued invitation code in the HID Reader Manager app.

2.2 Reader configuration

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

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

1. The Reader Technician checks the reader firmware version and, if necessary, performs a reader firmware upgrade. See **Firmware upgrade**.
2. The Reader Technician creates a configuration template to simplify programming the reader. See **Create a new template**.
3. The Reader Technician applies the created configuration template to the reader. See **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 confirm communication with the reader and BLE operations perform as configured.
- If you have loaded any mobile keys, ensure that all credentials work at the reader.

2.3 Basic app functionality

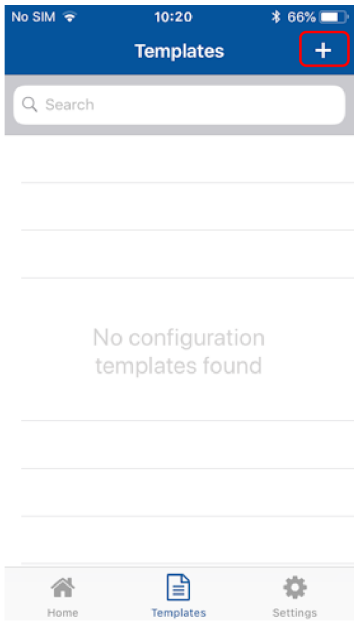
2.3.1 Create a new template

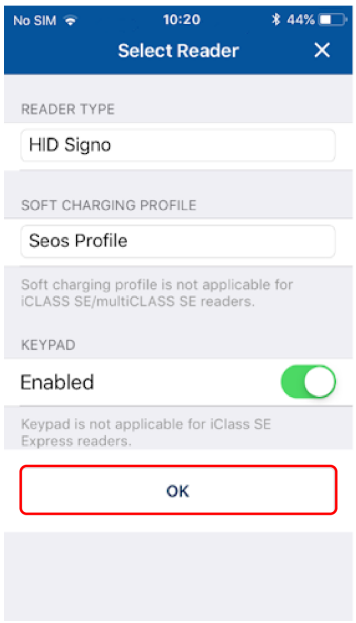
Templates store reader settings. When a template is created it can be applied to multiple readers that require the same configuration or shared with other Technicians to speed up the configuration of multiple readers.

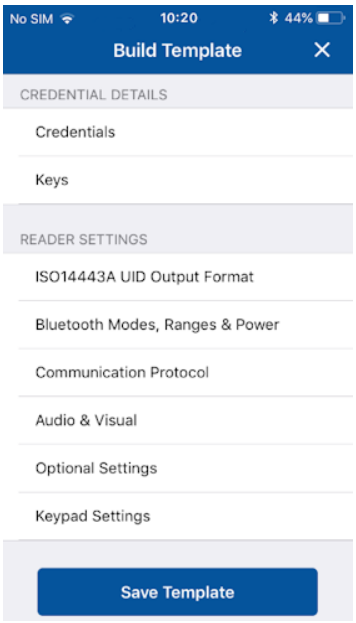
To create a new template:

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

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



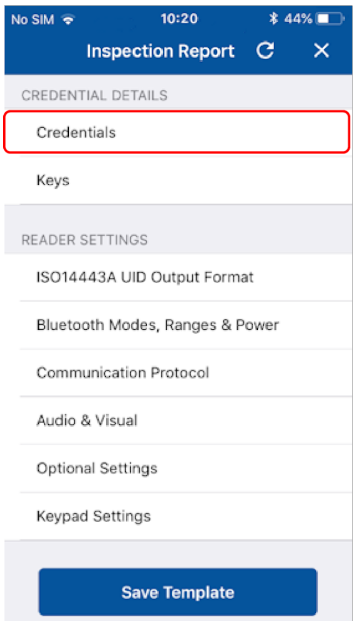


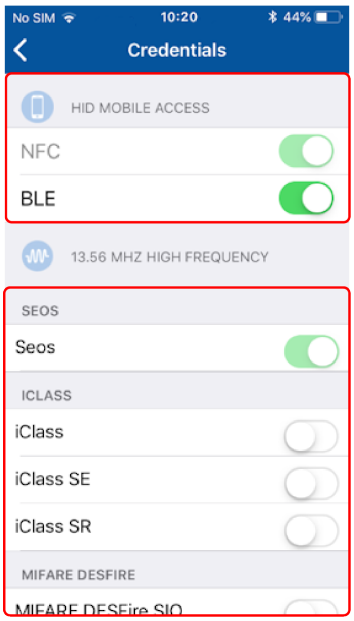


Credential settings

1. From the **CREDENTIAL DETAILS** section, tap **Credentials**.
2. Select the required communication protocol option and enable/disable the required credential types.

   Note: For the iCLASS SE Express reader BLE, MIFARE® DESFire® UID, and MIFARE Classic® UID settings can only be changed if the reader was initially configured with these options when ordered.
3. Tap **Add to the template** to save.

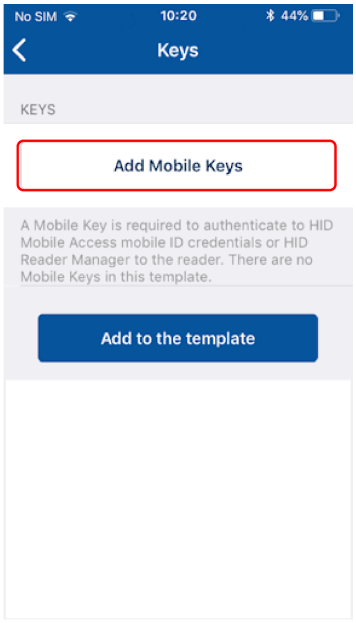


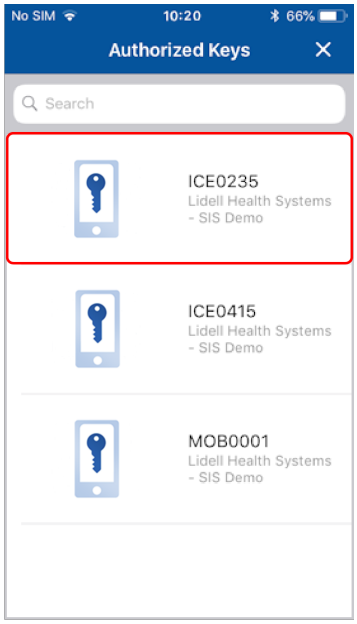


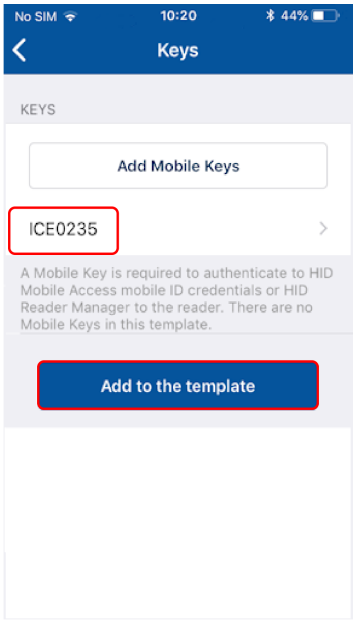
Add Mobile Keys

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

   Note: For the iCLASS SE Express reader BLE, MIFARE® DESFire® UID, and MIFARE Classic® UID settings can only be changed if the reader was initially configured with these options when ordered.
4. Tap **Add to the template** to save.



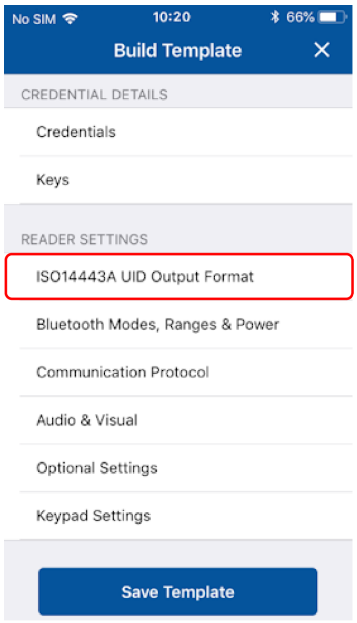


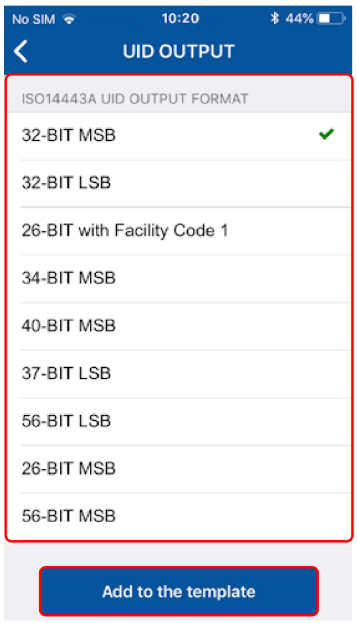


ISO14443A UID Output Format settings

Note: For iCLASS SE Express R10 readers, ISO14443A UID Output Format configuration settings are only valid for certain soft charging profiles.

1. From the **READER SETTINGS** section, tap **ISO14443A UID Output Format**.
2. Select output format from the displayed list.
3. Tap **Add to the template** to save.

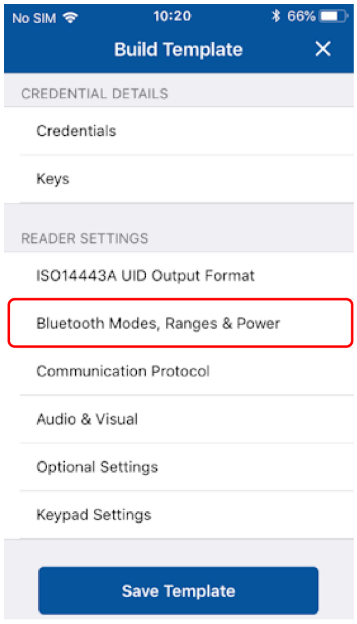


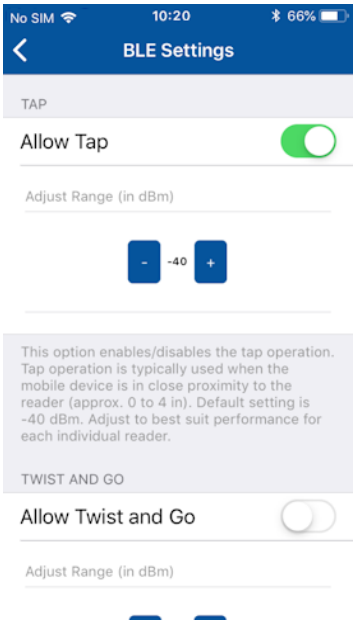


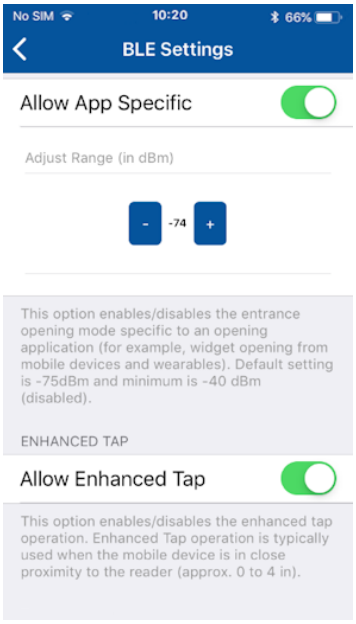
Bluetooth Modes, Ranges & Power settings

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

   Note: Default range value information is provided for each opening operation on the **BLE Settings** screen.







4. The default **Transmit Power** setting (-4 dBm) should not be exceeded unless absolutely necessary. In certain installations a higher or lower **Transmit Power** may be required, however this setting should only be adjusted if the **Range** settings do not result in the desired read range.
5. Tap **Add to the template** to save.

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

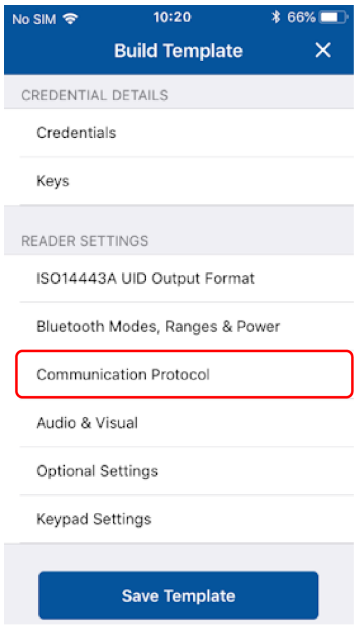
As opening ranges deviate between different mobile devices, you should always test and fine tune settings for a specific site. The Read Range settings listed below provide a starting point for common locations:

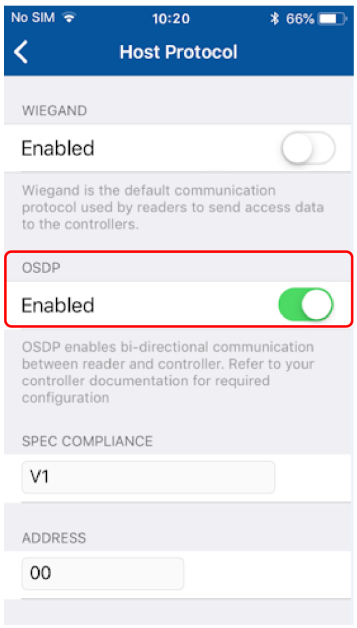
Location	Tap	Twist and Go
Office environment	-48 dBm	-67 dBm
Elevators	-40 dBm	-57 dBm
Outdoor entrances	-48 dBm	-67 dBm
Garage (user inside vehicle)	-53 dBm	-74 dBm

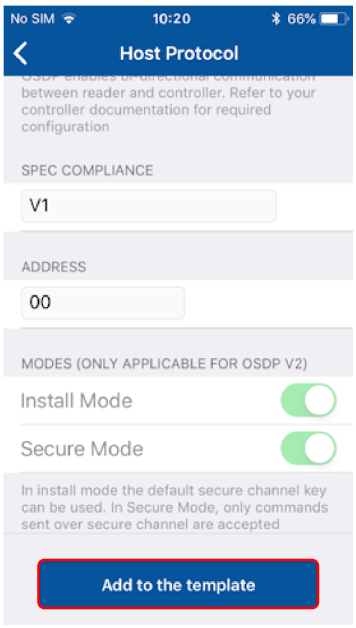
Communication Protocol settings

1. From the **READER SETTINGS** section, tap **Communication Protocol**.
2. Enable the required Reader to Controller communication protocol. This can be set as **Wiegand** or **OSDP** (not both).

   Note: OSDP is not applicable to iCLASS SE Express R10 readers as these readers are Wiegand capable only.
3. Tap **Add to the template** to save.

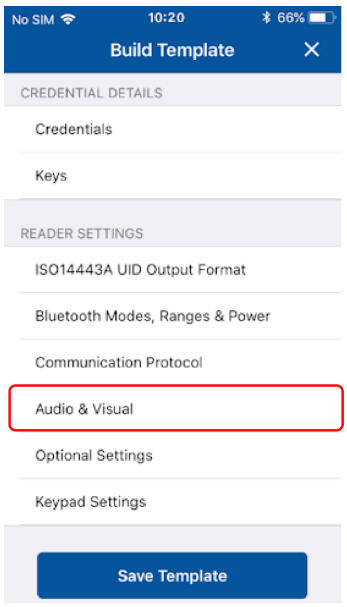


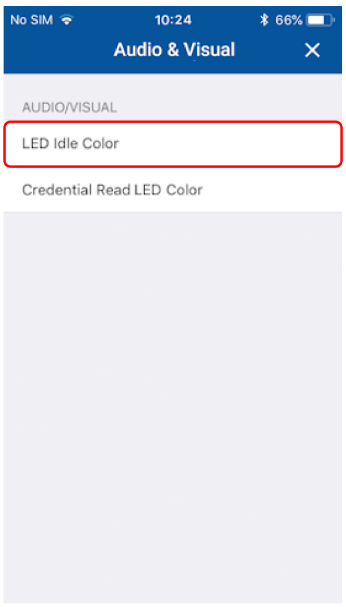


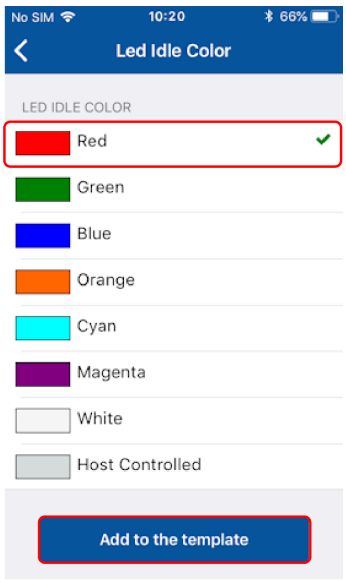


Audio & Visual settings

1. From the **READER SETTINGS** section, tap **Audio & Visual**.
2. From the **AUDIO/VISUAL** section, tap **LED Idle Color**.
3. Select a color and tap **Add to the template**.
   Note: Idle LED Color selections for HID Signo and iCLASS SE Express R10 readers are **Red** or **Blue**.

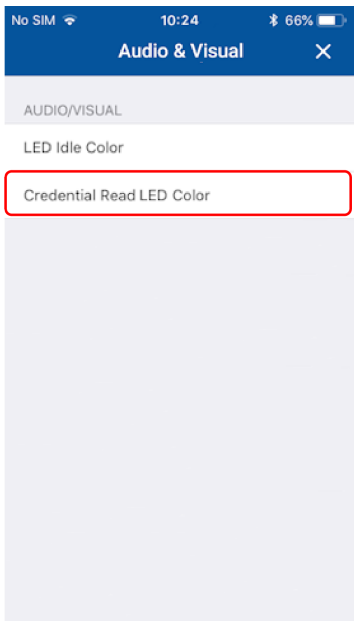


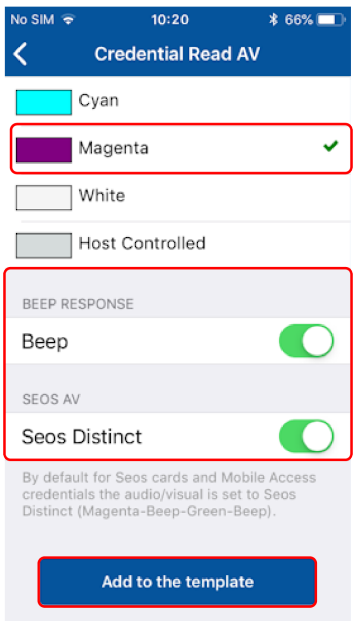




4. Tap **Credential Read LED Color**.
5. Select a color and enable/disable the **BEEP RESPONSE** and **SEOS AV** settings using the options. Tap **Add to the template** to save.

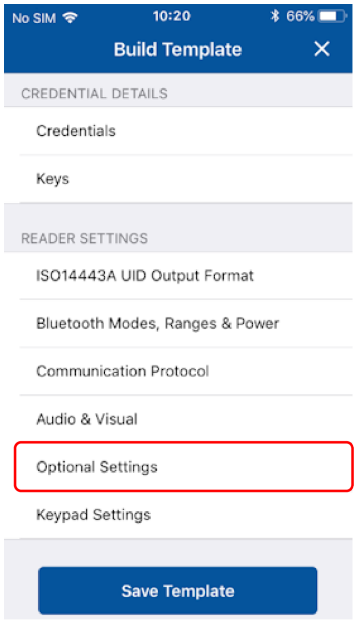
   Note: Credential Read Led Color selections for HID Signo and iCLASS SE Express R10 readers are **Green** or **No Response**.

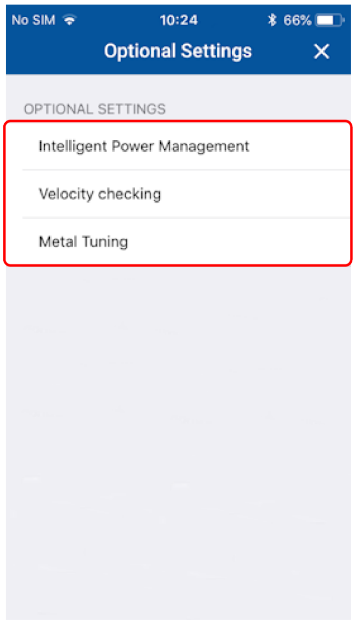


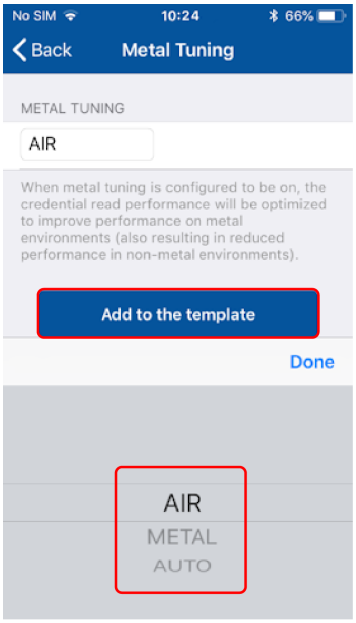


Optional Settings

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



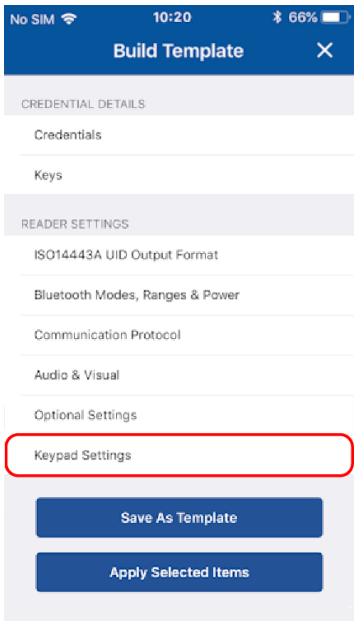


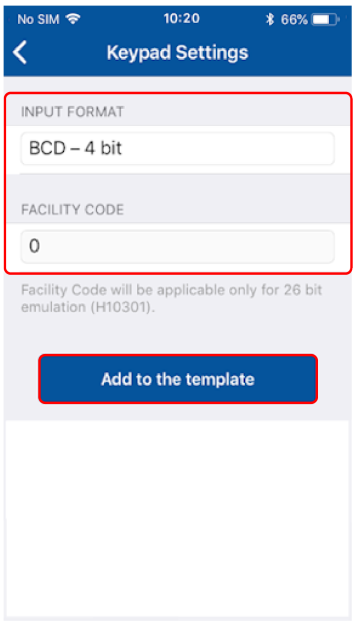


Keypad Settings

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

1. From the **READER SETTINGS** section, tap **Keypad Settings**.
2. Select an available **INPUT FORMAT** and, if applicable, enter a **FACILITY CODE**.
3. Tap **Add to the Template** for any changed settings.





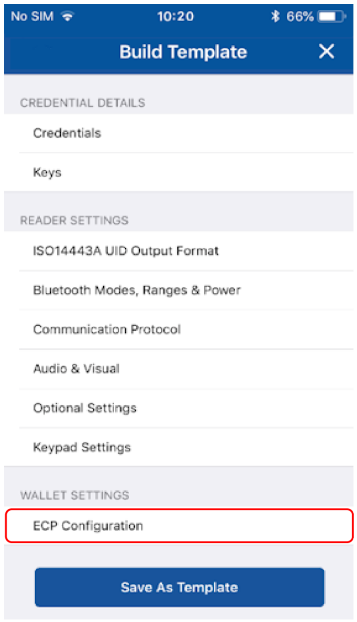
Wallet Settings

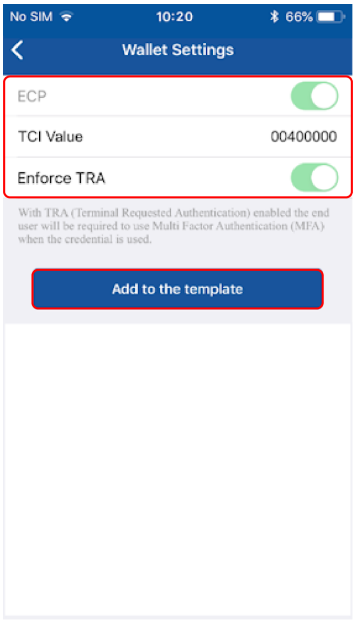
Enabling ECP (Enhanced Contactless Polling) will allow Wallet keys to get pushed along with Mobile Access keys. The following reader configuration specifications apply:

- Wallet settings are only applicable for MOB/ICE Readers.
- Wallet settings are only supported in HID iCLASS/multiCLASS SE Readers running firmware Version 8.9 and above. HID iCLASS/multiCLASS SE Readers running firmware below Version 8.8 must be upgraded to firmware Version 8.9 for Wallet settings to be supported.
- Wallet settings are supported in HID Signo readers by default for all firmware versions.

If the reader configuration supports Wallet settings:

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





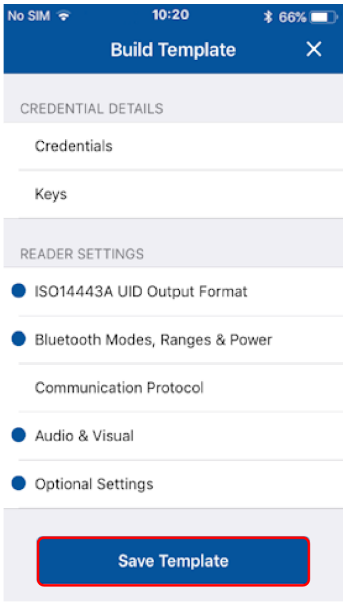
2.3.2 Manage templates

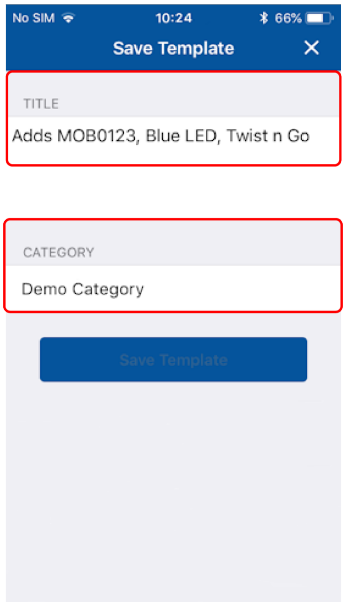
Save a new template

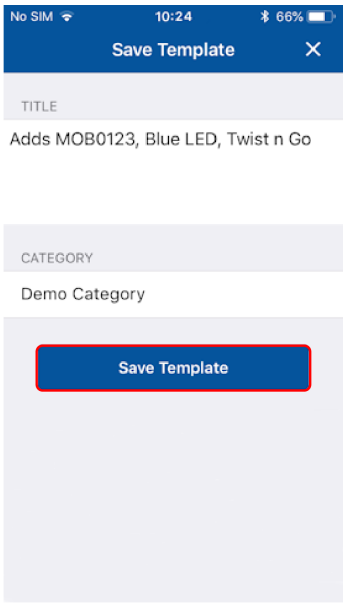
1. When configuration settings are selected and added to the template, tap **Save Template**.
2. Tap in the **TITLE** area and enter a title for the template.
3. Tap in the **CATEGORY** area and tap **Select Category**. Select an existing category from the displayed list or add a new category and select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

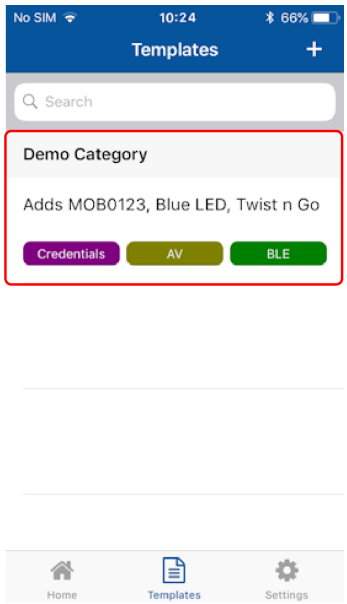
   Note: A category must be selected before the template can be saved.

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





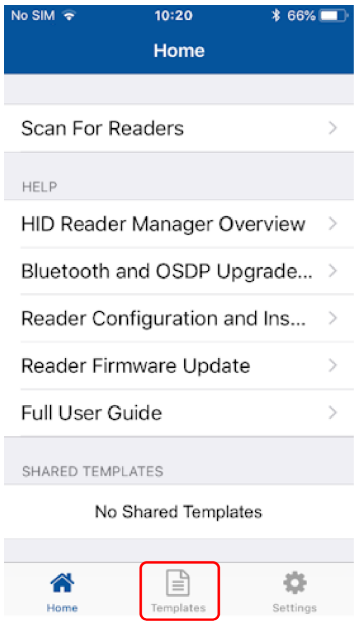


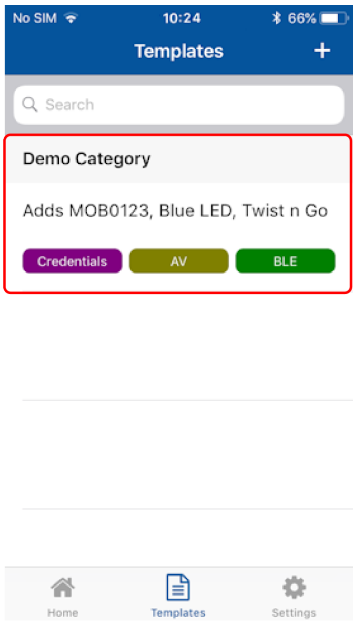


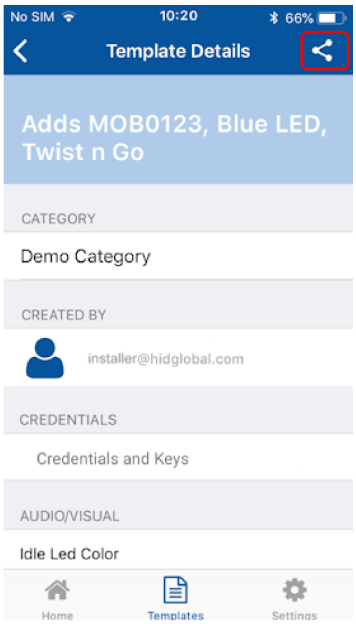
Share a template

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

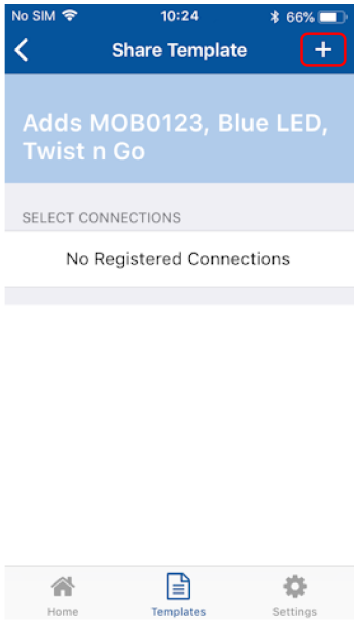
1. On the **Home** screen, tap the **Templates** icon and select a displayed template to be shared. On the **Template Details** screen tap the share icon [ ].

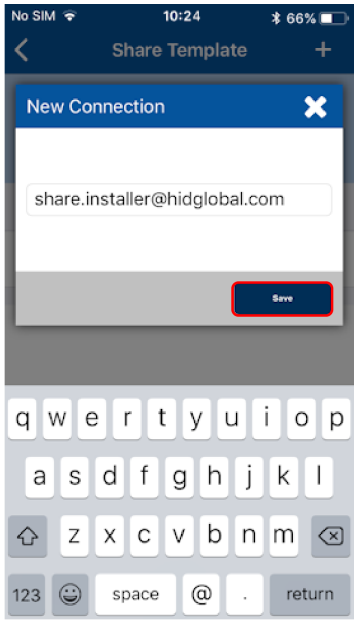


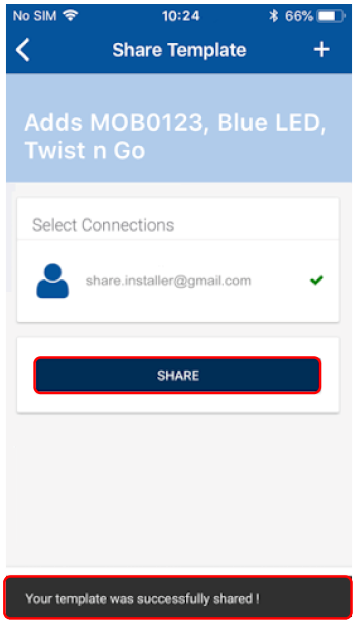




2. Tap the plus icon [ ] and, in the **New Connection** box, enter the email address of another Technician (this can be any Technician that is already registered). Tap **Save**.
3. When the connection has been made, tap **SHARE**. A message will appear at the bottom of the screen to indicate success.

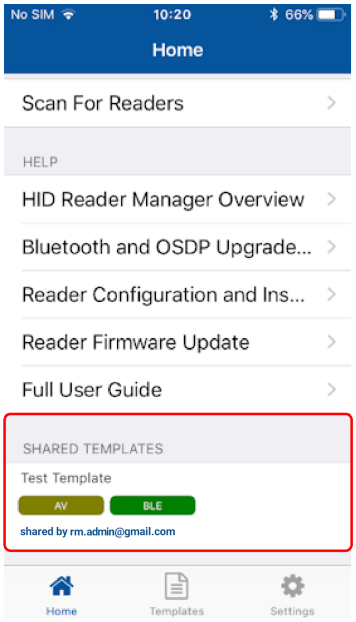


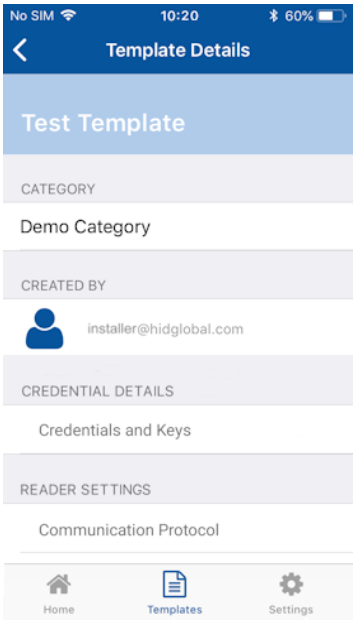




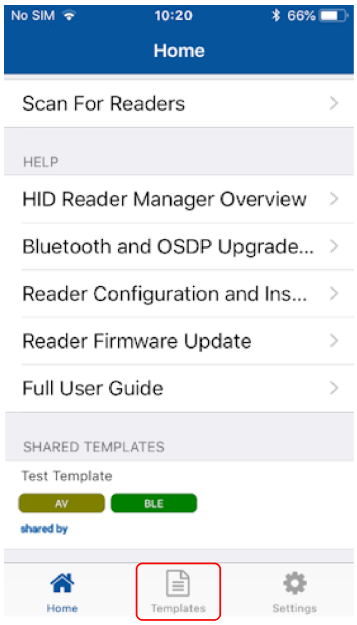
Display template details

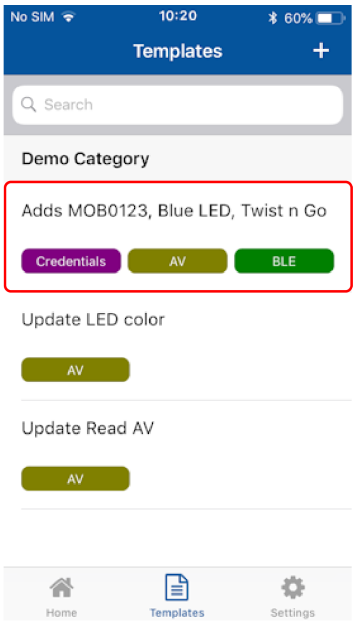
Configuration templates shared with a Reader Technician that is logged into HID Reader Manager app are displayed in the **SHARED TEMPLATES** area on the **Home** screen. Tap on a displayed shared template to view the template details.

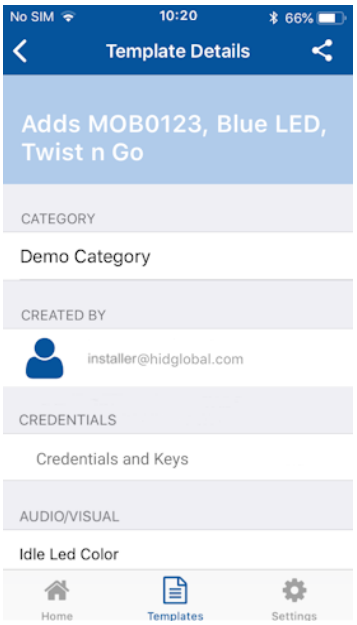




To view the list of created templates tap the **Templates** icon on the HID Reader Manager Home screen. Existing templates are listed on the **Templates** screen. Tap on a displayed template to view the template details.



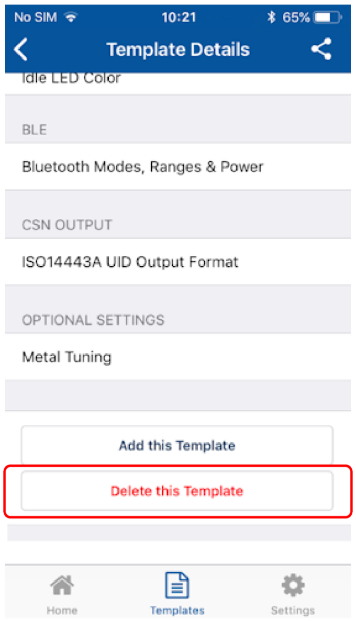


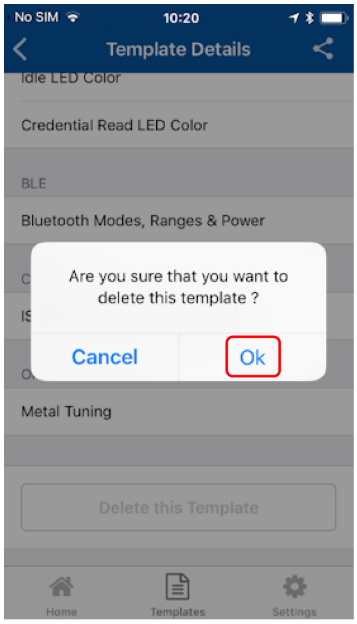


Delete a template

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

1. Swipe down to the bottom of the **Template Details** screen and tap **Delete this Template**.
2. Tap **OK** to delete the template.

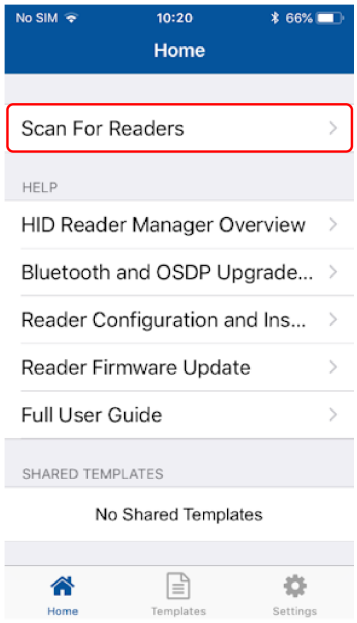


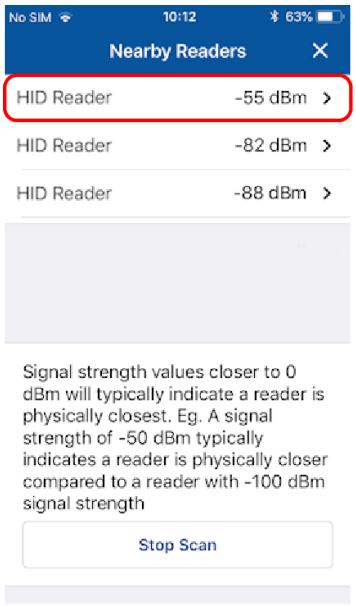


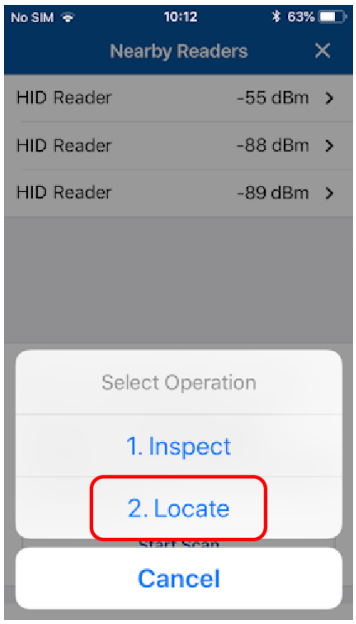
2.3.3 Connect to a reader

1. On the HID Reader Manager **Home** screen, tap **Scan For Readers**. This will scan for nearby Mobile Access® readers (i.e. readers with either the BLE Communication module installed or readers that are already “Mobile-ready” or "Mobile-enabled").

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

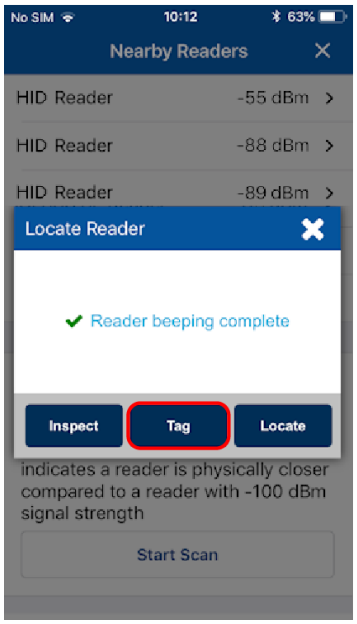


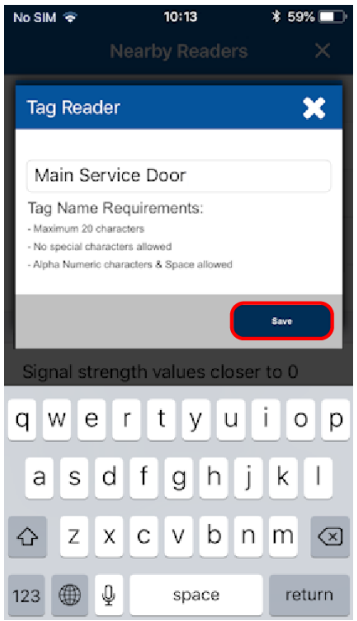


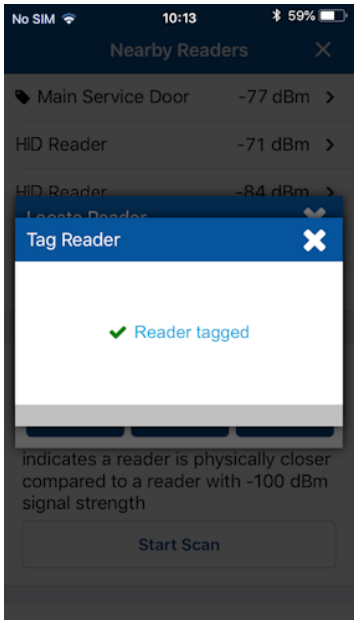


3. If you wish to name the reader for easier identification, tap **Tag**, enter a name (for example, the reader location), and tap **Save**.

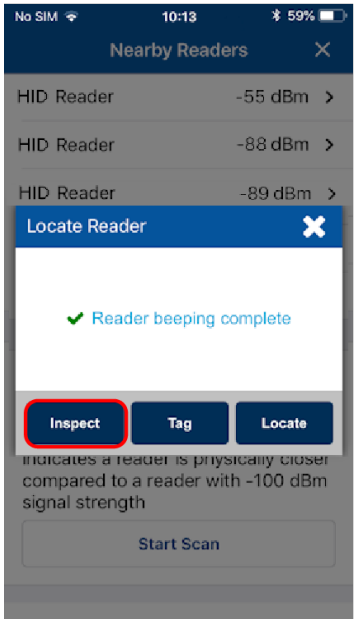
   Note: The tagged reader name is only visible on your mobile device.

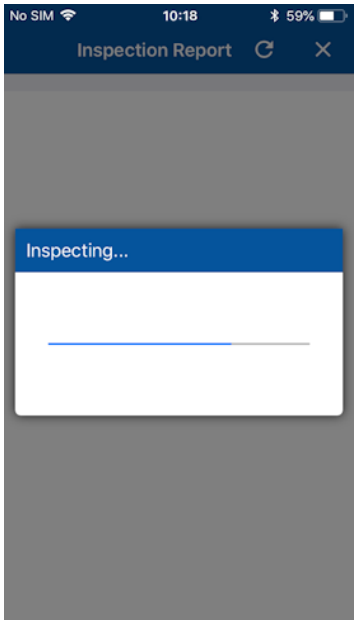


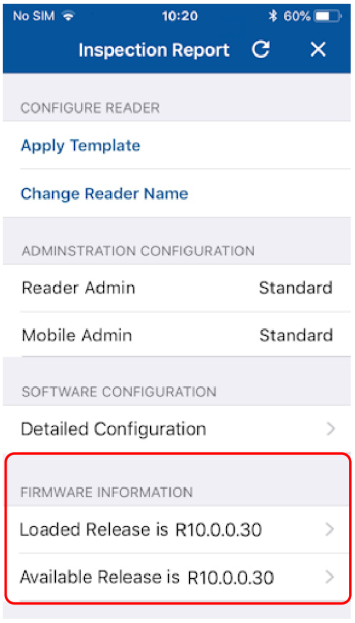




4. Tap **Inspect**. The reader is now connected and reader information is displayed on the **Inspection Report** screen, see **Reader inspection report**.







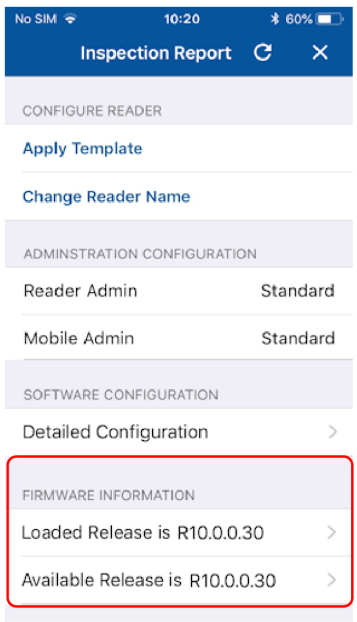
2.3.4 Reader inspection report

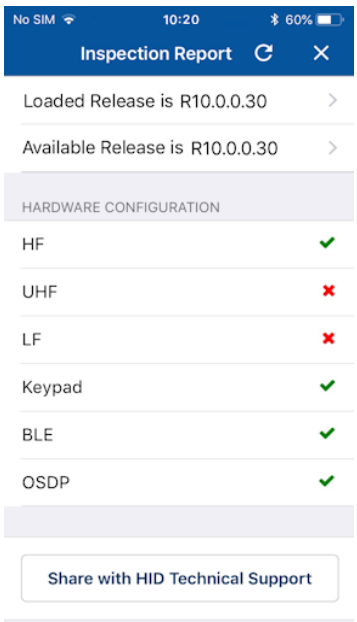
The **Inspection Report** screen displays configuration details for a connected reader and allows you to carry out the following:

- View reader **Firmware Information** and, if necessary, perform a reader **Firmware Upgrade**. See **Firmware upgrade**.
- Tap **Detailed Configuration** to access detailed reader settings, modify settings and directly apply them to the reader. See **View detailed reader configuration**.
- Configure the reader:
  - Tap **Apply Template** to select and apply template configuration settings to the reader. See **Apply configuration changes**.

    Note: Before applying a template, inspect the reader with the Reader Manager app to determine available configuration settings. Only include valid configurations in the template definition.
  - Tap **Change Reader Name** to assign a name to the reader. See **Change reader name**.

    Note: Only iCLASS SE/multiCLASS SE readers support the assignment of a reader name.
- Tap **Share with HID Technical 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 **Contact HID Technical Support**.

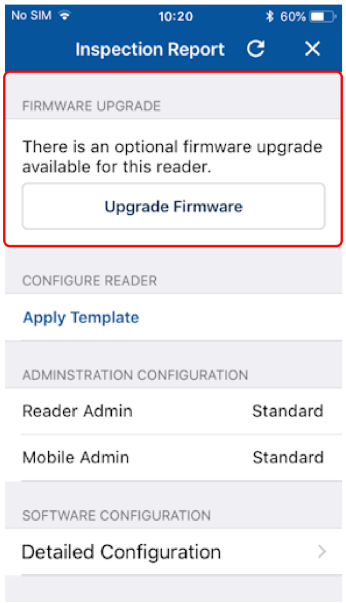


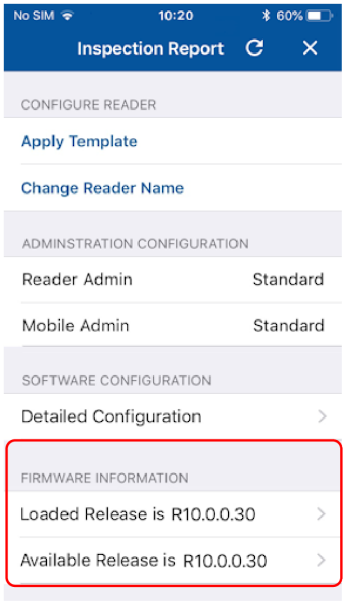


2.3.5 Firmware upgrade

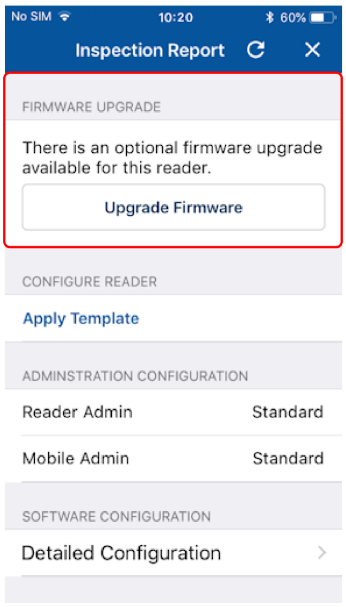
When connected to a reader, if a newer version of firmware is available, you will be notified about the update in the **FIRMWARE UPGRADE** section on the **Inspection Report** screen. If the firmware is already at the latest release or the currently loaded firmware is not supported then the **Upgrade Firmware** option will not be available.

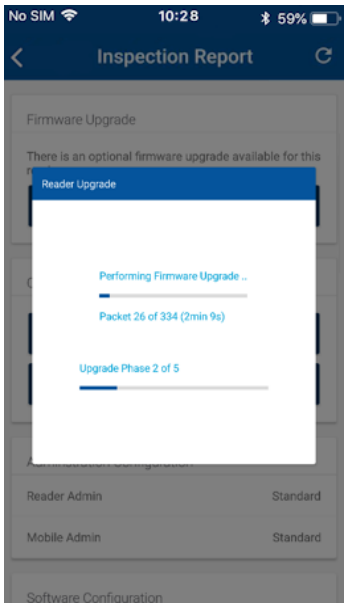
Note: Other than to resolve a specific issue, it is recommended that **optional** firmware upgrades are not implemented.

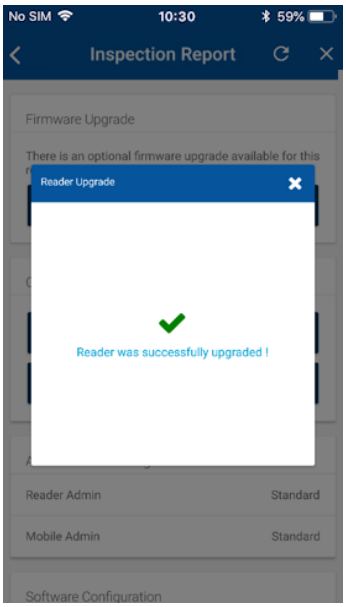




If a firmware upgrade is necessary, tap **Upgrade Firmware** to begin the firmware update process.







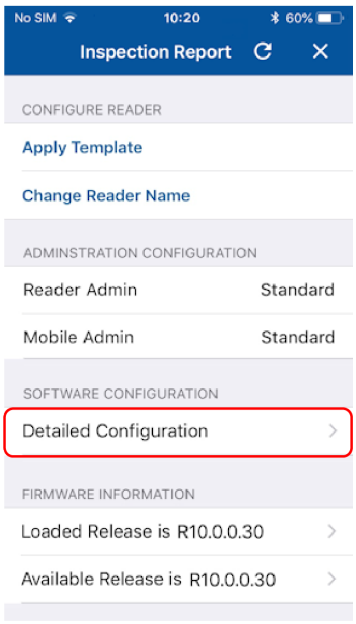
Note: Do not change devices if the firmware upgrade process has started. If any phase of the process is interrupted then restart the process and the upgrade will automatically resume when connection to the device is restored. If the firmware upgrade operation fails, for example “SNMP Authentication Failed”, refer to **Troubleshooting** for a possible description of the cause for the failure.

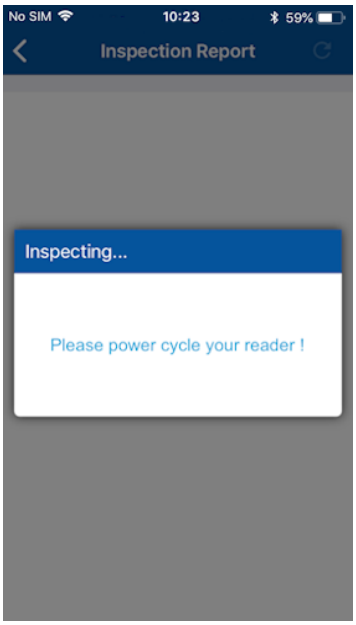
2.3.6 View detailed reader configuration

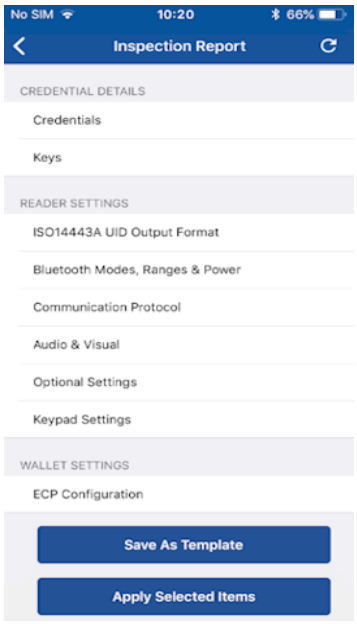
When connected to a reader, on the **Inspection Report** screen, tap **Detailed Configuration** to access detailed reader configuration settings.

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

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







Credential details

The **CREDENTIAL DETAILS** section provides access to options for enabling/disabling credential settings and adding authorization keys:

- Credentials, see **Credential settings**.
- Keys, see **Add Mobile Keys**.

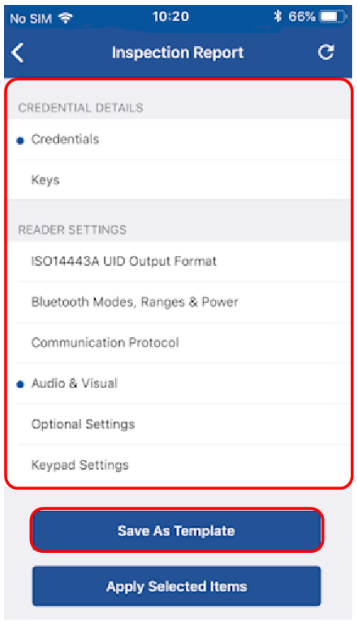
Reader Settings

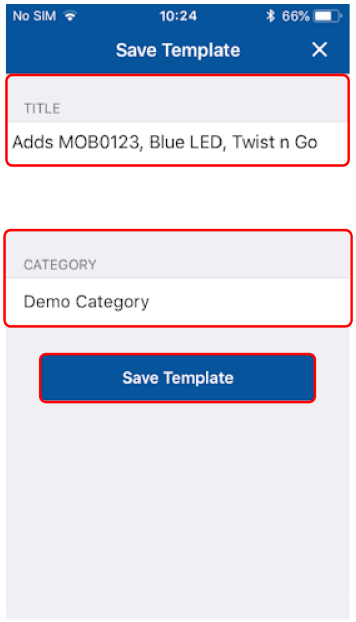
In the **READER SETTINGS** section the following can be configured:

- **ISO14443A UID Output Format**, see **ISO14443A UID Output Format settings**.
- **Bluetooth Modes, Ranges & Power**, see **Bluetooth Modes, Ranges & Power settings**.
- **Communication Protocol**, see **Communication Protocol settings**.
- **Audio & Visual**, see **Audio & Visual settings**.
- **Optional Settings**, see **Optional Settings**.
- **Keypad Settings**, see **Keypad Settings**.
- **Wallet Settings**, see **Wallet Settings**.

Save as template

Any changed configuration settings are indicated with a blue circle. To save changed configuration settings to a template, tap **Save as Template**, enter a template **Title** and **Category** and tap **Save Template**. To apply template settings, see **Apply configuration changes**.

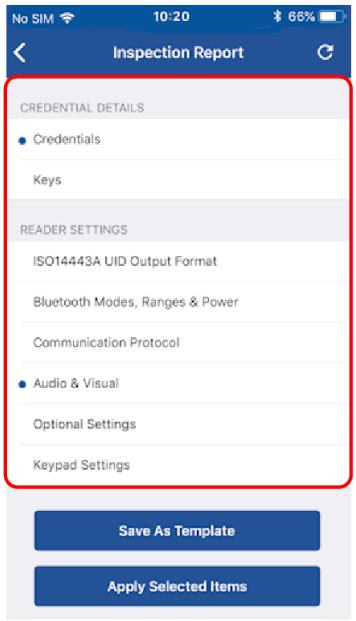


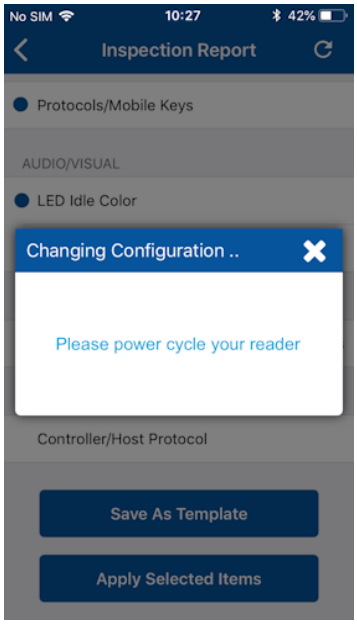


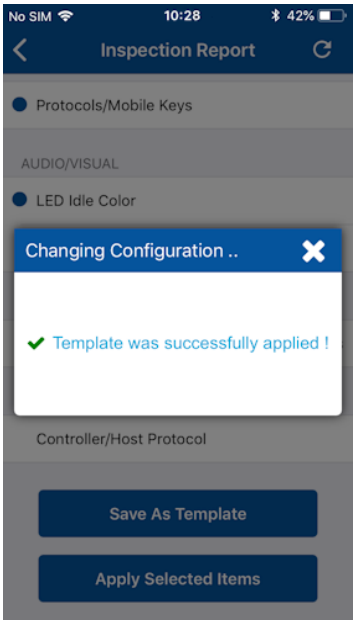
Apply selected items

Any changed configuration settings are indicated with a blue circle. To apply changed configuration changes directly to the connected reader, tap **Apply Selected Items**.

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





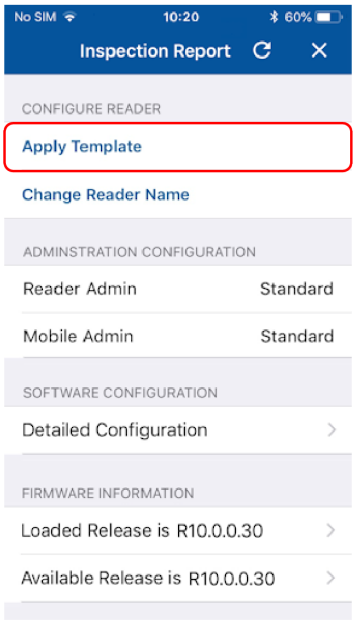


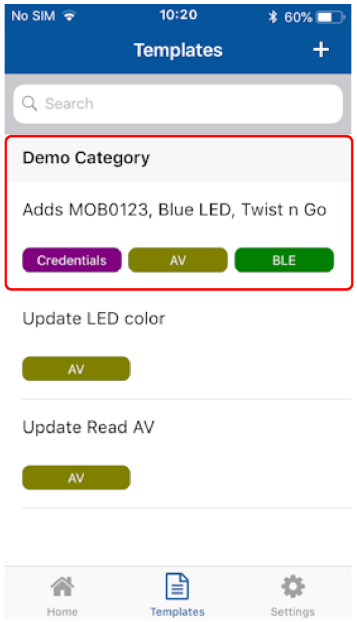
2.3.7 Apply configuration changes

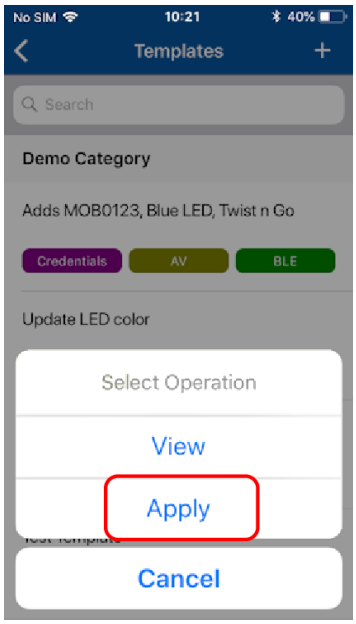
When viewing a reader **Inspection Report**:

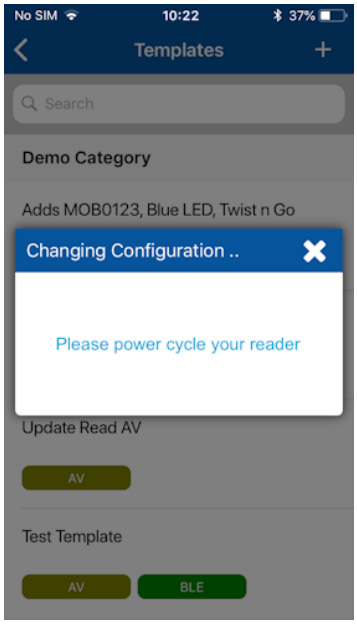
1. Tap **Apply Template**.
2. Select a listed template from the **Templates** screen. From the **Select Operation** menu, tap **Apply**.

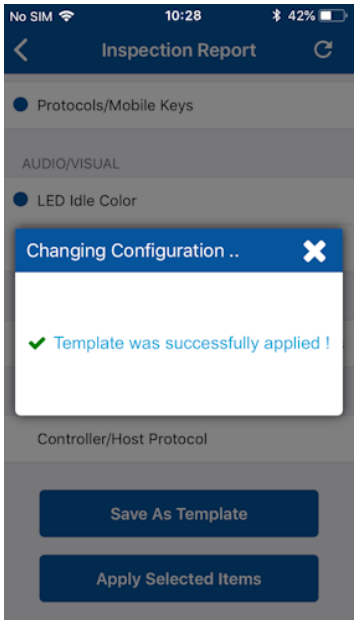
   Note: If the reader is a Standard enabled reader or an iCLASS SE Express R10 reader you will be prompted to power cycle the reader. For ICE/MOB enabled readers no reader power cycle is required.











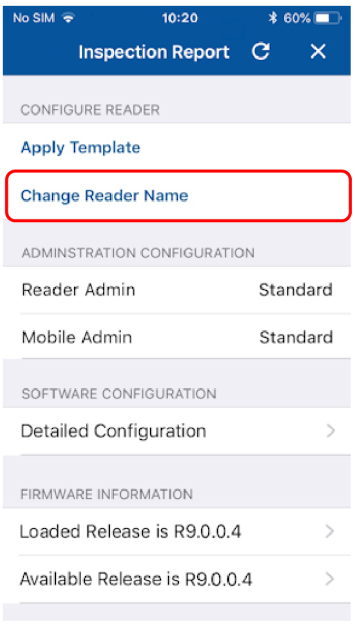
Note: If the operation to apply configuration changes fails, for example “SNMP Authentication Failed”, refer to **Troubleshooting** for a possible description of the cause for the failure.

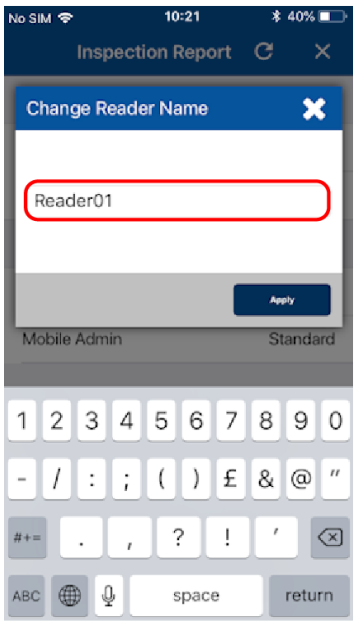
2.3.8 Change reader name

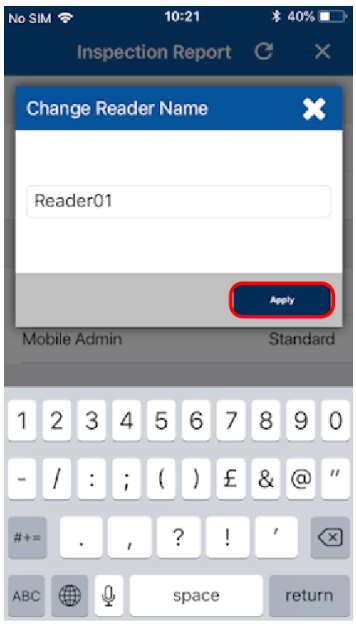
On the **Inspection Report** screen the reader name can be changed. When changing a reader name with **Change Reader Name**, the reader's name, for example, "iCLASS SE Reader", is changed to a custom name. This custom reader name is visible from within any other Technician's Reader Manager app.

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

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







Section 03

HID Reader Manager Portal

Powering
Trusted Identities

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

3.1 Mobile Access setup

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

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

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

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

3.1.1 Reader Manager Portal setup

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

- For organizational accounts setup up on the HID® Origo™ Management Portal, access to the Reader Manager Portal is available by default.
- For organizational accounts setup up on the legacy Secure Identity Services (SIS) Portal, adding or removing the HID Reader Manager Portal for a company must be completed by HID Global. Follow the process detailed in the *HID Mobile Access® Portal – HID Reader Manager Portal Change Form*, available from:

  https://www.hidglobal.com/documents

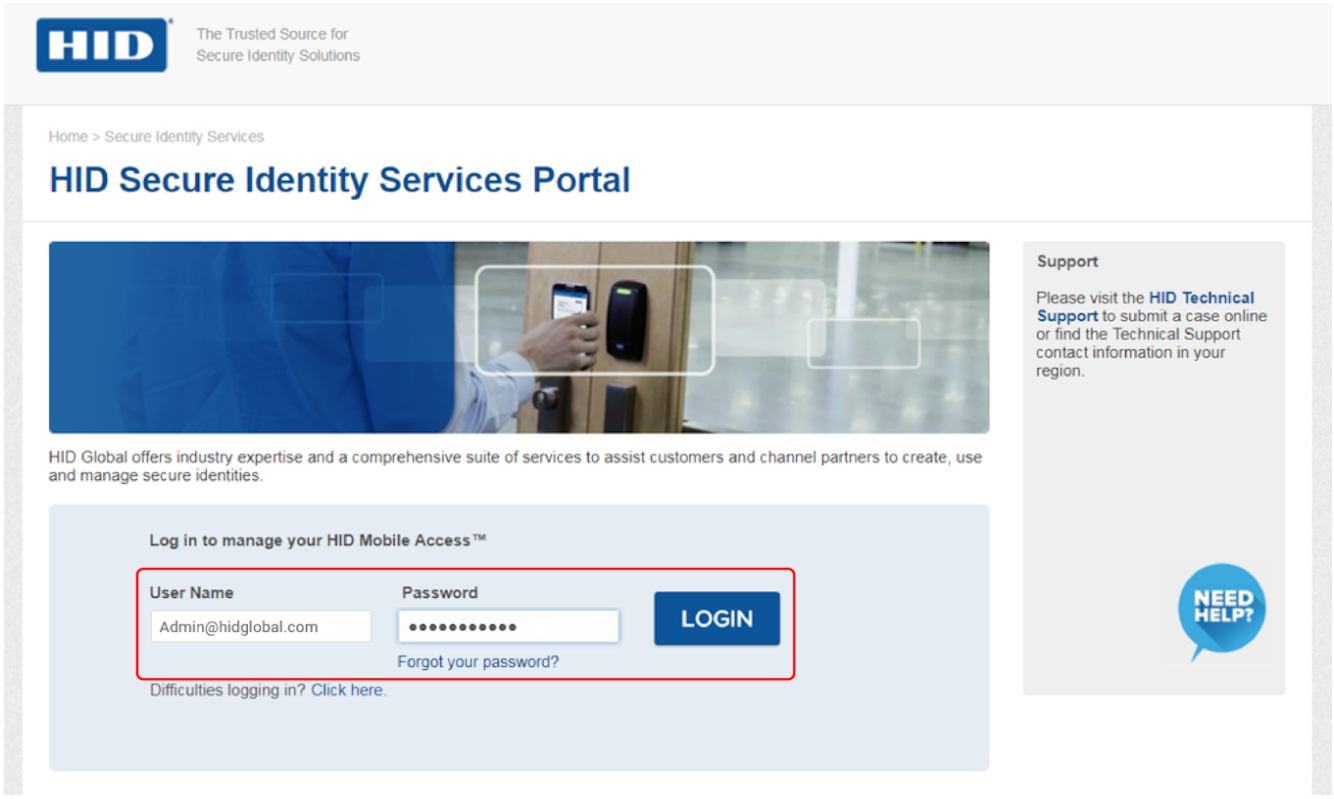
3.2 Access the HID Reader Manager Portal

The HID Reader Manager Portal is a hosted service available to registered Reader Manager Administrators.

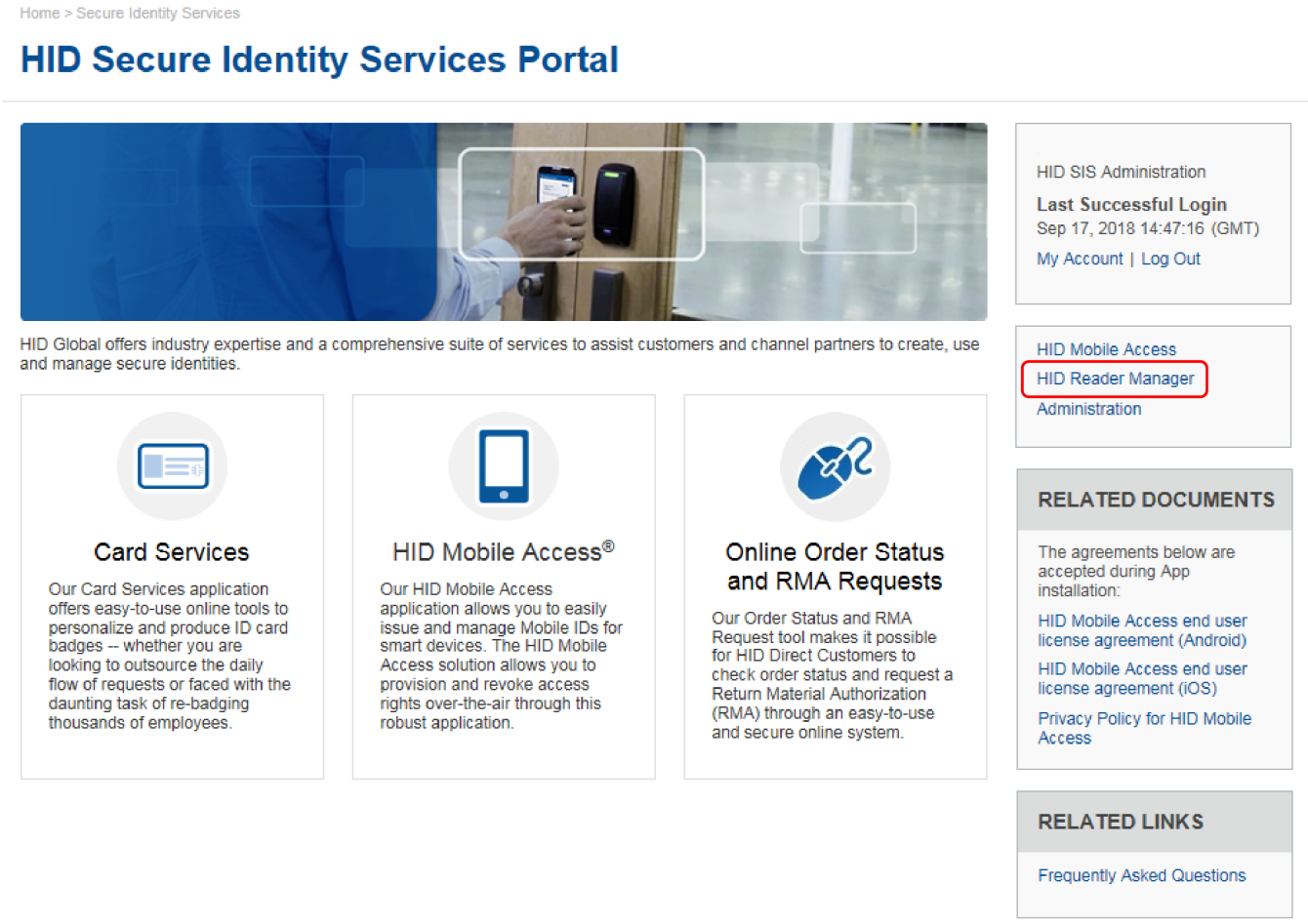
3.2.1 Access the HID Reader Manager Portal (HID SIS Portal)

To access the Reader Manager Portal:

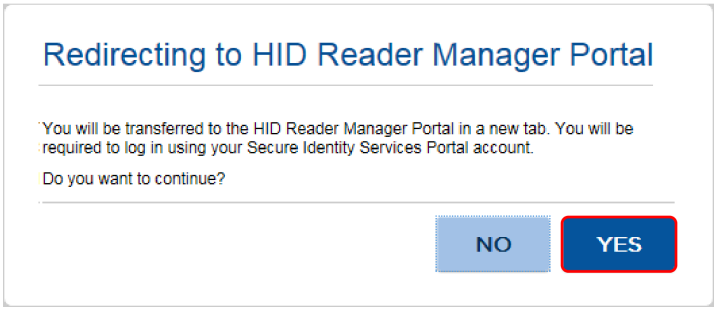
1. Log into the HID Secure Identity Services (SIS) Portal as Organization Admin.
   Note: This is the same login page and login credentials used for the Mobile Access Portal.



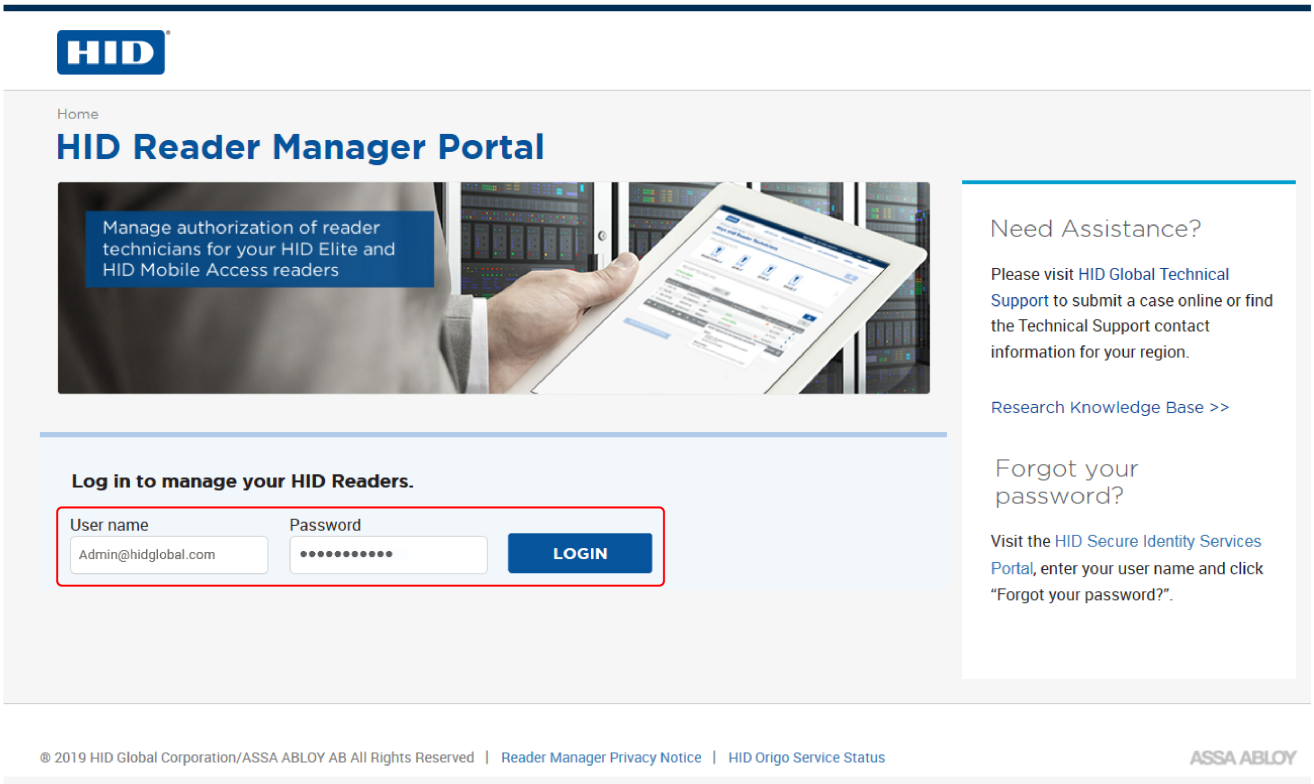
2. Select the **HID Reader Manager** link on the main HID Secure Identity Services Portal page.



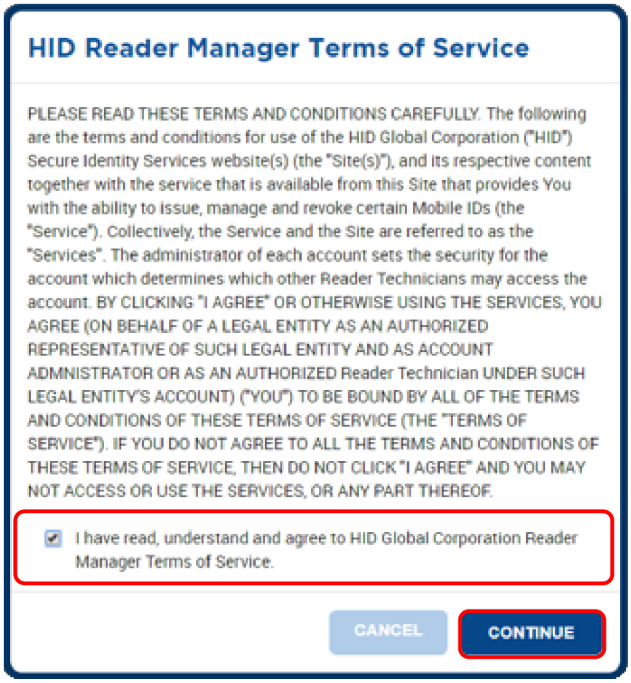
3. Click **YES** to be redirected to your organizations instance of the HID Reader Manager Portal.



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



Note: If this is the initial login as Reader Manager Administrator you will be asked to read and accept the **HID Reader Manager Terms of Service**. Click **Continue**.

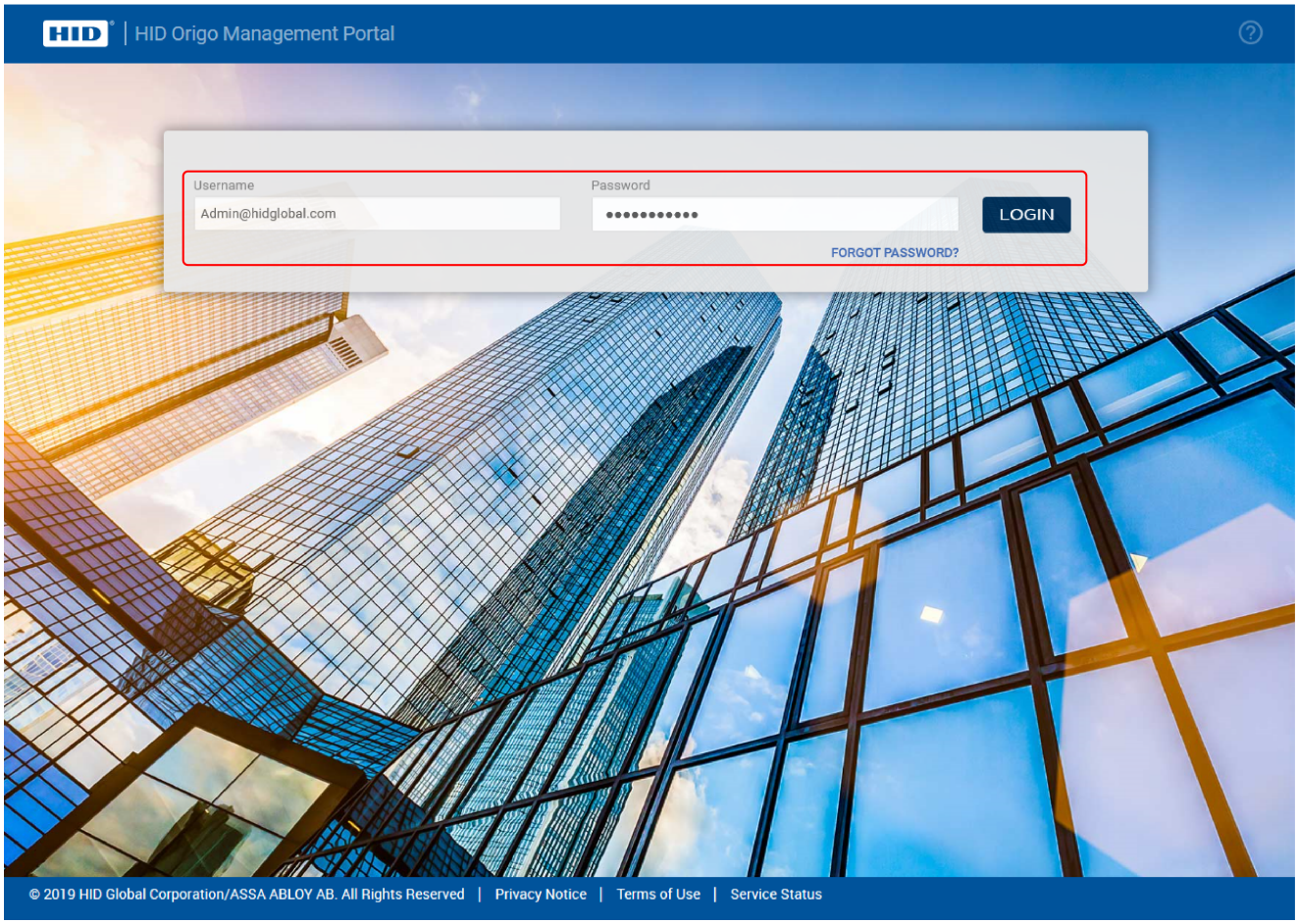


The Reader Manager Administrator can now perform Reader Technician enrollment and authorization key issuance tasks in the HID Reader Manager Portal.

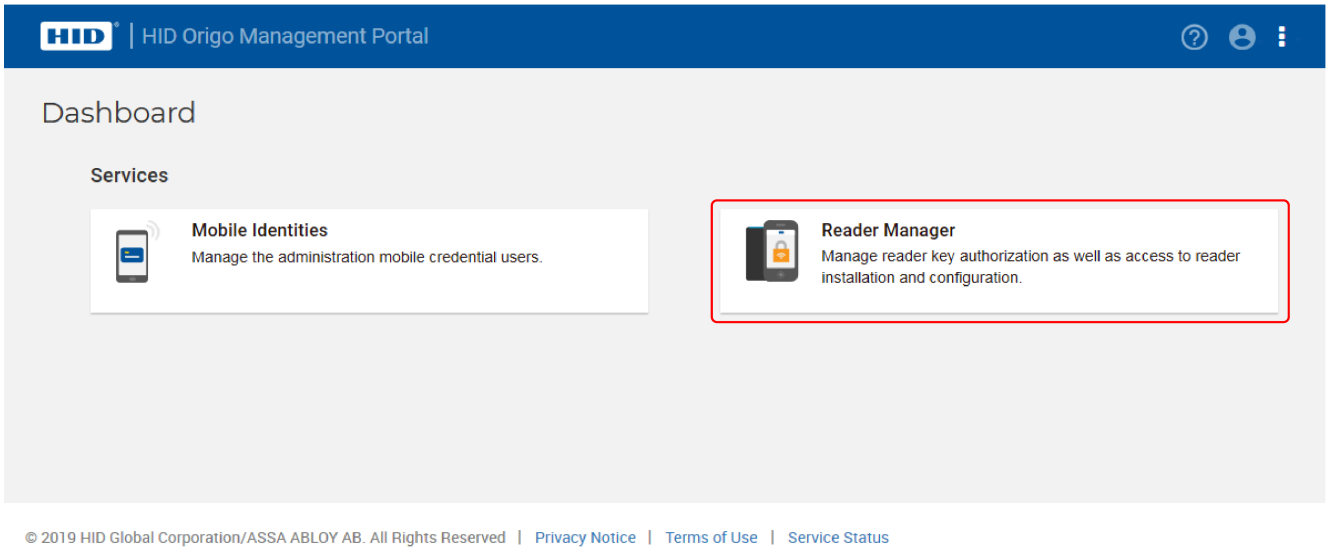
3.2.2 Access the HID Reader Manager Portal (HID® Origo™ Management Portal)

To access the HID Reader Manager Portal:

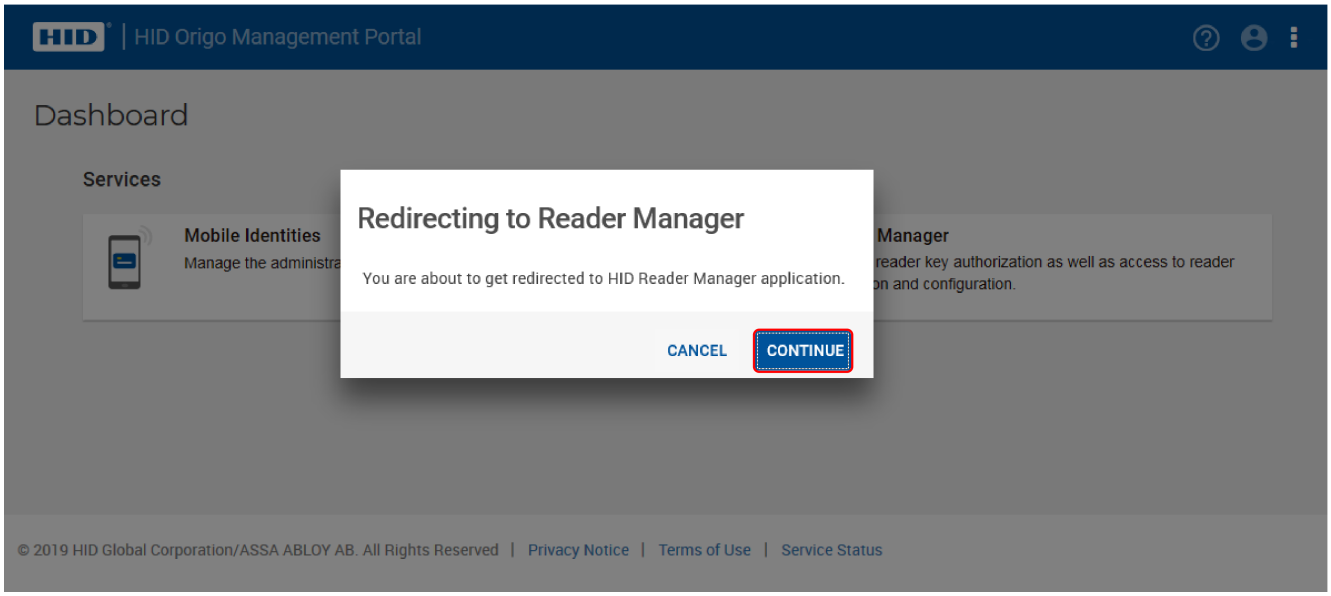
1. Log into the HID Origo Management Portal as Organization Admin.



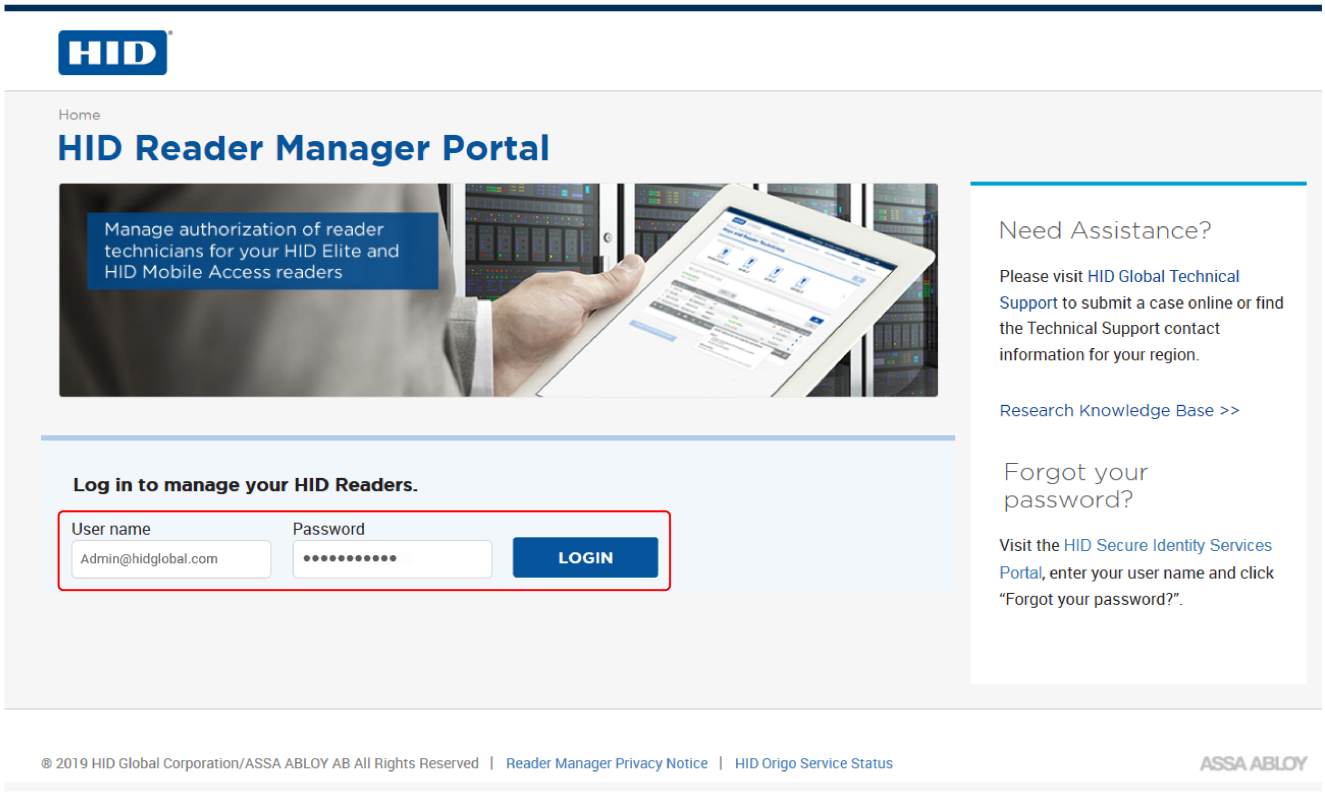
2. Select **Reader Manager** on the **Dashboard** page.



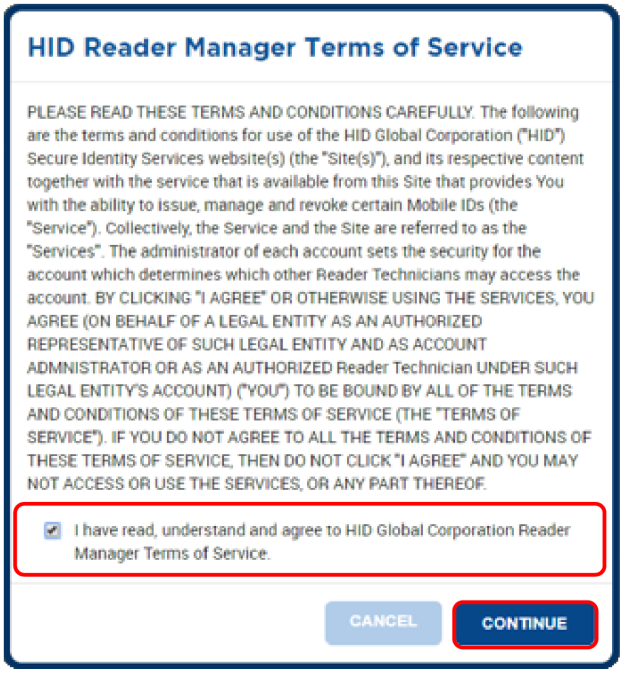
3. Click **CONTINUE** to be redirected to your organizations instance of the HID Reader Manager Portal.



4. Login as Reader Manager Administrator using the User name and Password setup in the HID Origo Management Portal.



Note: If this is the initial login as Reader Manager Administrator you will be asked to read and accept the **HID Reader Manager Terms of Service**. Click **Continue**.



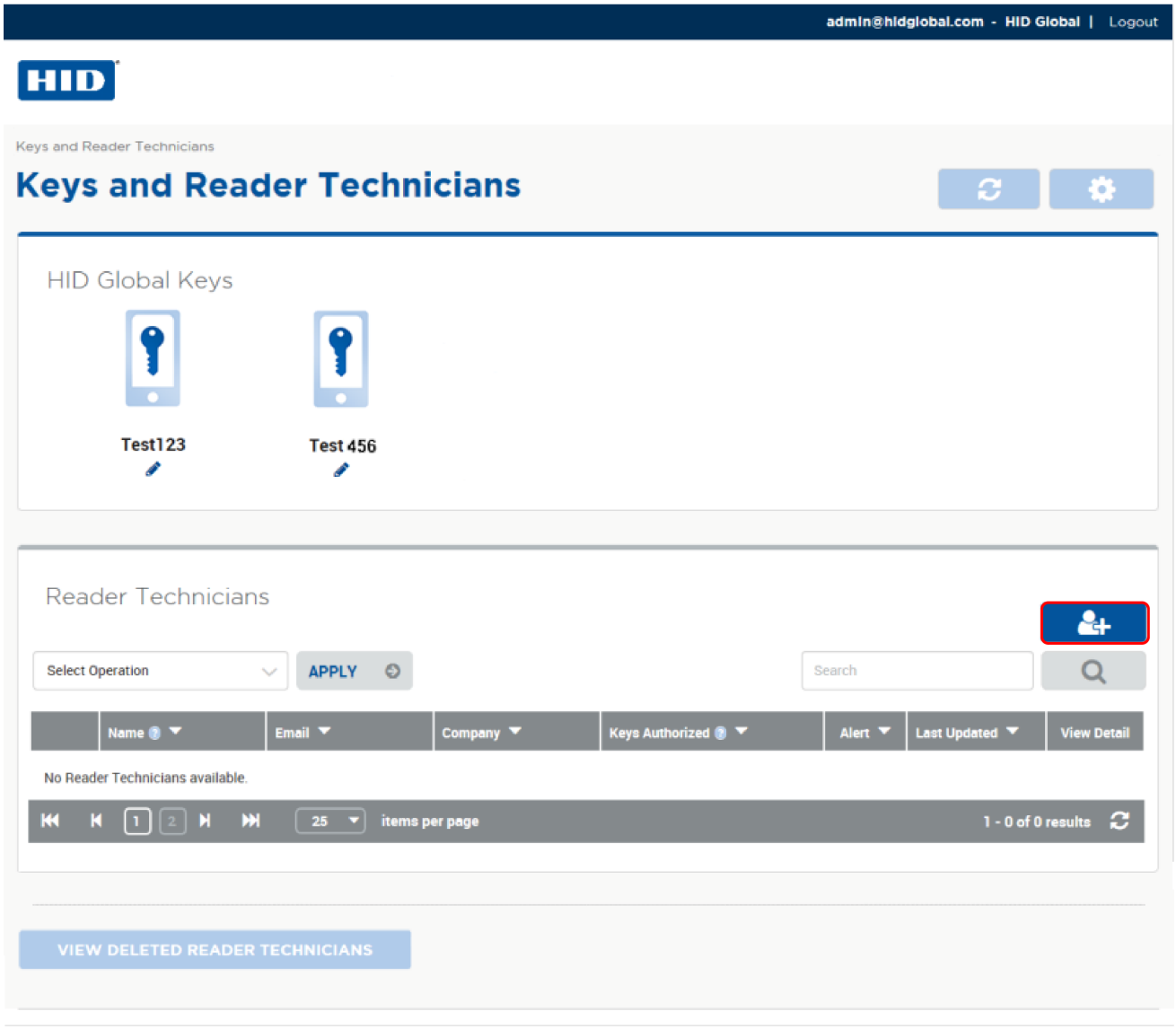
The Reader Manager Administrator can now perform Reader Technician enrollment and authorization key issuance tasks in the HID Reader Manager Portal.

3.3 Enroll a Reader Technician

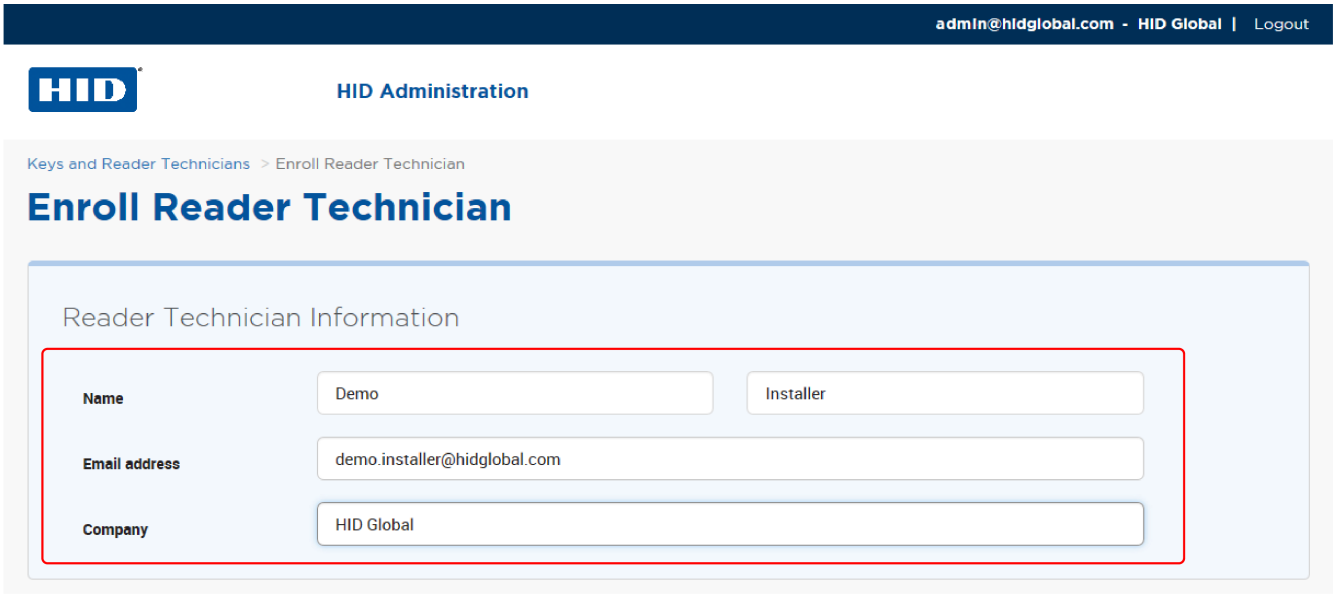
As a prerequisite to enrolling a Reader Technician, the Reader Technician must have installed and registered the HID® Reader Manager™ App on their mobile device, see **Download and install the Reader Manager app** and **Register a new account within the app**.

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

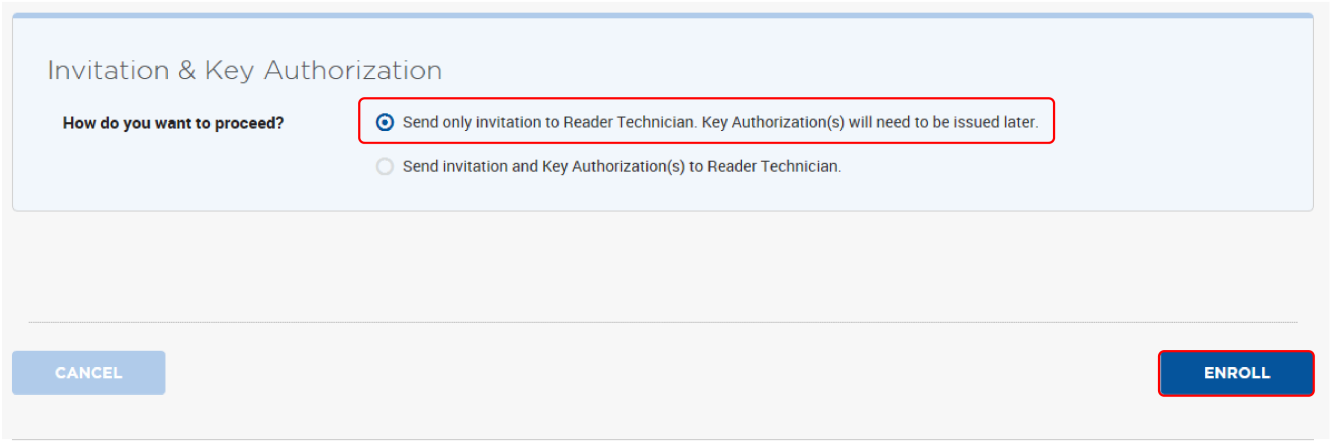
1. Scroll to the **Reader Technicians** section on the **Keys and Reader Technicians** page.
2. Select the enroll technician icon [ ].



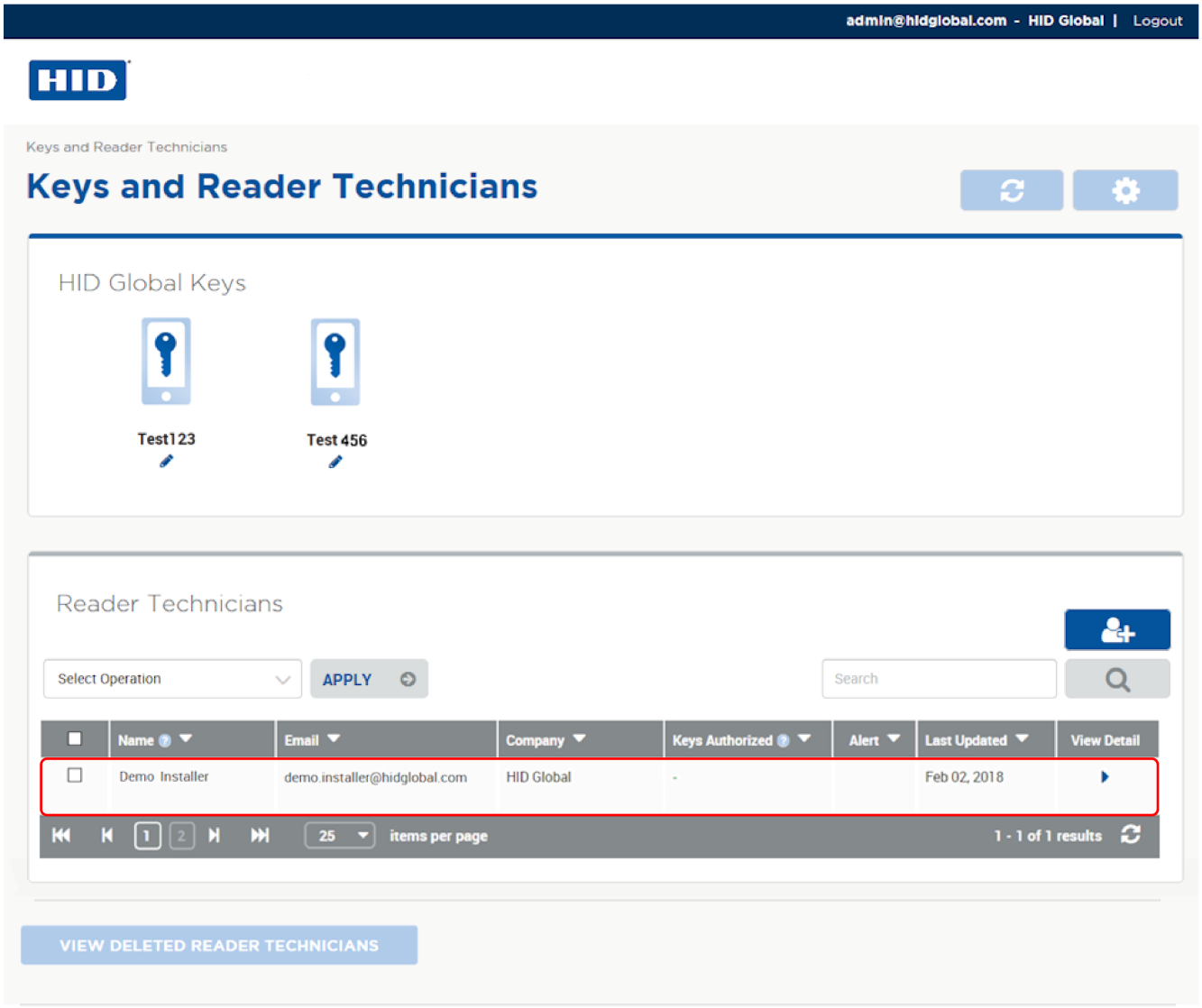
3. Enter the **Name**, **Email address**, and **Company** of the new Reader Technician on the **Enroll Reader Technician** page.



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



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

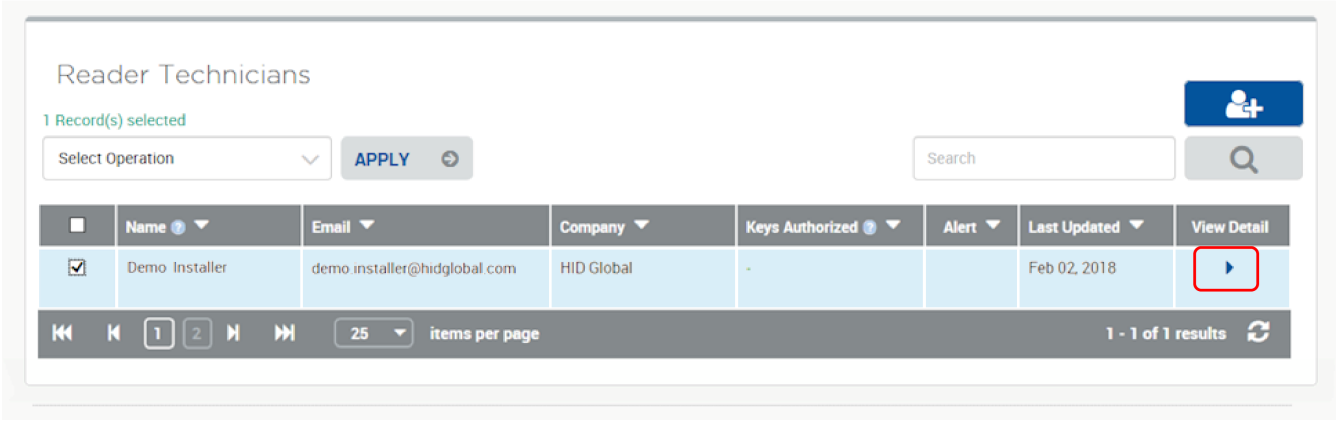


The enrolled Reader Technician will receive a Reader Manager invitation email in their registered email inbox containing an invitation code for activating the HID Reader Manager app. See **Activate the HID Reader Manager app**. When the Reader Manager app is activated the administrator can issue key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

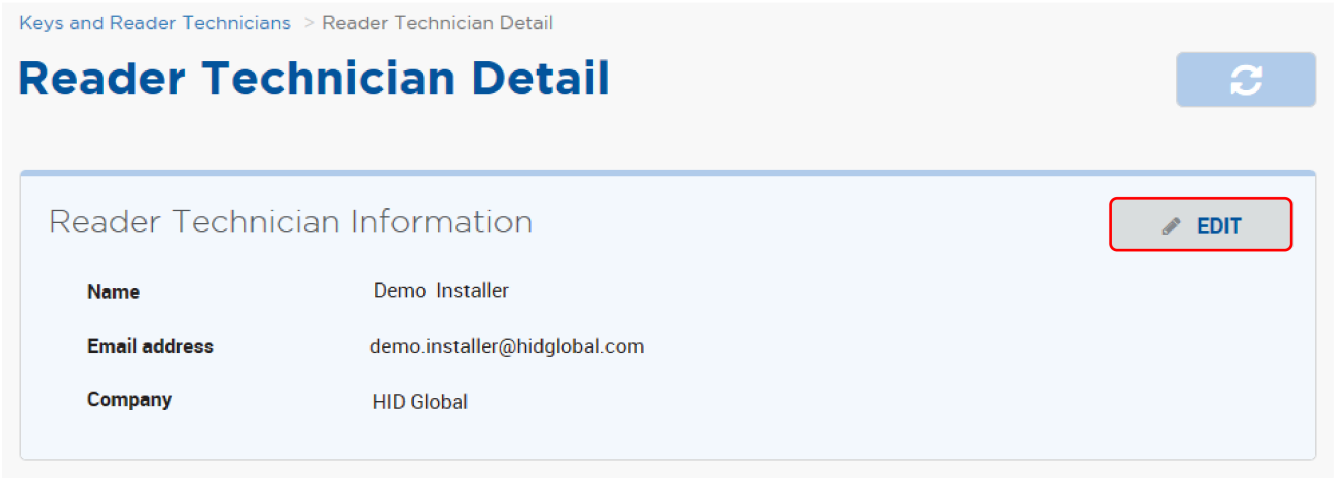
3.3.1 Edit Reader Technician information

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.



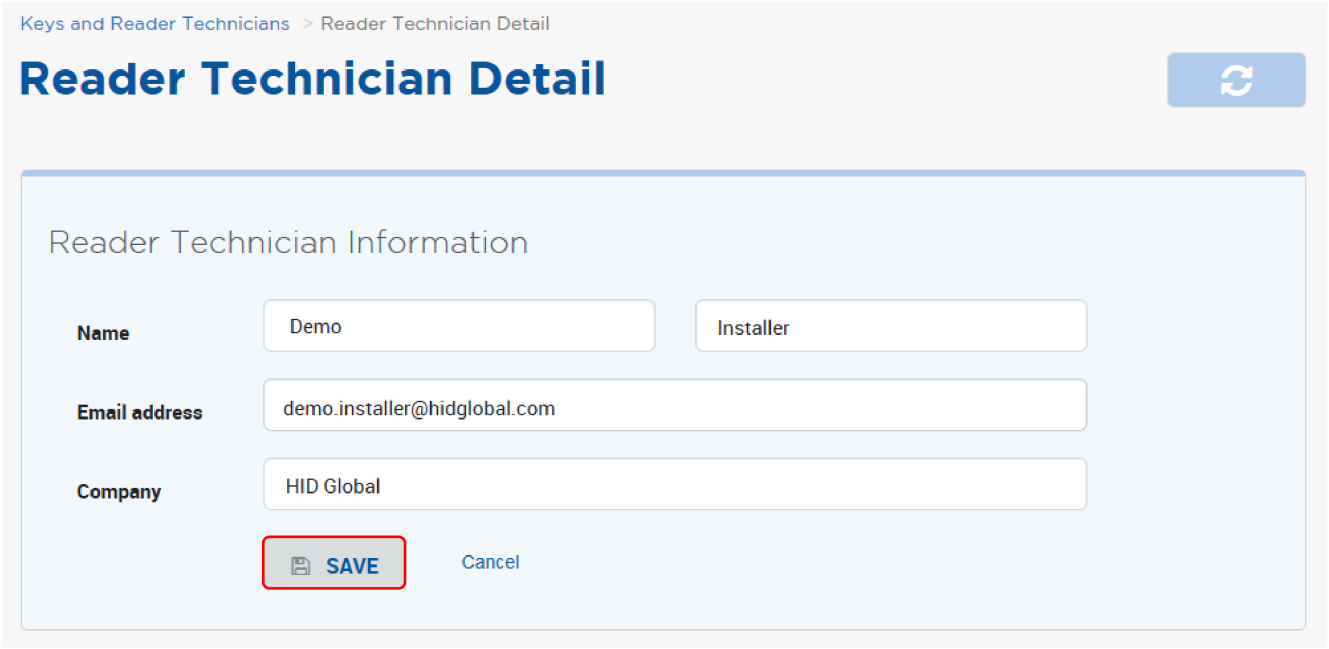
3. Click **EDIT** in the **Reader Technician Information** section.



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.

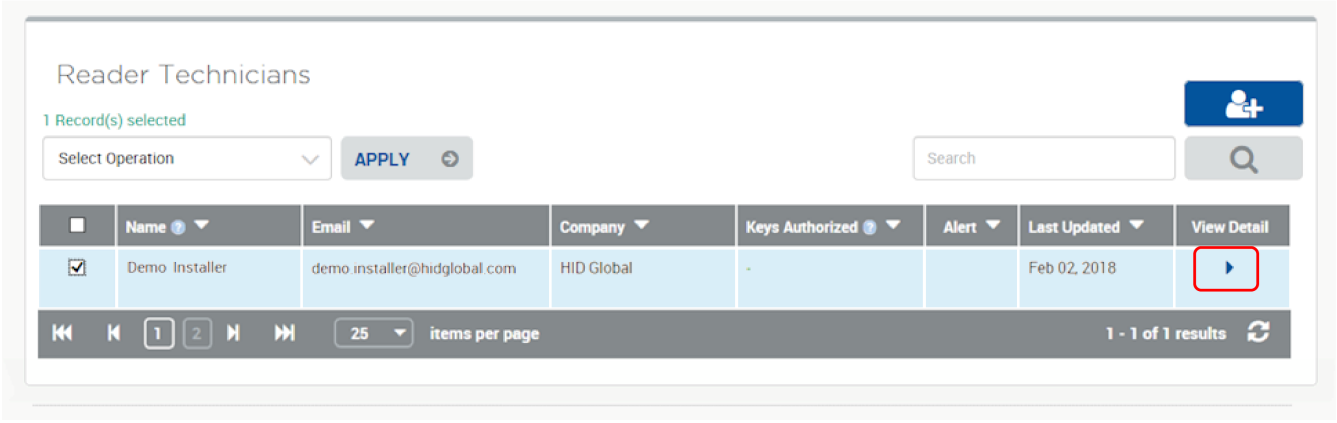
   Note: If the Reader Technician uses the edited email address to log into the Reader Manager app then the mobile device must be registered again and all the authorization keys must be re-issued.



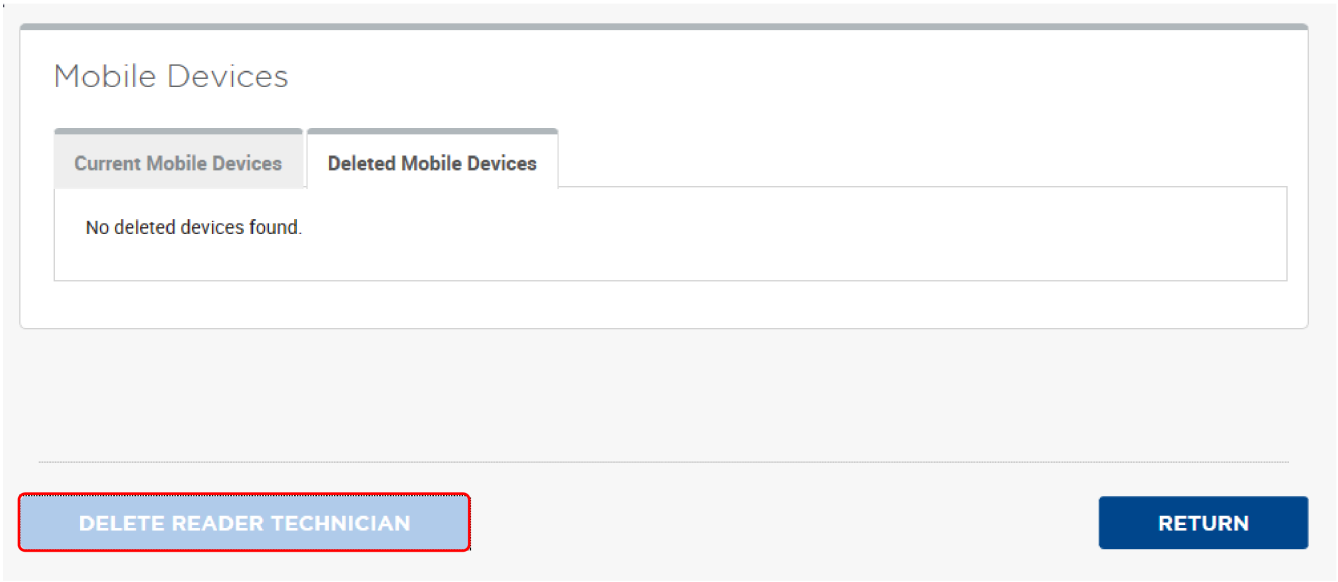
3.3.2 Delete an enrolled Reader Technician

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.



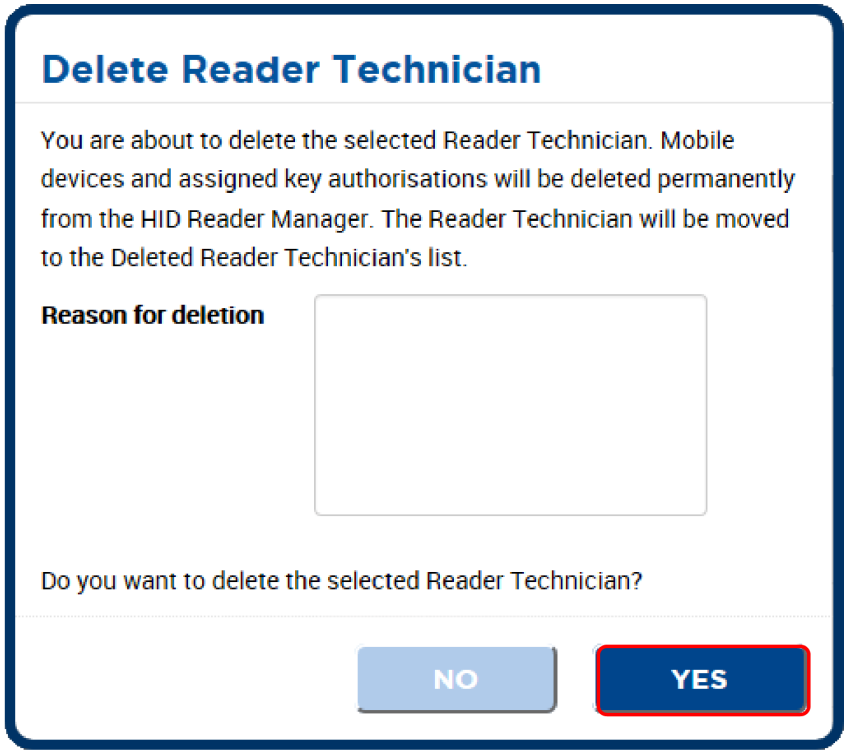
3. Scroll to the bottom of the **Reader Technician Detail** page and click **DELETE READER TECHNICIAN**.



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



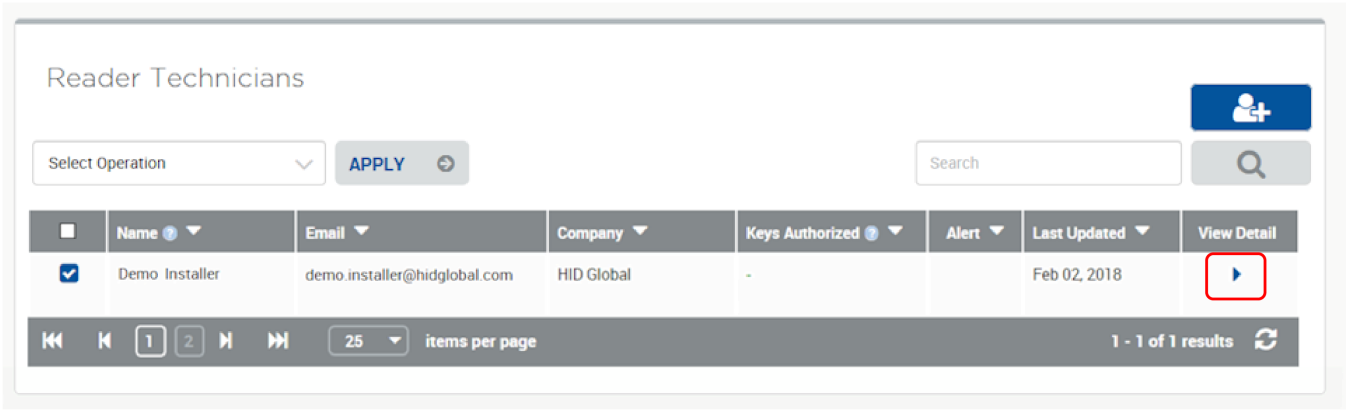
The deleted Reader Technician appears in the list of **Deleted Reader Technicians**.

3.4 Issue authorization keys

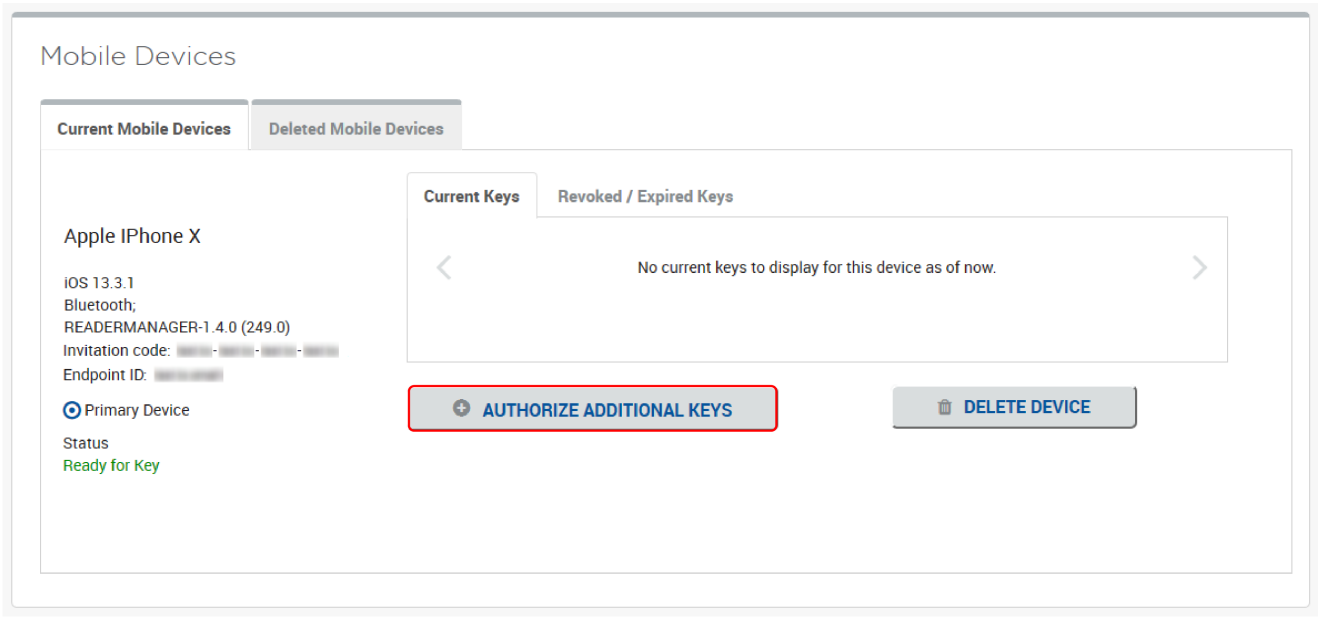
HID Reader Manager uses authorization keys to securely connect and control access by the mobile app.

To issue authorization keys in the HID Reader Manager Portal:

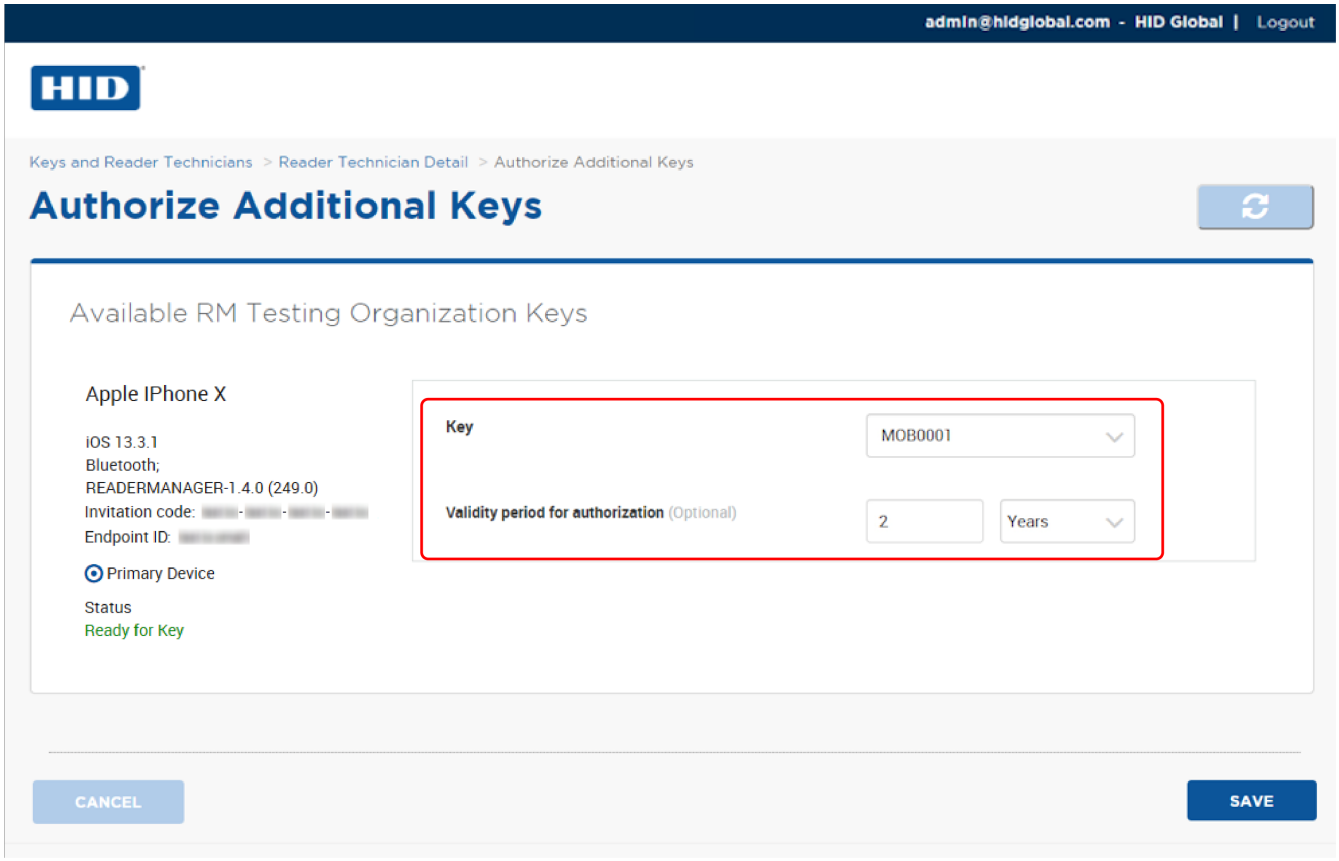
1. Scroll to the **Reader Technicians** section on the **Keys and Reader Technicians** page.
2. Select a displayed Reader Technician entry and click on the associated **View Detail** icon [▸] to access the **Reader Technician Detail** page.



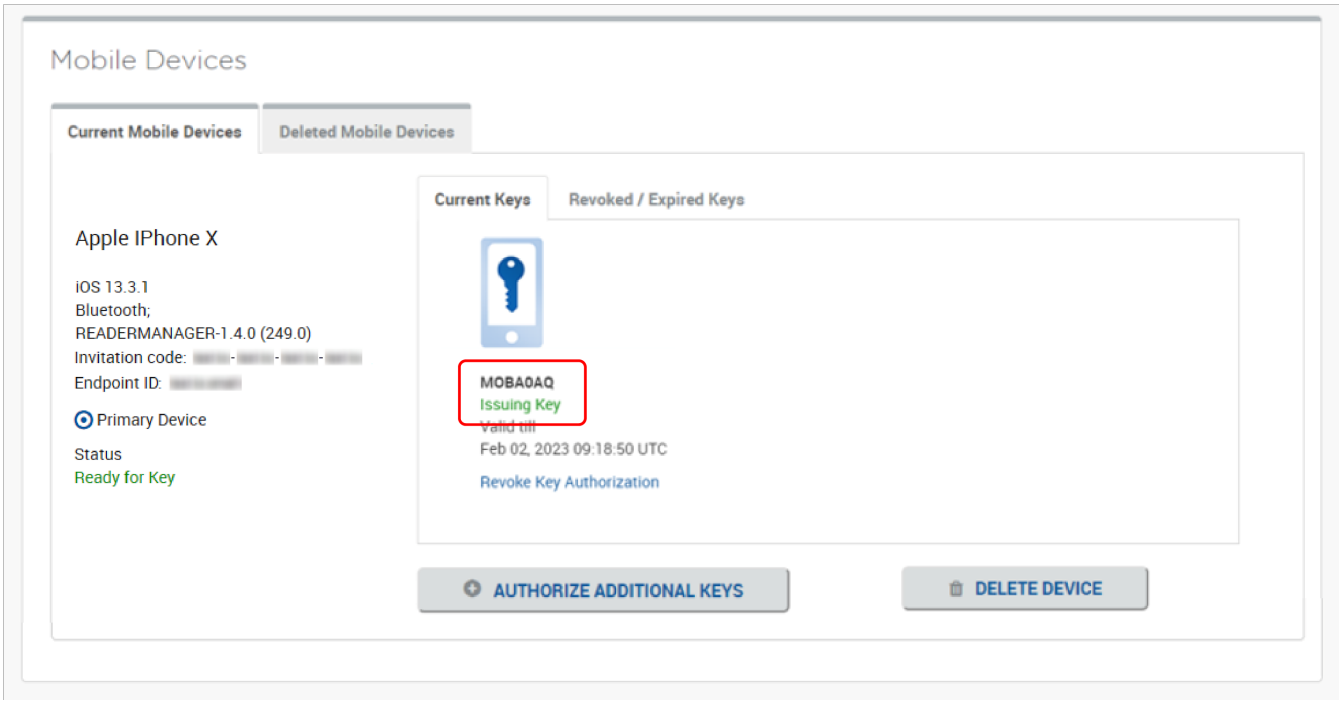
3. Scroll to the **Mobile Devices** section and click **AUTHORIZE ADDITIONAL KEYS**.



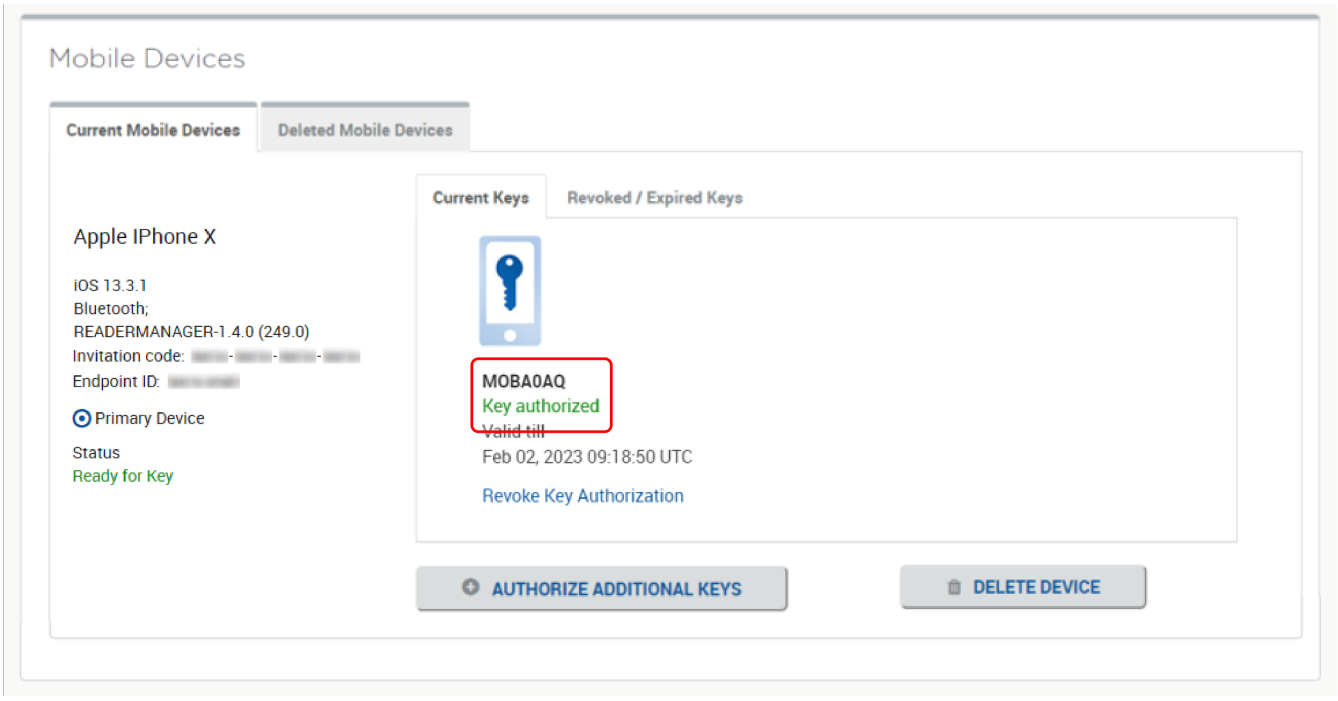
4. On the **Authorize Additional Keys** page select a key reference from the **Key** drop-down menu.
5. As an option set a authorization validity period.
   Note: If the validity period for authorization is not set the default period is five years.
6. Click **SAVE**.



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



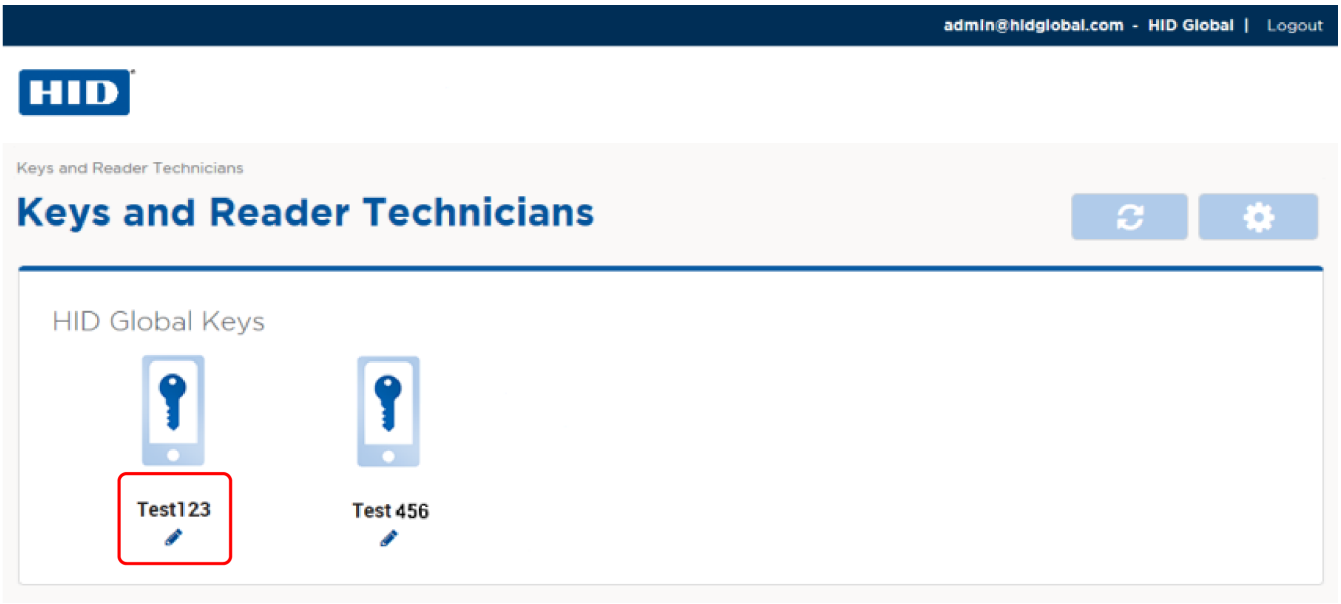
7. Check with the Reader Technician that the authorization key has been issued to the Reader Manager app. See **Display authorized keys**.
8. Refresh the **Reader Technician Detail** page and verify that the key status is changed to **Key authorized**.



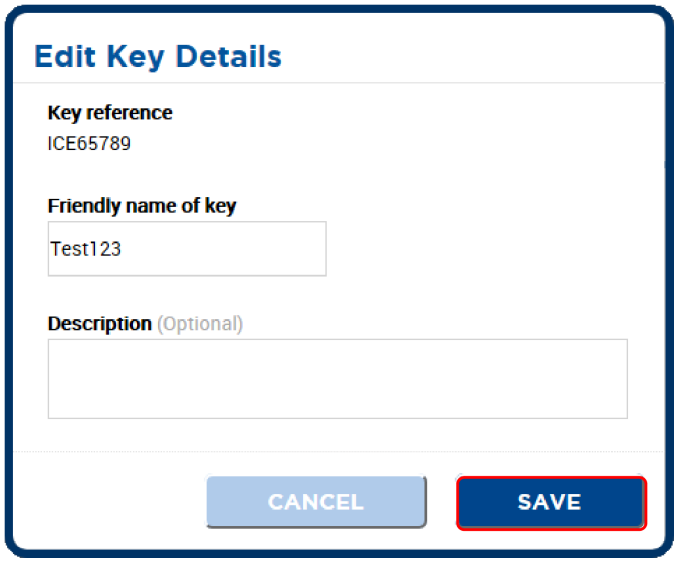
3.4.1 Edit authorization key information

To edit authorization key information:

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

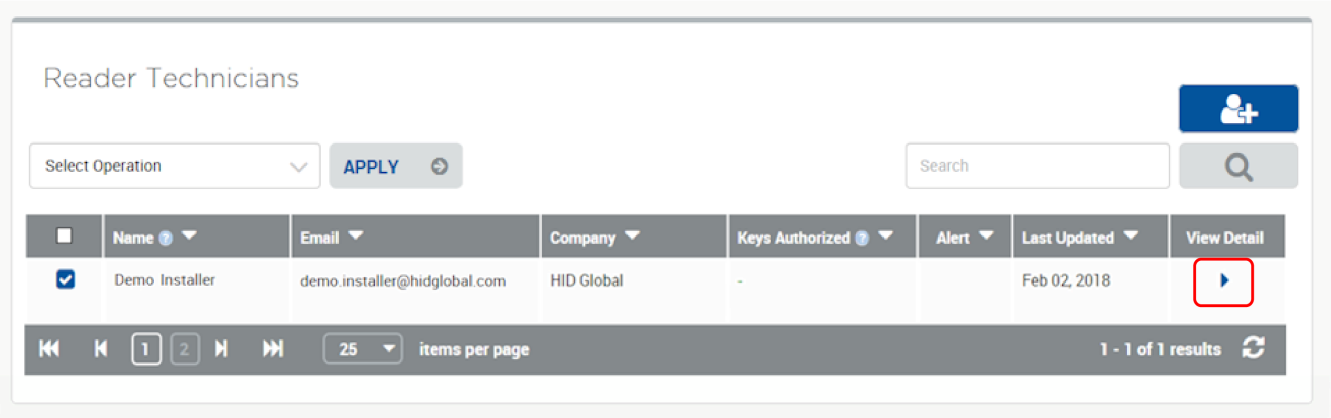


2. Edit the authorization key information as required and click **SAVE**.

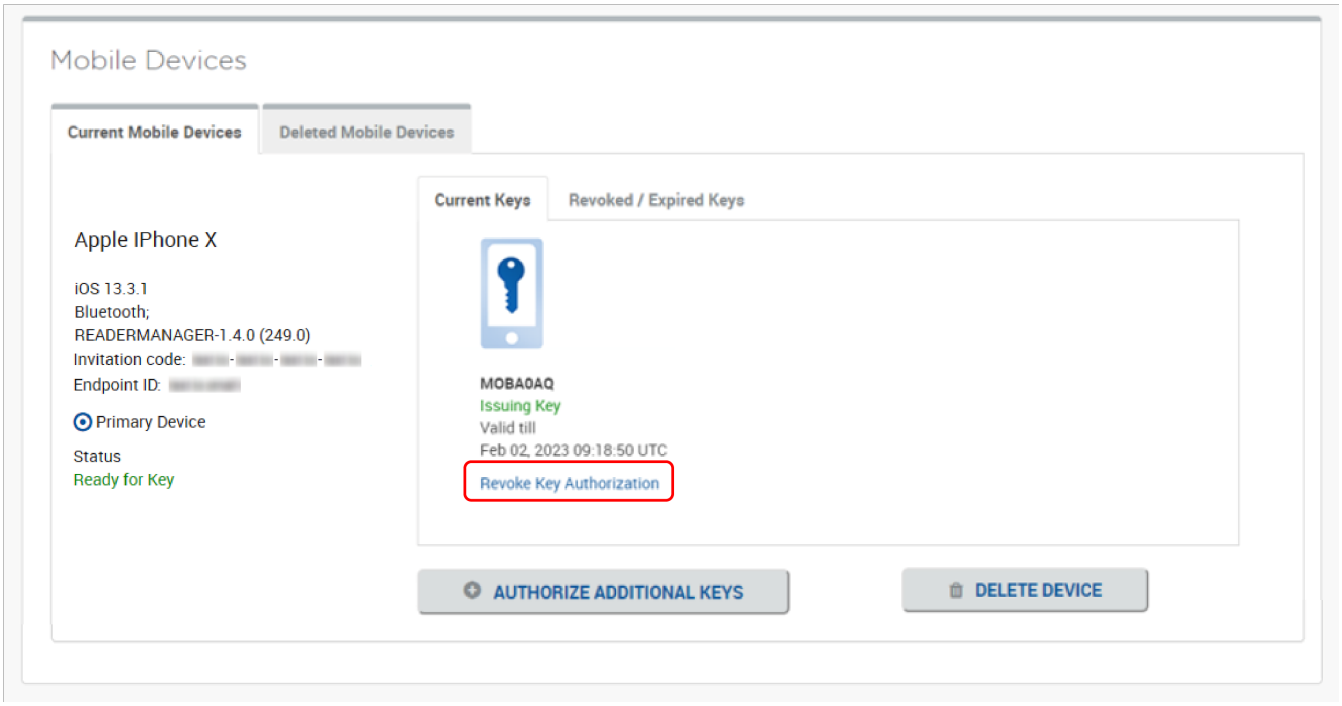


3.4.2 Revoke (delete) an authorization key

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



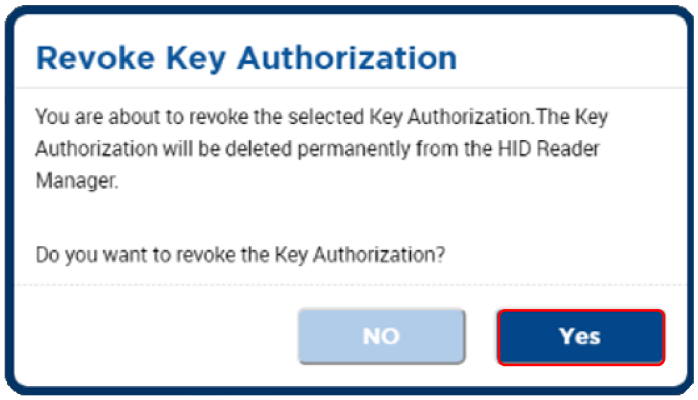
3. Scroll to the **Mobile Devices** section. For the authorization key to revoke, click **Revoke Key Authorization**.



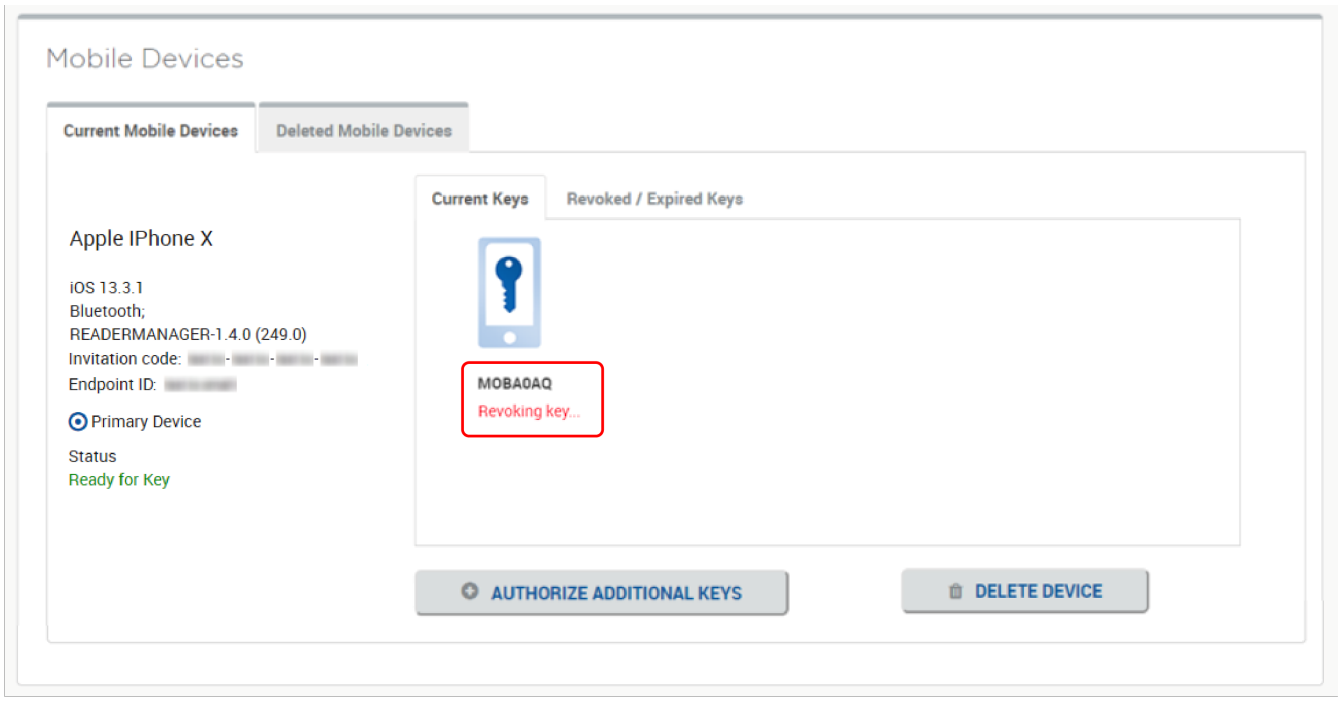
4. Click **YES** to revoke the selected key authorization from the HID Reader Manager.

   Note: Any key authorizations issued to the Reader technician will immediately have revocation attempted. If the mobile device is not reachable (for example, turned off or out of range), the system will periodically retry the delete operation.

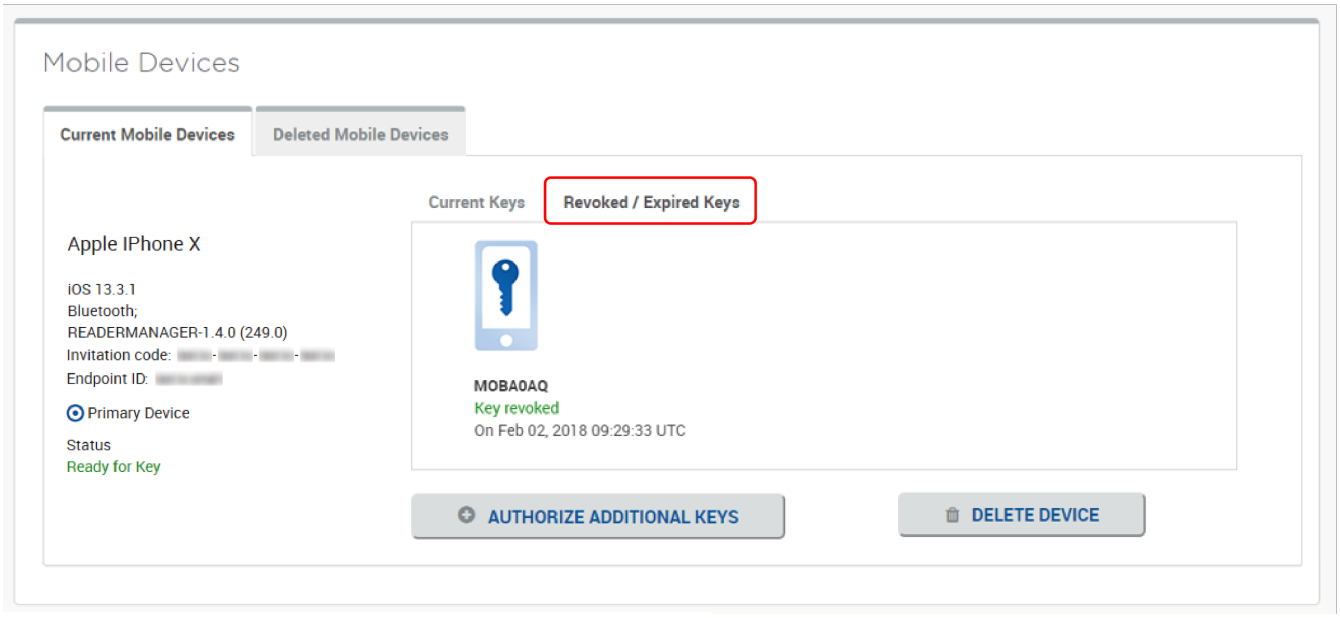
   When the Delete Threshold time (see **Configure Delete Threshold**), has elapsed the system automatically completes the delete operation and places the key authorization in a revoked state.



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

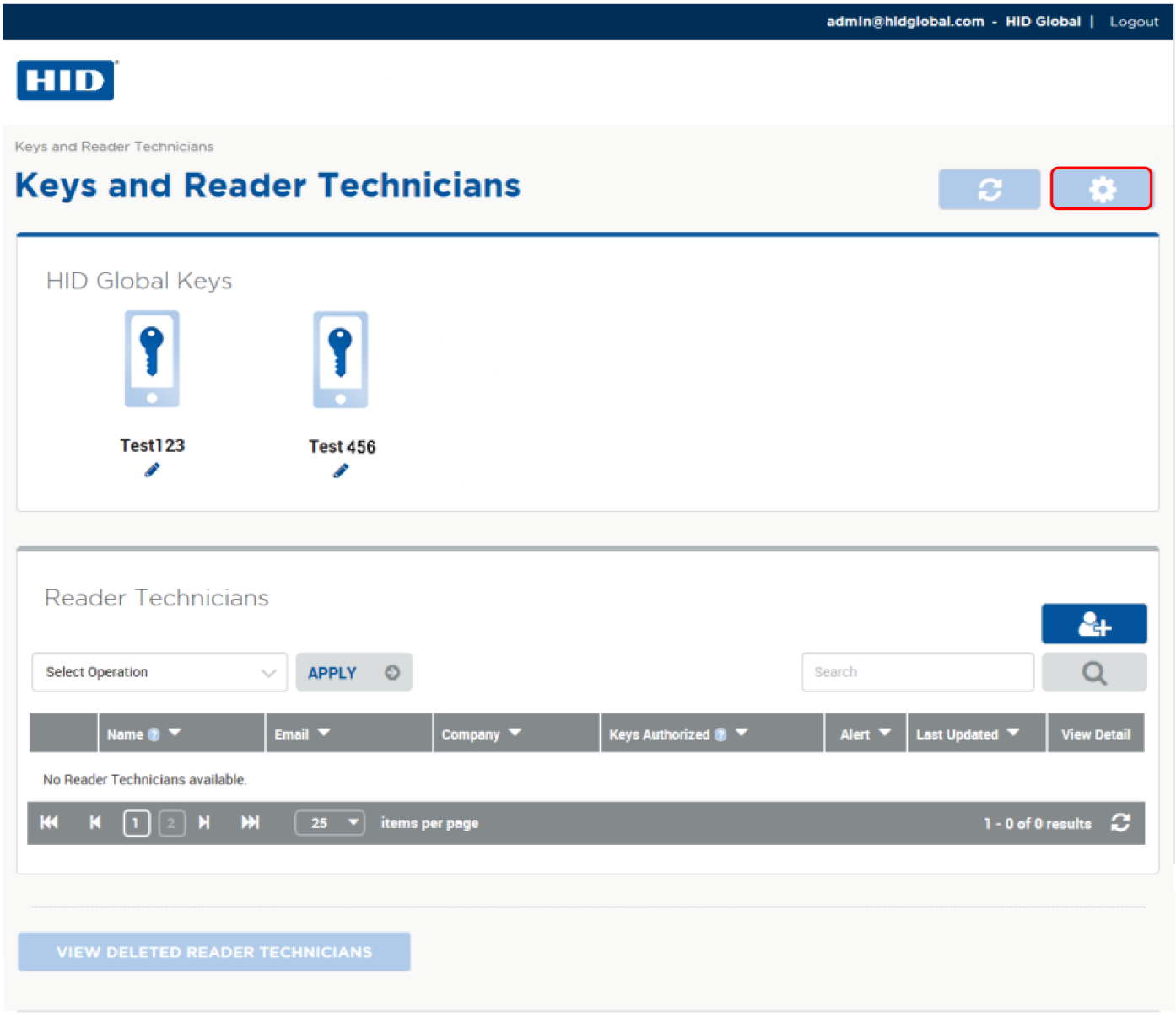


5. Check with the Reader Technician that the authorization key has been revoked in the HID Reader Manager app.
6. Refresh the **Reader Technician Detail** page and verify that the revoked key has been moved to the **Revoked / Expired Keys** tab.



3.5 Configure HID Reader Manager Portal settings

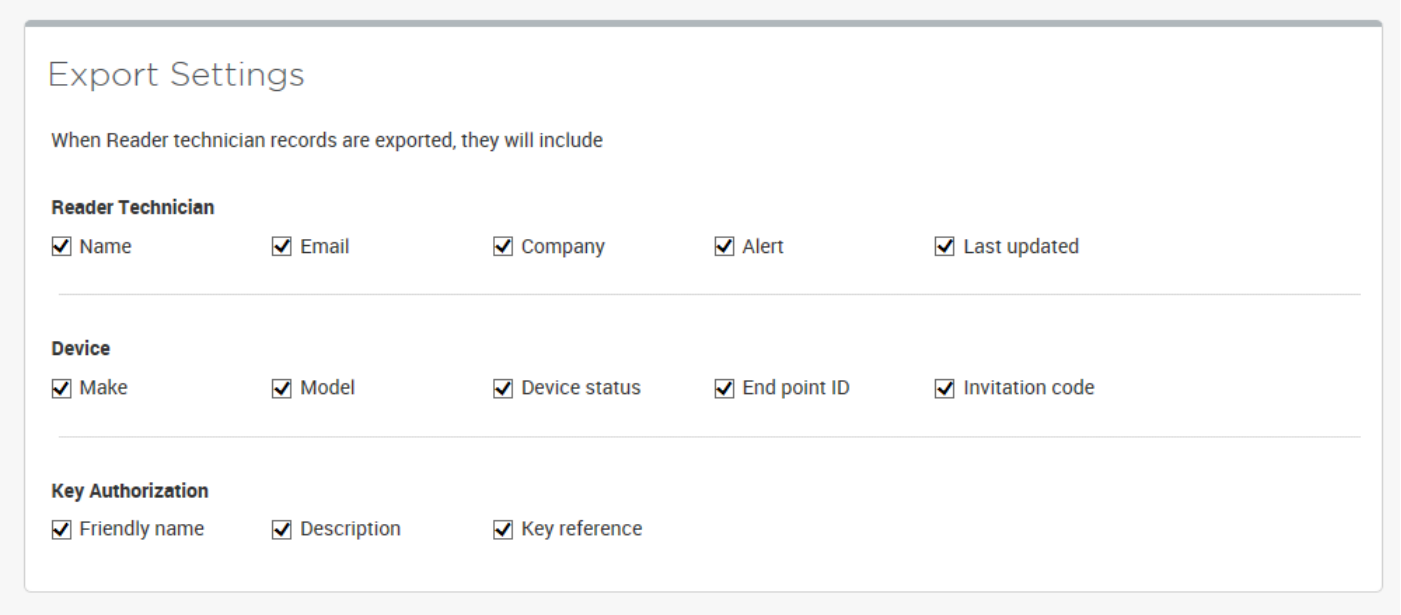
To access HID Reader Manager Portal settings click the **Settings** icon [ ] on the **Keys and Reader Technicians** page.



3.5.1 Export Reader Technician record settings

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

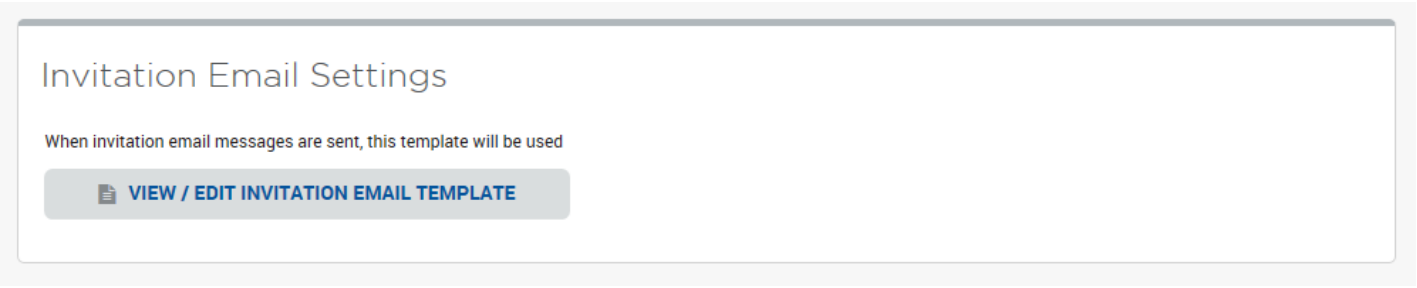
Once the selections have been made, click **SAVE** to implement.



3.5.2 Invitation Email settings

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

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

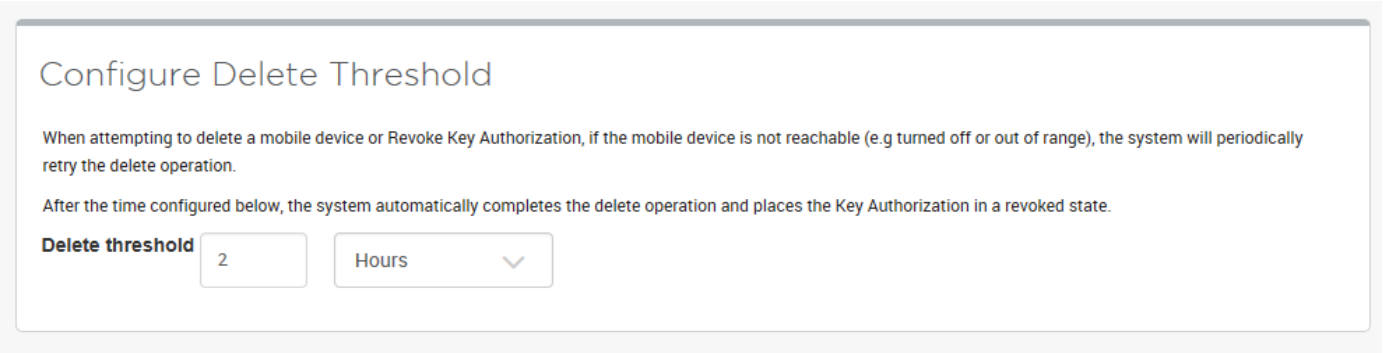


3.5.3 Configure Delete Threshold

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

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

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

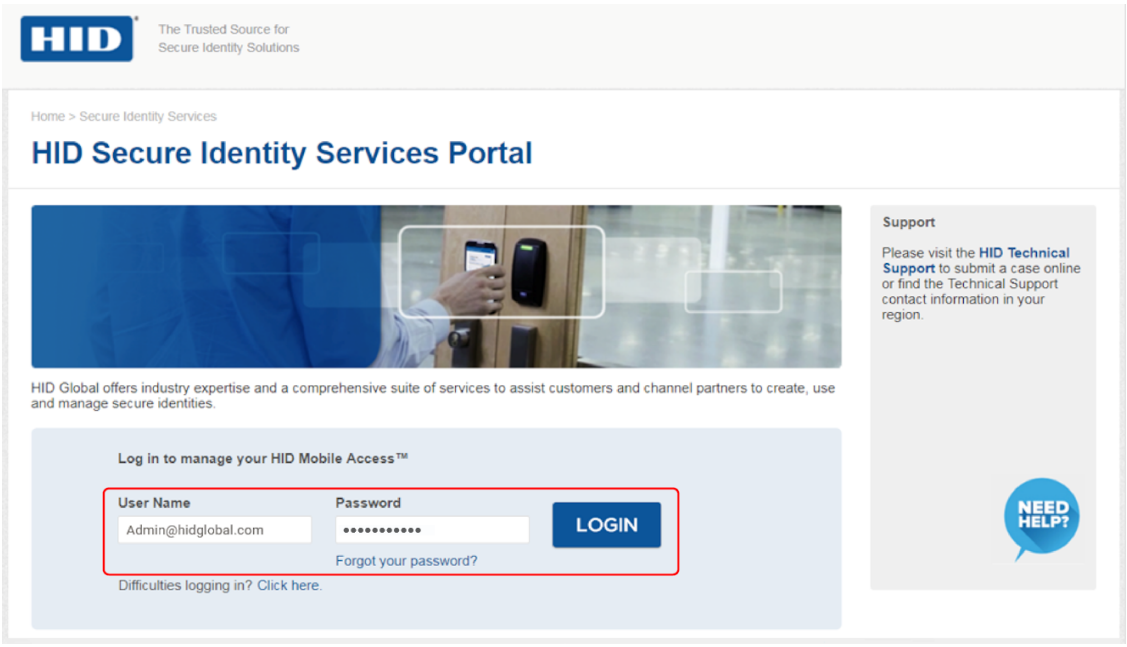


3.6 Add additional Reader Manager Admin

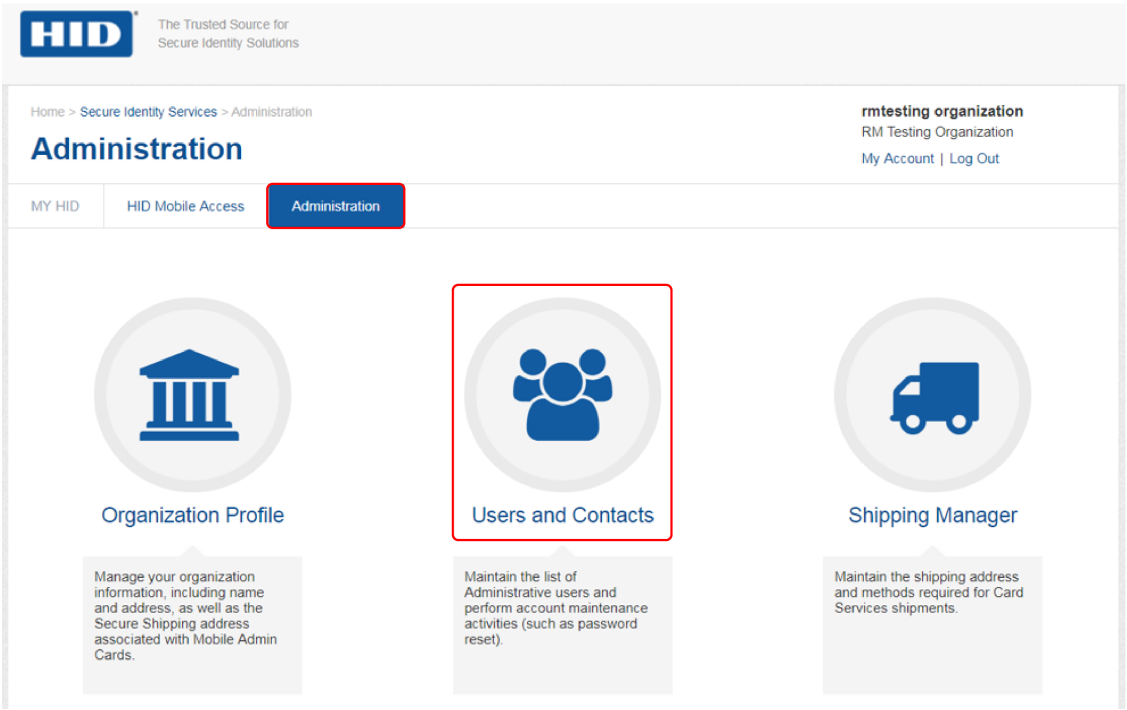
3.6.1 Add Reader Manager Admin (HID SIS Portal)

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

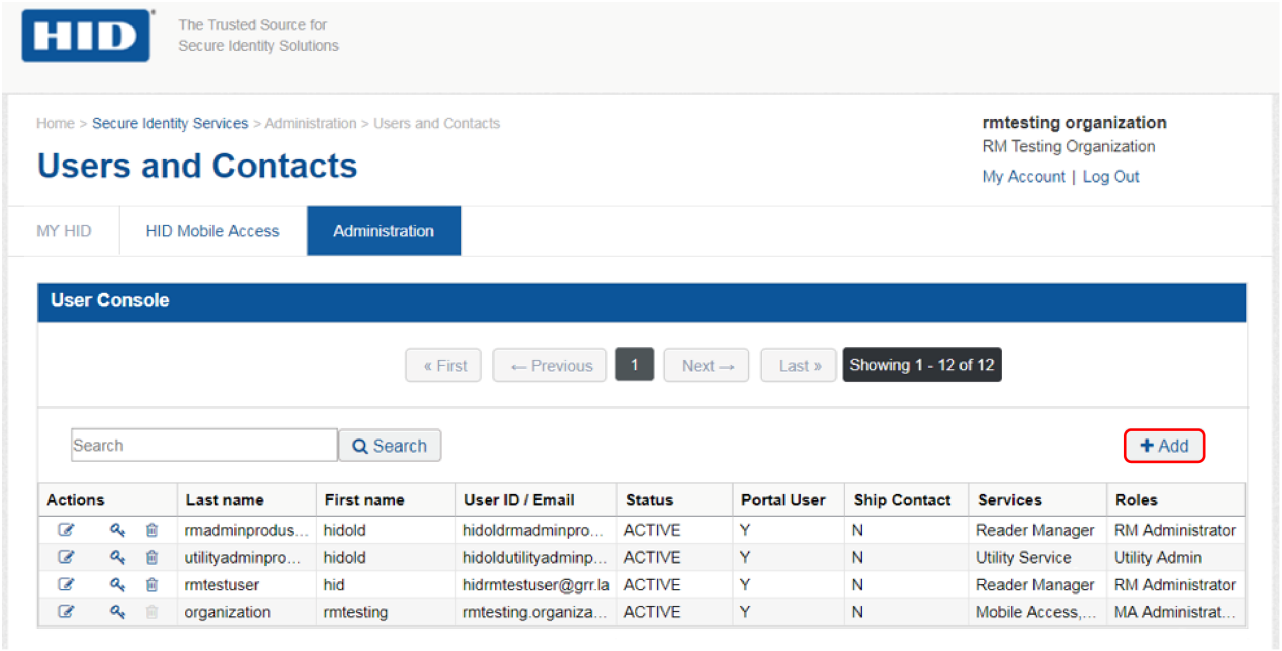
1. Log into the Portal as Organization Admin.



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

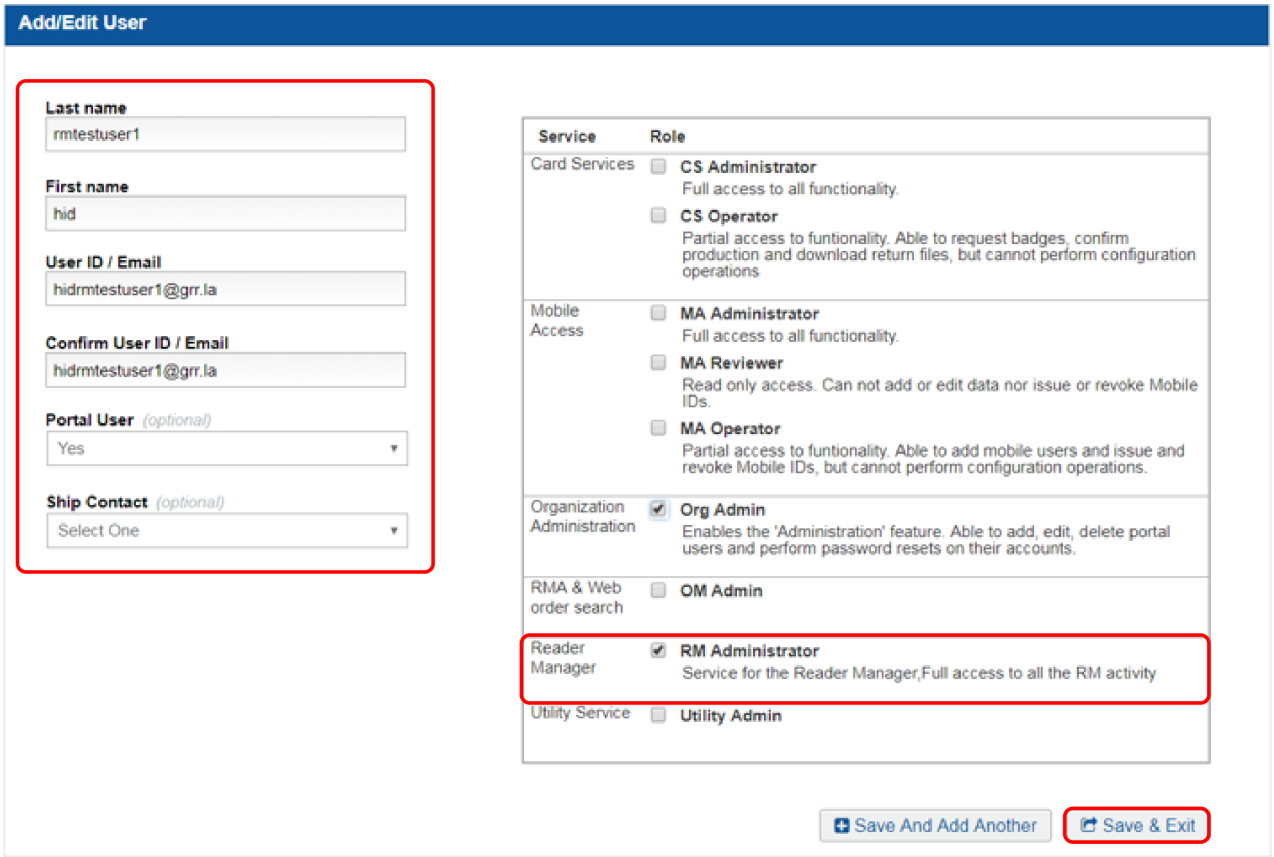


4. In the **User Console** section click **Add**.

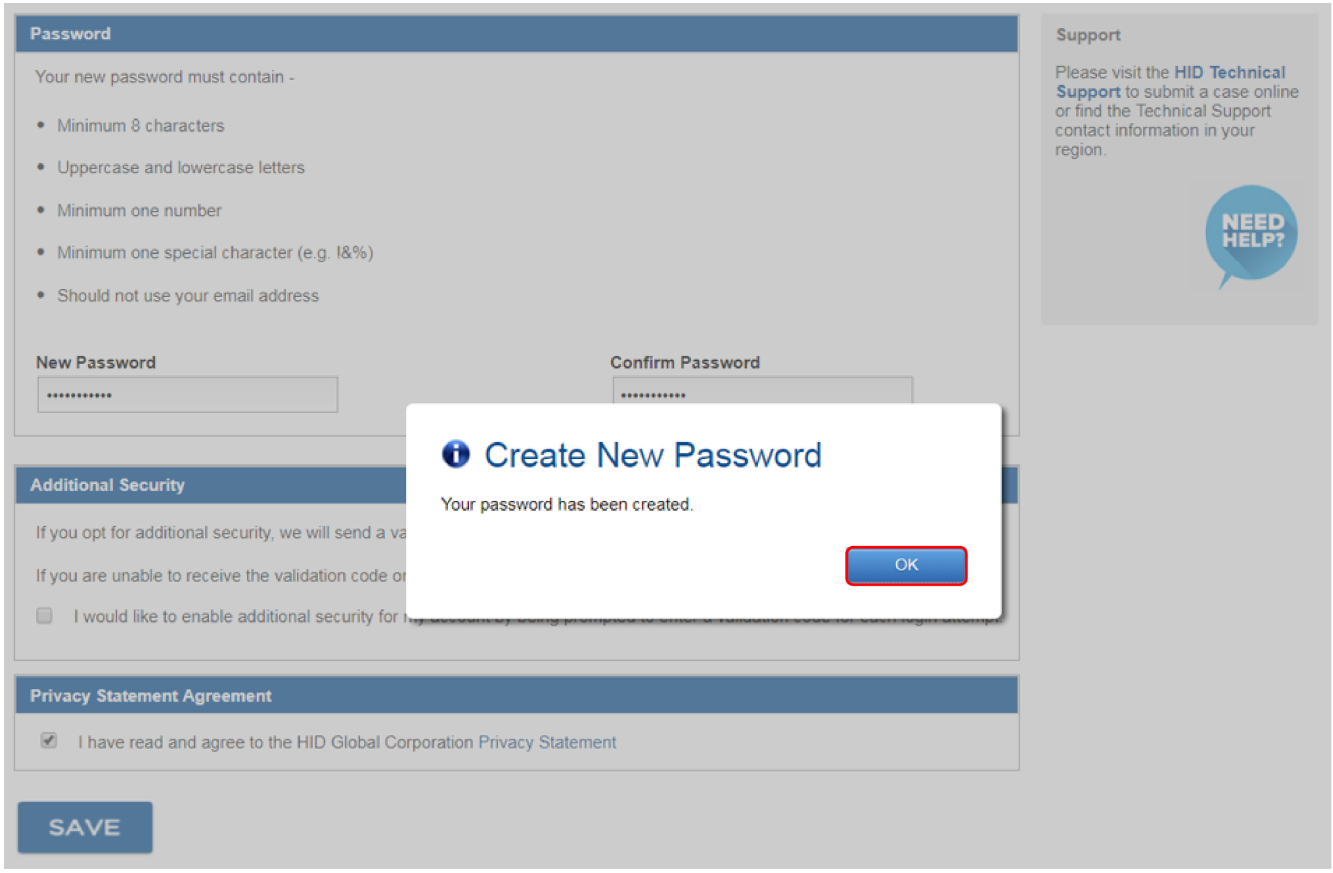


5. In the **Add/Edit User** section, enter the administrator details and enable the **RM Administrator** option.

6. Click **Save & Exit** and log out of the SIS Portal.



7. The newly created RM Administrator should check their email inbox for a mail 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.

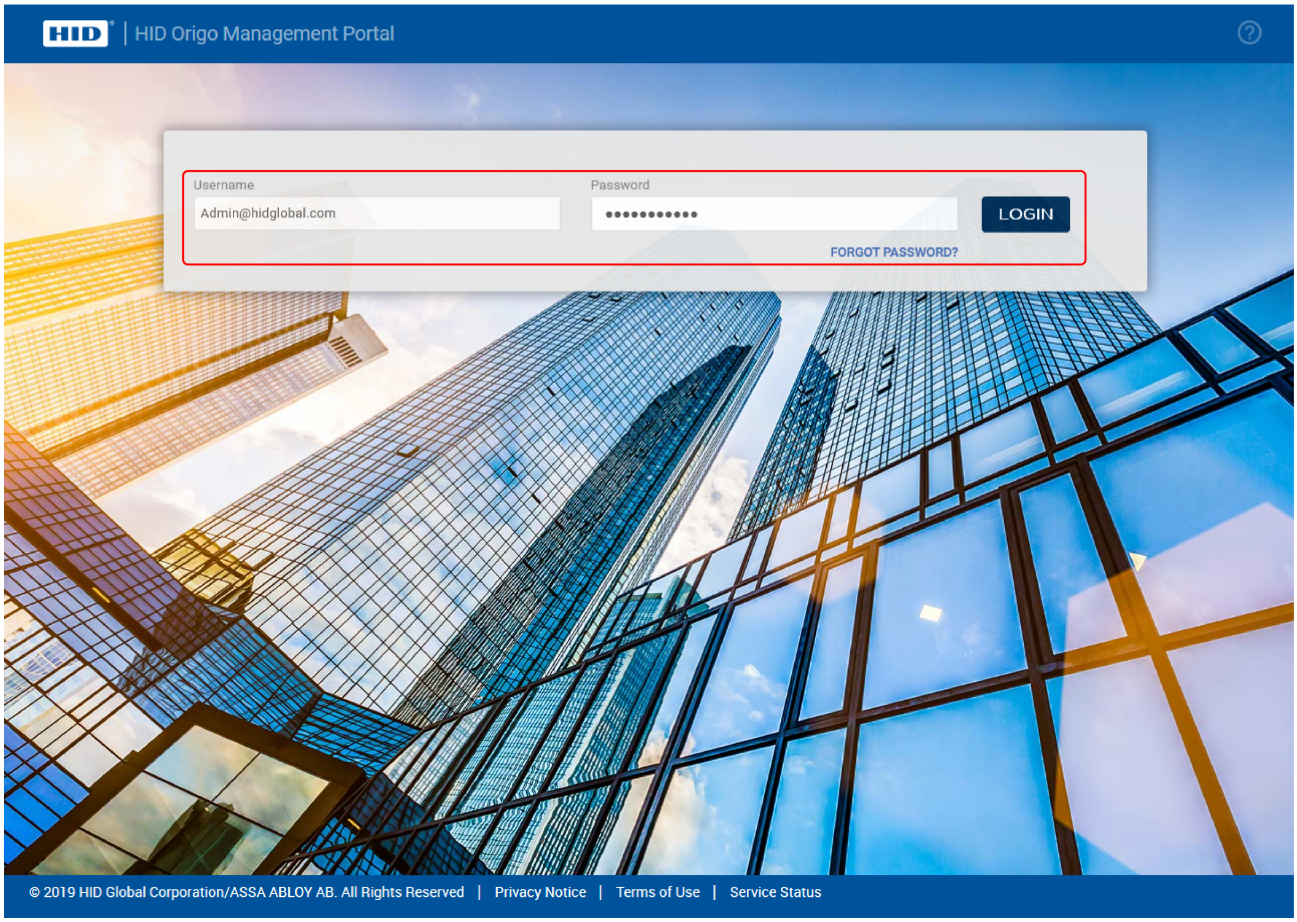


10. The RM Administrator can now log back into the SIS Portal using their new password and select the **HID Reader Manager** link to be redirected to HID Reader Manager. For detailed information, see **Access the HID Reader Manager Portal (HID SIS Portal)**.

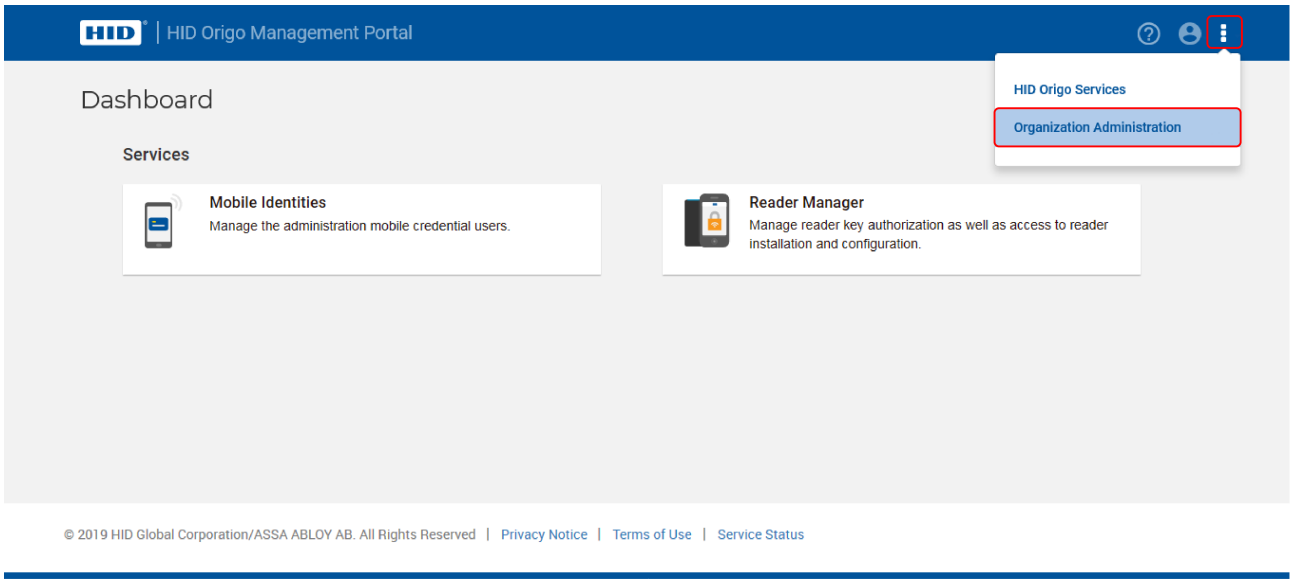
3.6.2 Add Reader Manager Admin (HID™ Origo® Management Portal)

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

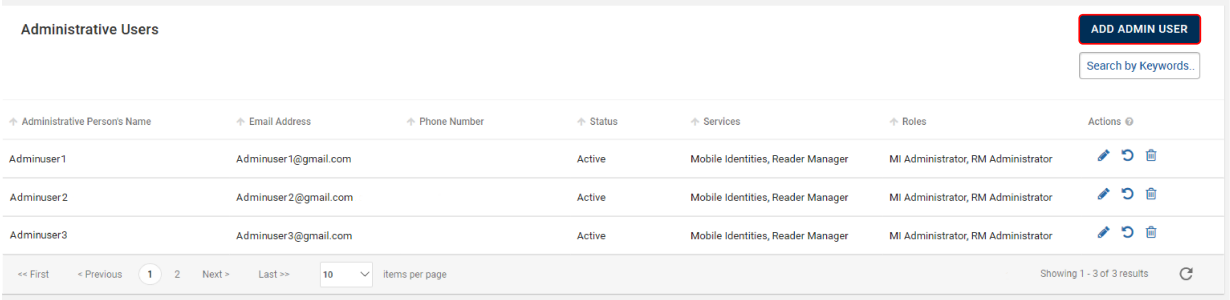
1. Log into the Portal as Organization Admin.



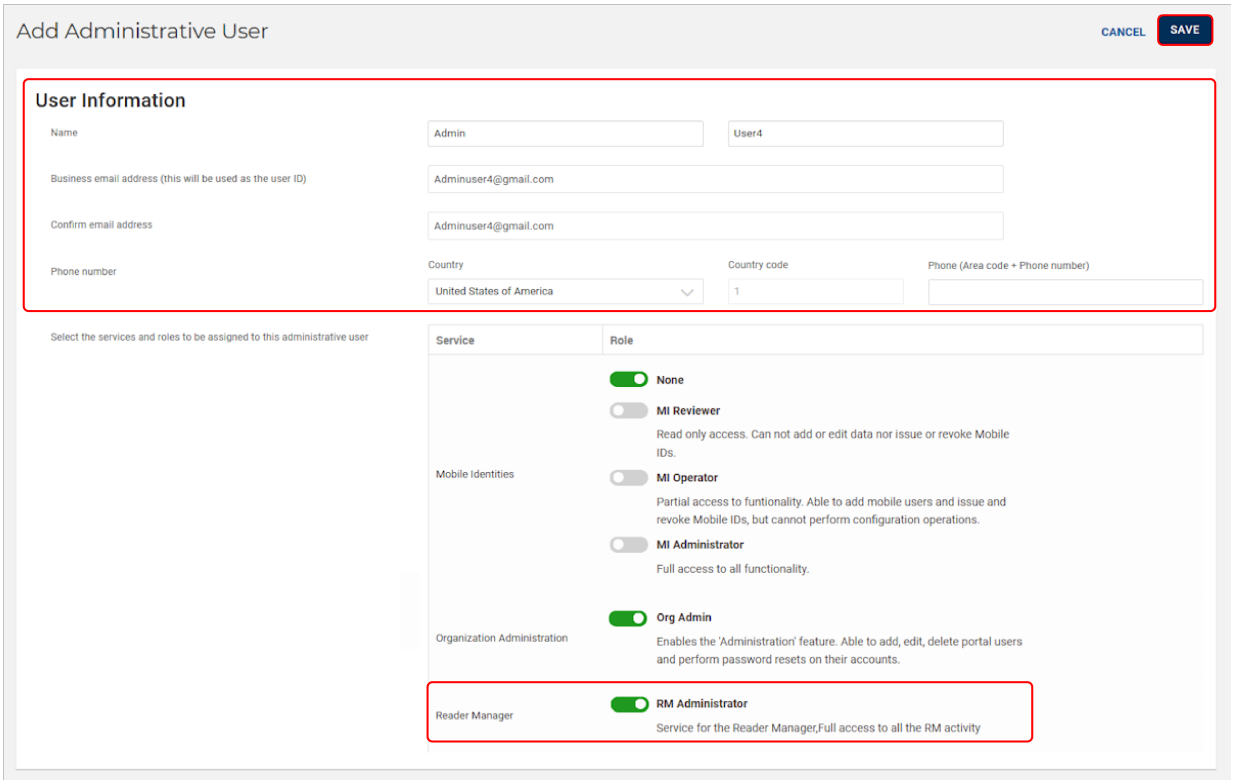
2. Select the menu icon [⋮] on the **Dashboard** screen, then select **Organization Administration**.



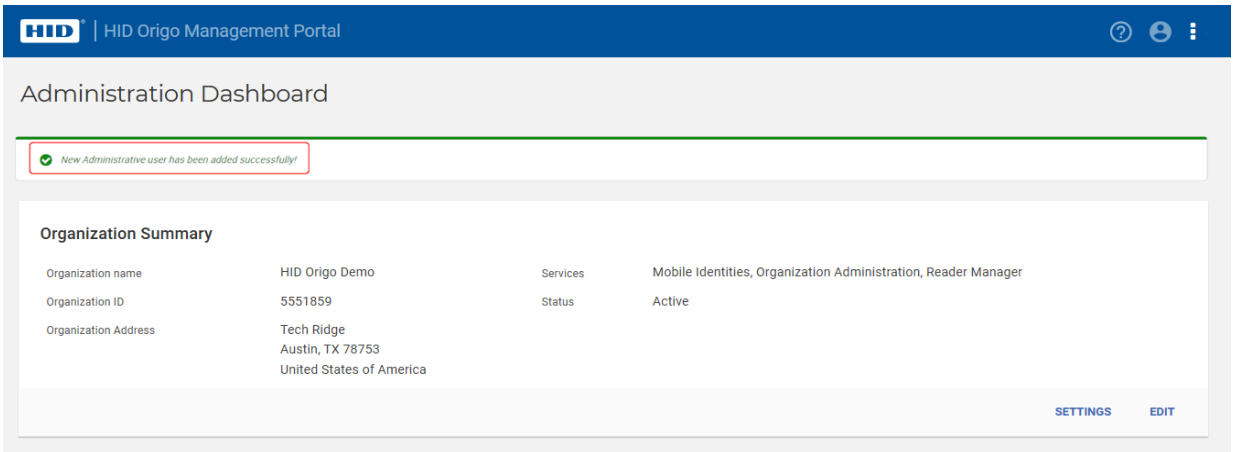
3. In the **Administrative Users** section, click **ADD ADMIN USER**.



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

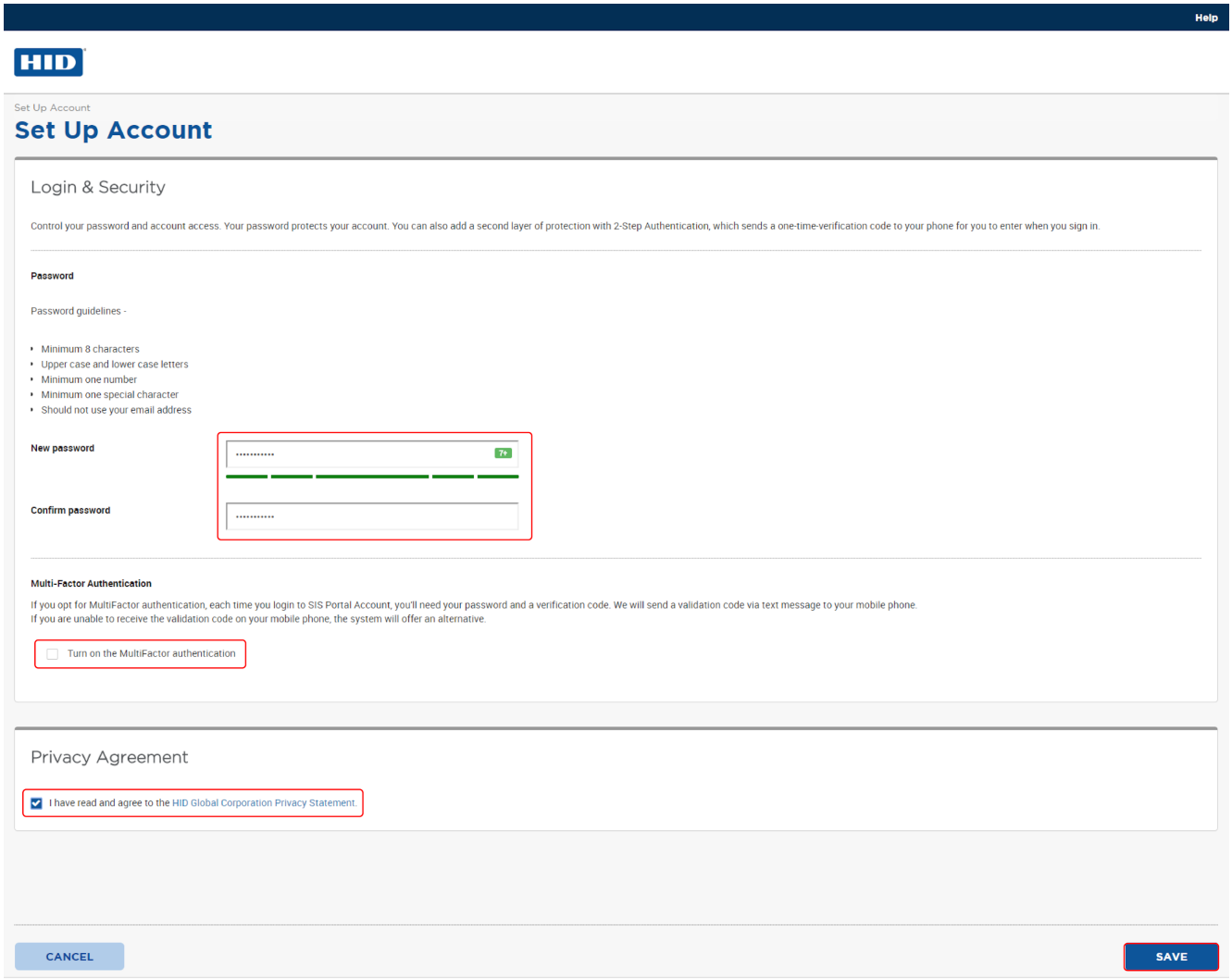


5. You will be notified that a new administrative user has been added. Click **Logout** to exit the Portal.



6. The newly created Reader Manager Administrator should check their email inbox for an email containing a username, a temporary password, and a Portal landing page link. Click the **Here** link in the email to be directed to the Portal **Set Up Account** page.

7. On the **Set Up Account** page, create a new password (refer to the on screen password requirements). If required, opt for additional login security. Accept the Privacy Statement Agreement and click **SAVE** to log out of the Portal.

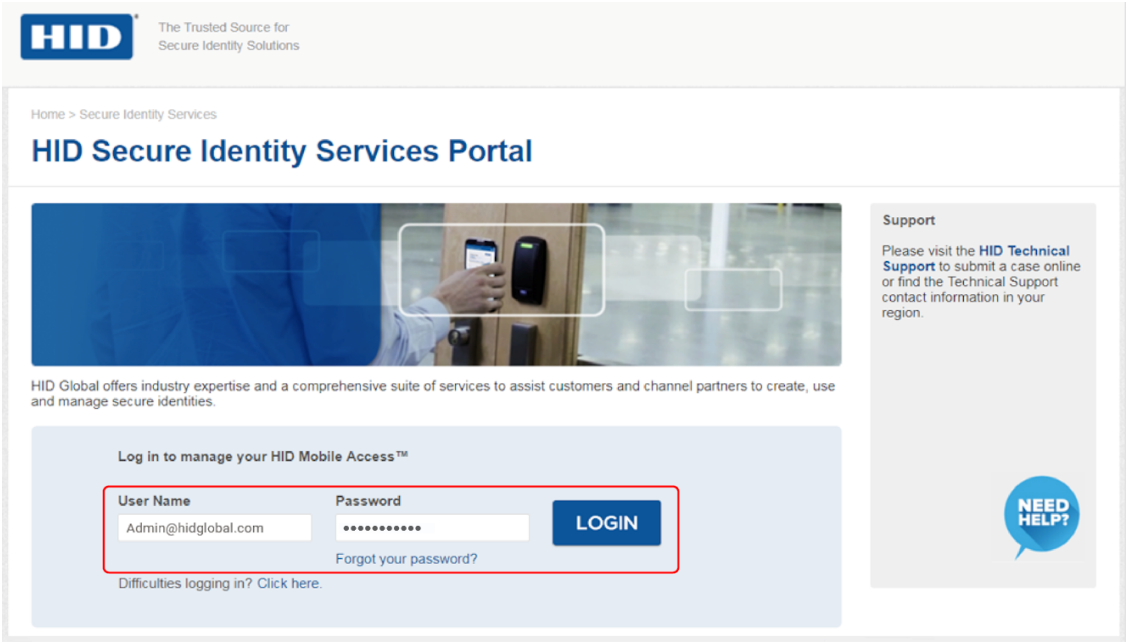


8. The RM Administrator can now log back into the HID Origo Management Portal using their new password and select the **Reader Manager** option to be redirected to HID Reader Manager. For detailed information, see **Access the HID Reader Manager Portal (HID® Origo™ Management Portal)**.

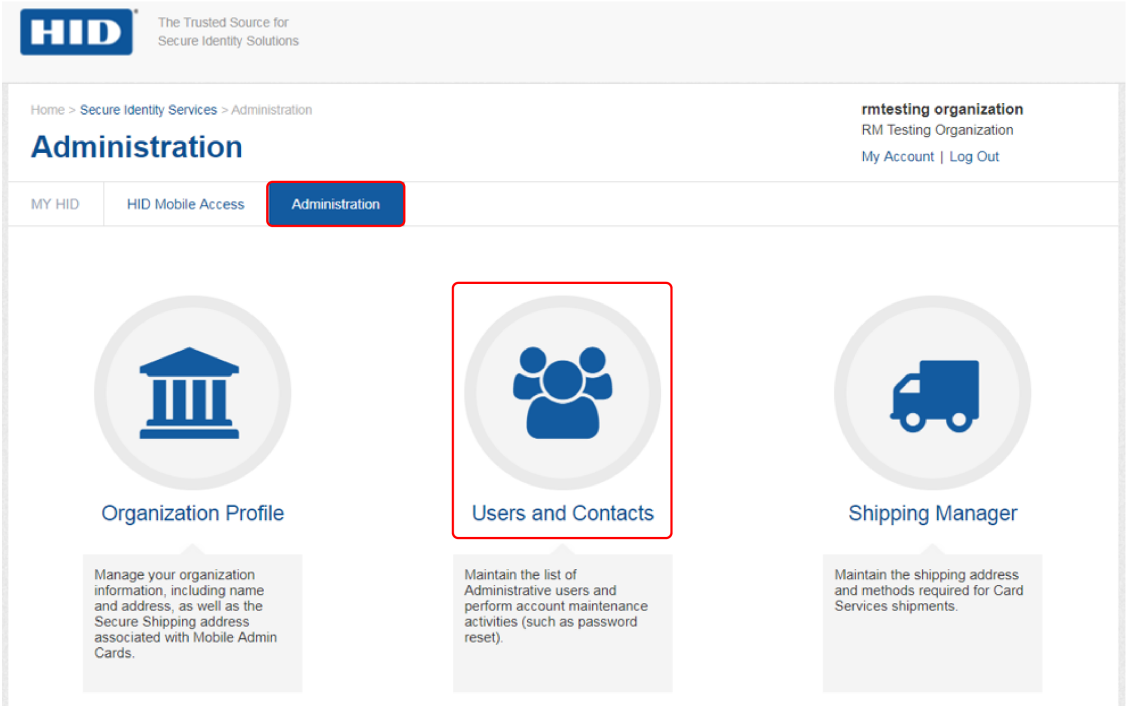
3.7 Edit existing Admin Services and Roles

3.7.1 Edit Admin Services and Roles (HID SIS Portal)

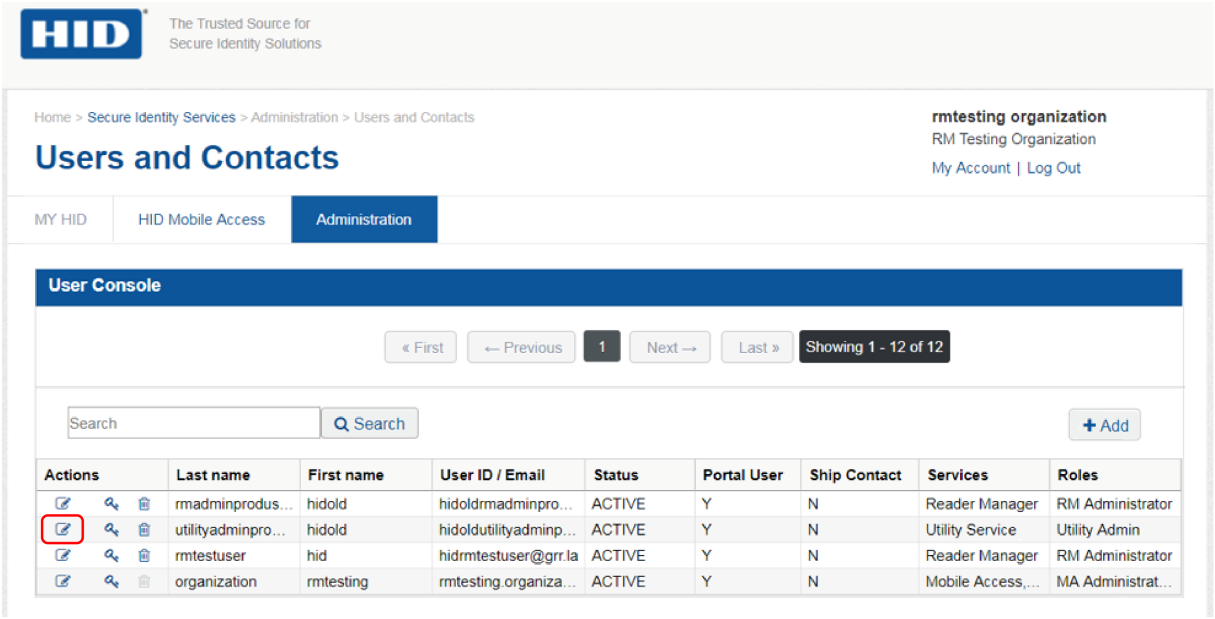
1. Log into the HID SIS Portal as Organization Admin.



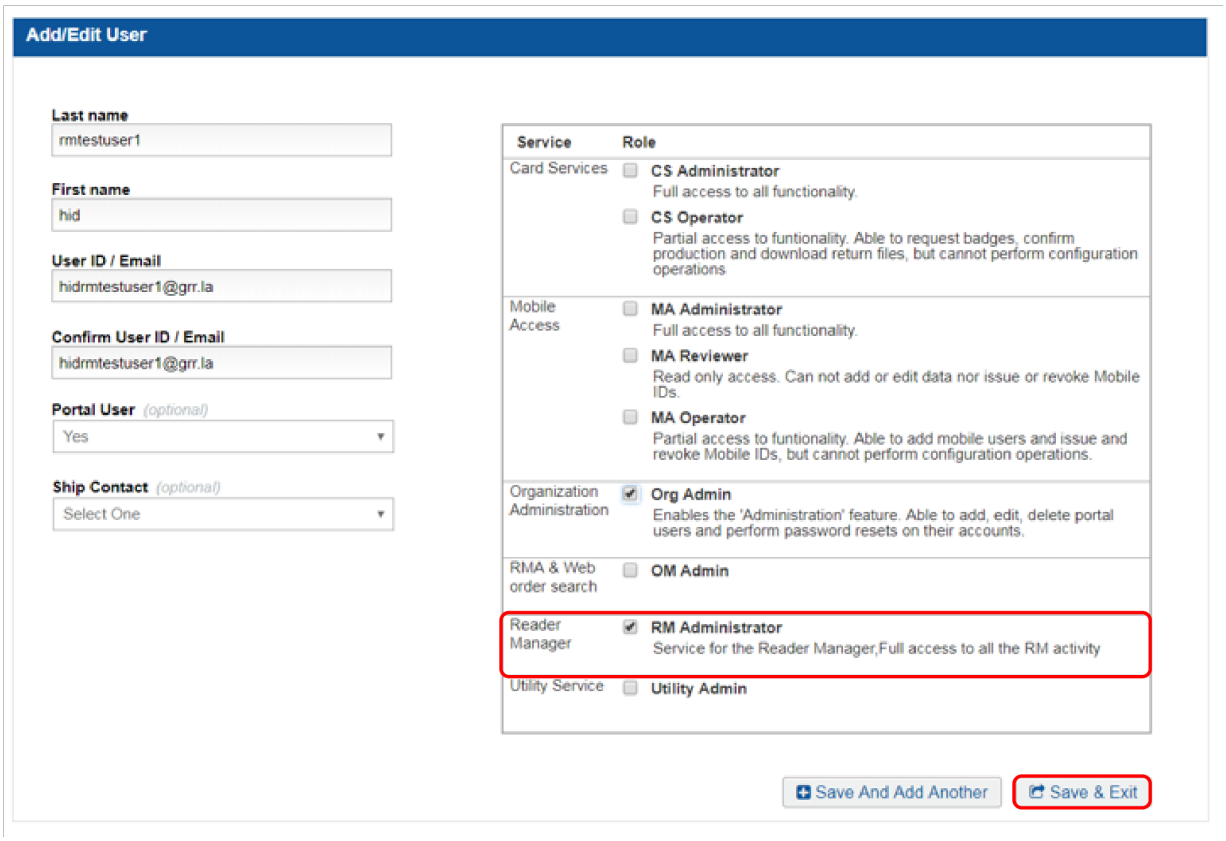
2. Select the **Administration** tab.
3. Select **Users and Contacts**.



4. In the **User Console** section click on the edit icon [✎] associated with a listed user.



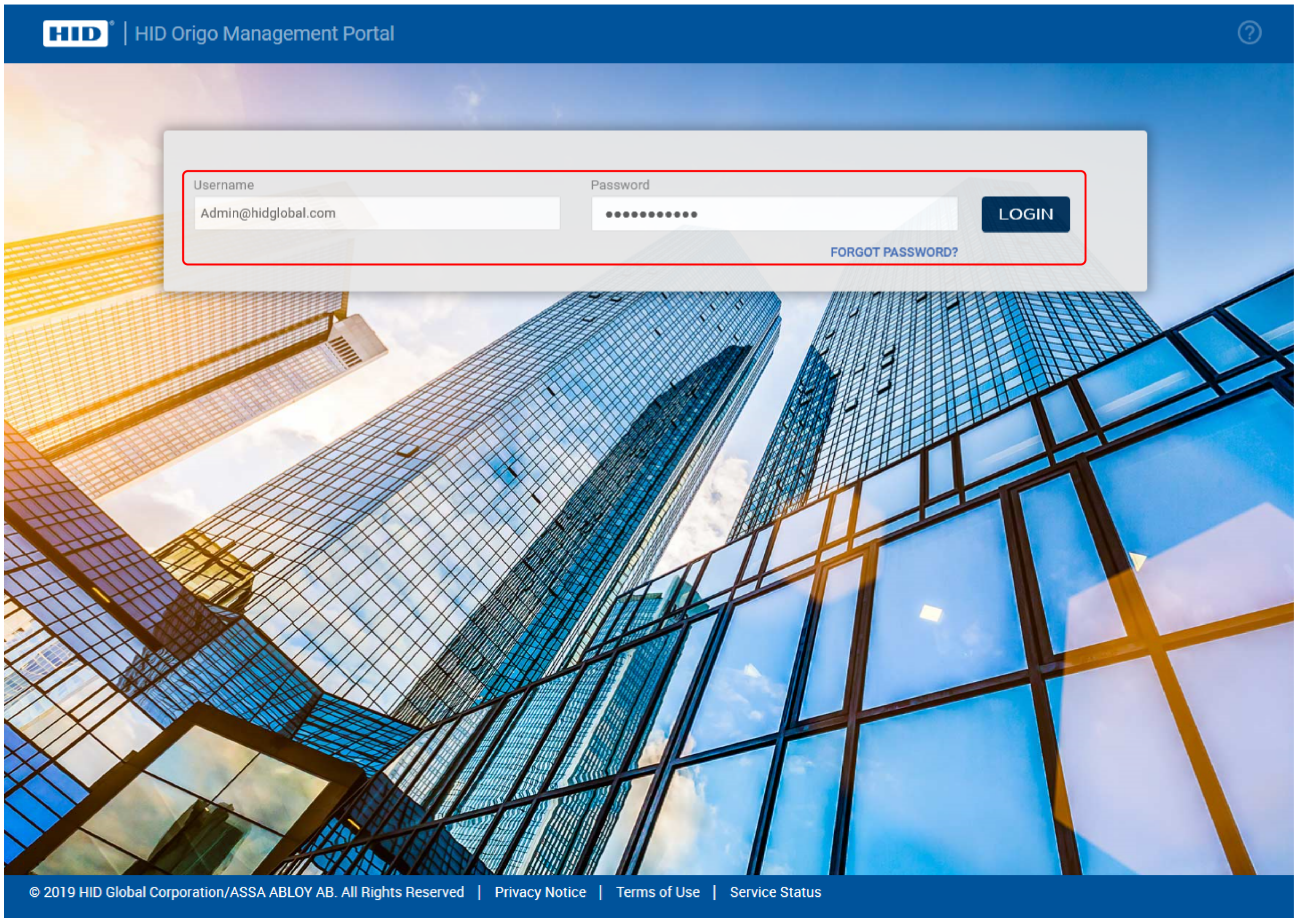
5. In the **Add/Edit User** section, enable the **RM Administrator** option.
6. Click **Save & Exit** and log out of the portal.



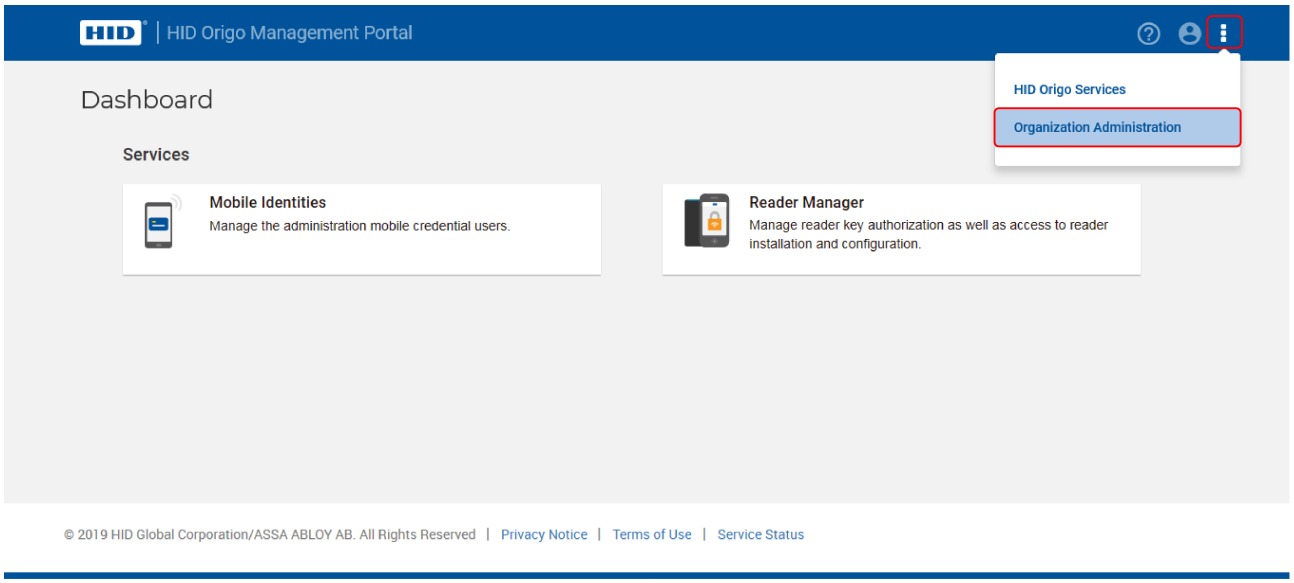
7. The RM Administrator can now log back into the SIS Portal and select the **HID Reader Manager** link to be redirected to HID Reader Manager. For detailed information, see **Access the HID Reader Manager Portal (HID SIS Portal)**.

3.7.2 Edit Admin Services and Roles (HID™ Origo® Management Portal)

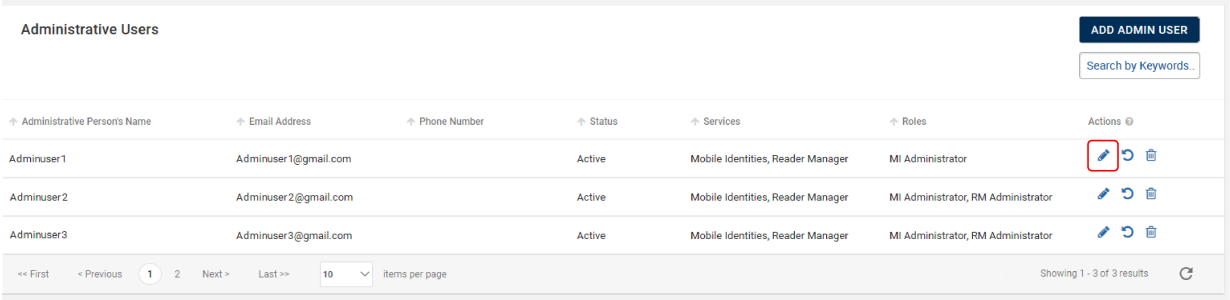
1. Log into the HID Origo Management Portal as Organization Admin.



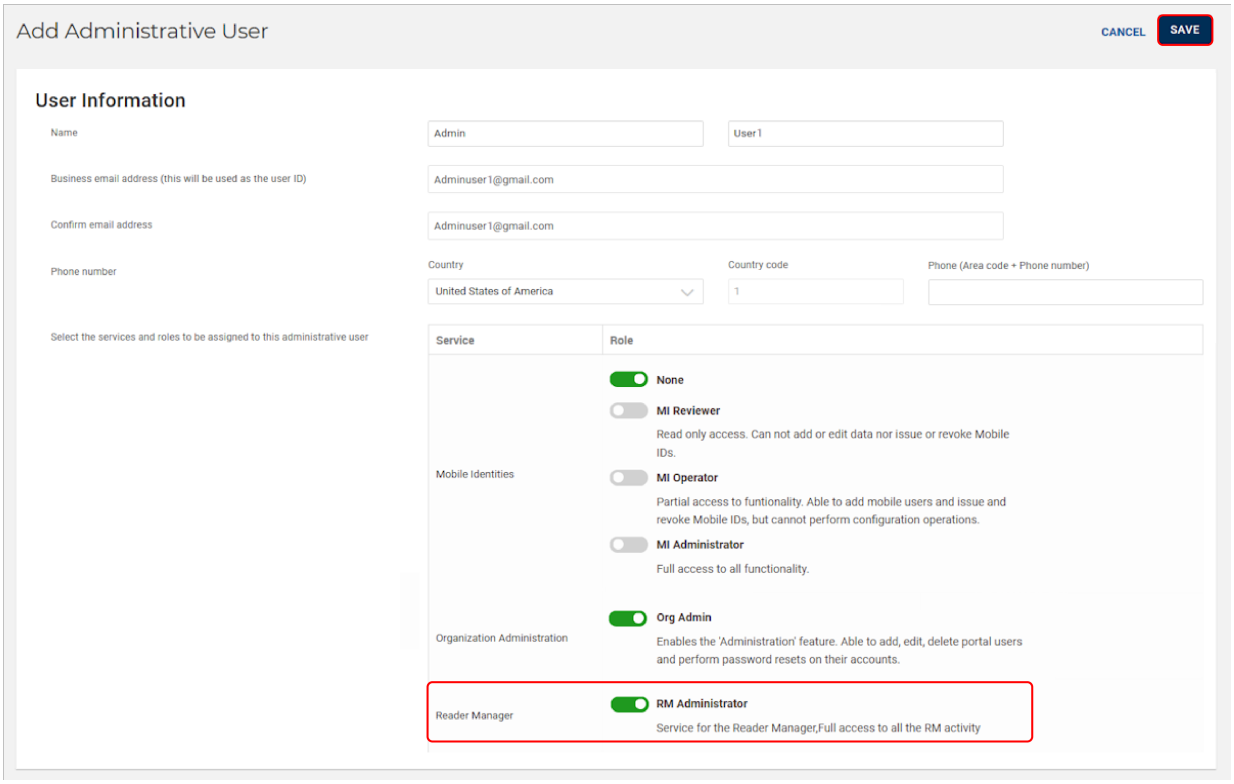
2. Select the menu icon [⋮] on the **Dashboard** screen, then select **Organization Administration**.



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



4. In the **Service**/**Role** table enable the **RM Administrator** option.
5. Click **Save** and and log out of the portal.



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

Section 04
Troubleshooting

Powering
Trusted Identities

4.1 Reader Manager App messages

4.1.1 Error and warning messages

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

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

4.1.2 Information messages

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

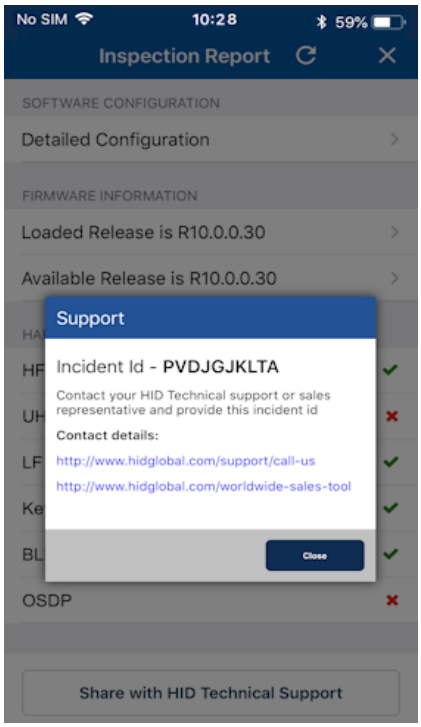
4.1.3 Validation messages

Message	Description and next step to attempt resolution
"New Password is not compliant to requirements"	The new Password entered has not met the password requirement rules. Please use a password which meets the requirements detailed on the screen.
"New Password & Confirm New Password are not same"	The entered Password and Confirm password do not match. Please re-enter passwords.
"Invalid old Password"	A previously used password has attempted to be used. Please use a different password.
"No Configuration item has been selected"	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 **Share with HID Technical Support**.
2. Take a note of the displayed **Incident Id** number and contact HID Technical Support. Refer to **https://www.hidglobal.com/support**.



Appendix **A**
Reader upgrade

Powering
Trusted Identities

A.1 Verify reader firmware compatibility

Supported iCLASS SE/multiCLASS SE Rev E firmware versions:

Reader Firmware	Admin Configuration	Supported?	Comment
R7 SP1	Standard	Yes	Requires module firmware from 8.6.0.4 release
R7 SP1	ICE/MOB	Yes	Requires module firmware from 8.6.0.4 release
R7 SP3	Standard	Yes	Requires module firmware from 8.6.0.4 release
R7 SP3	ICE/MOB	Yes	Requires module firmware from 8.6.0.4 release
R7 SP8	Standard	Yes	Requires module firmware from 8.6.0.4 release
R7 SP8	ICE/MOB	Yes	Requires module firmware from 8.6.0.4 release
R8.4.0.6	Standard	Yes	Requires module firmware from 8.6.0.4 release
R8.4.0.6	ICE/MOB	Yes	
R8.4.1.0	Standard	Yes	Requires module firmware from 8.6.0.4 release
R8.4.1.0	ICE/MOB	Yes	
R8.4.2.0	Standard	Yes	Requires module firmware from 8.6.0.4 release
R8.4.2.1	ICE/MOB	Yes	
R8.5.0.9	Standard	Yes	Requires module firmware from 8.6.0.4 release
R8.5.0.9	ICE/MOB	Yes	
R8.6.0.4	Standard	Yes	
R8.6.0.4	ICE/MOB	Yes	
R8.7	Standard	Yes	
R8.7	ICE/MOB	Yes	

A.2 iCLASS SE reader upgrade

A.2.1 iCLASS SE Bluetooth & OSDP upgrade kits

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

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

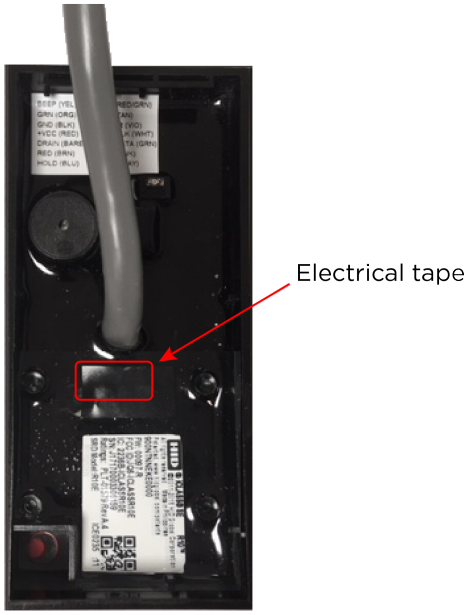
Upgrade kit part number	Description	Reader model
BLEOSDP-UPG-A-900	iCLASS SE Bluetooth & OSDP upgrade kit	R10/RP10
BLEOSDP-UPG-A-910	iCLASS SE Bluetooth & OSDP upgrade kit	R15/RP15
BLEOSDP-UPG-A-920	iCLASS SE Bluetooth & OSDP upgrade kit	R40/RP40
BLEOSDP-UPG-A-921	iCLASS SE Bluetooth & OSDP upgrade kit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

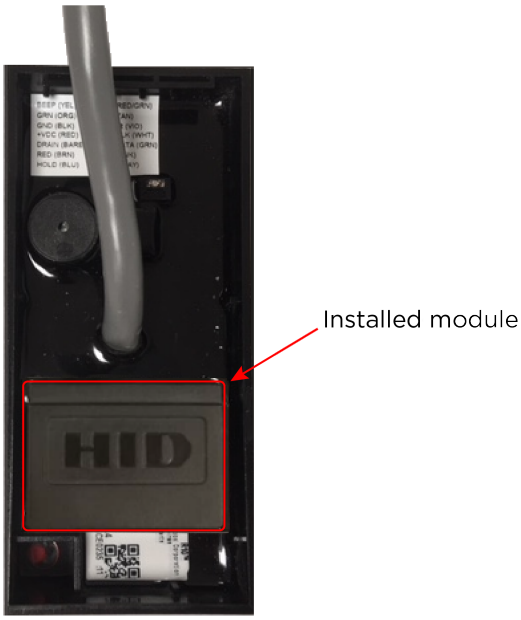
Note: The above iCLASS SE Bluetooth & OSDP upgrade kits can only be used for upgrading iCLASS SE/multiCLASS SE Rev E readers.

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

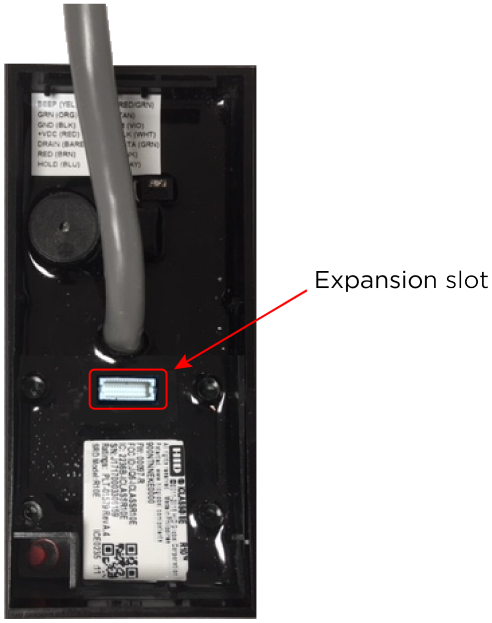
1. Disconnect power to the reader.
2. Remove the reader from the reader backplate.
3. On the back of the reader remove the electrical tape covering the module expansion slot.

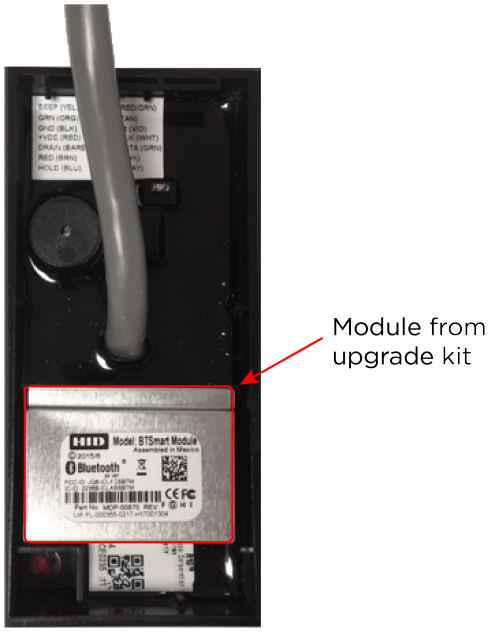
   Note: If the reader has a module already installed, remove this as it will be replaced with the module from the iCLASS SE Bluetooth & OSDP upgrade kit.





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.

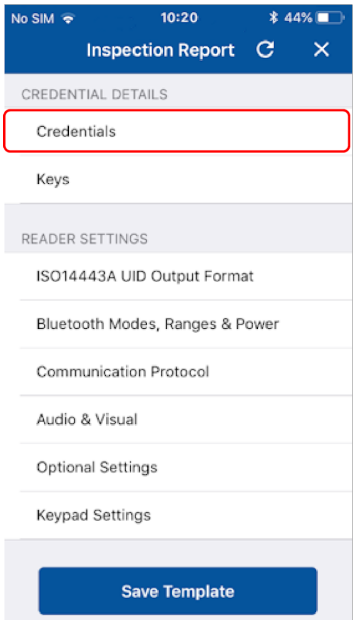
   Note: Different conductors are used for Wiegand vs OSDP communication.

A.2.3 Configure reader in HID Reader Manager

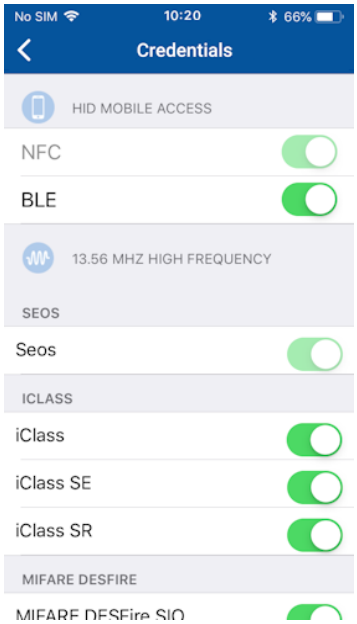
If the reader is ready to be configured, use the following procedure to configure the reader to support Bluetooth for HID Mobile Access and/or OSDP controller communication.

Note: This procedure assumes the Reader Technician has setup the HID Reader Manager app on a mobile device and the Reader Manager Administrator has enrolled the Reader Technician and issued key authorization in the HID Reader Manager Portal. See **Mobile application setup overview**.

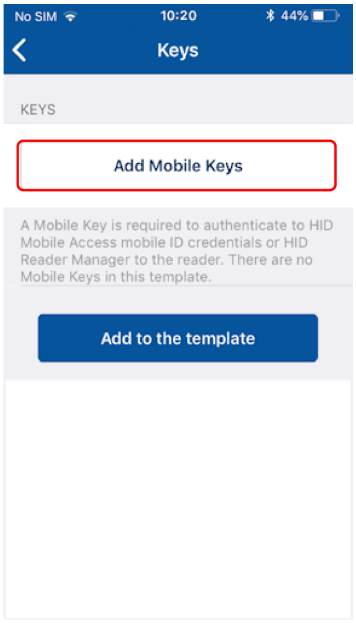
1. Log into the HID Reader Manager app.
2. Connect the HID Reader Manager app to the reader. See **Connect to a reader**.
3. In the HID Reader Manager app inspect the reader configuration and, if indicated, upgrade the reader firmware. See **Reader inspection report**.
4. To configure the reader to support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

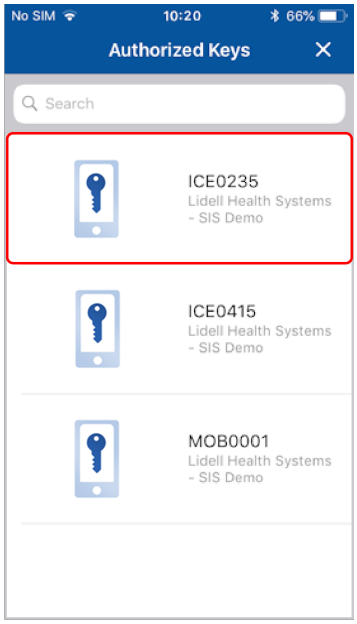


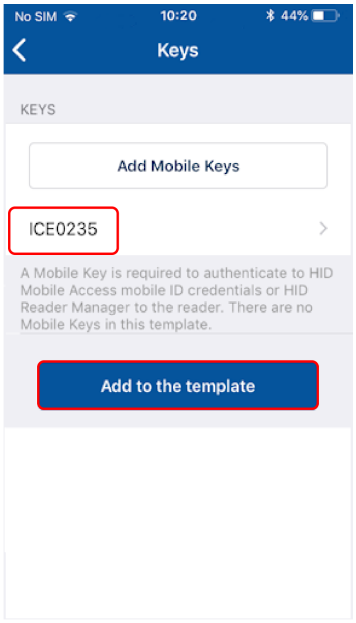
iCLASS SE / multiCLASS SE



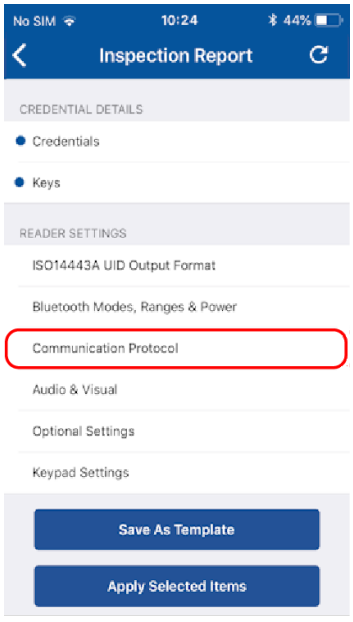
7. Tap **Add Mobile Keys** and select the authorization key to be loaded onto the reader (only one key can be loaded). The selected authorization key will be displayed on the screen.
8. Tap **Add to the template** to save.

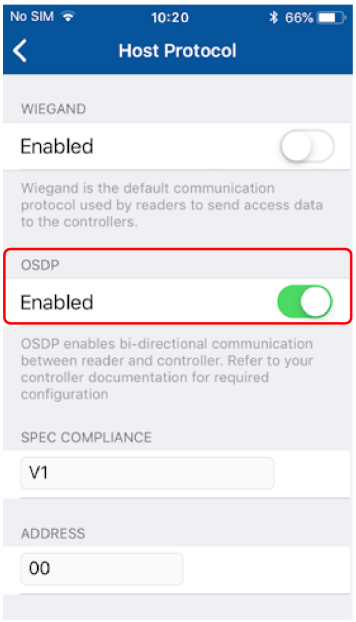


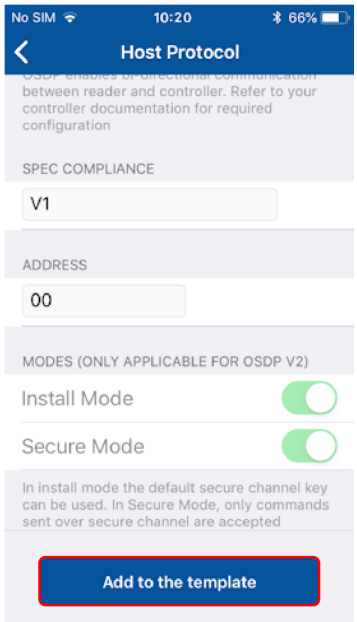




9. To configure the reader for OSDP controller communication (optional), in the **READER SETTINGS** section, tap **Communication Protocol**.
10. Enable the **OSDP** option and tap **Add to the template** to save.

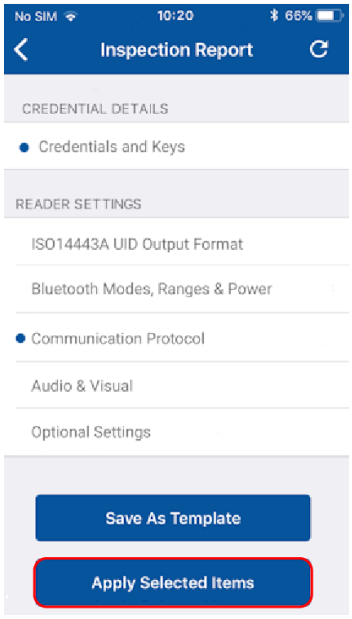


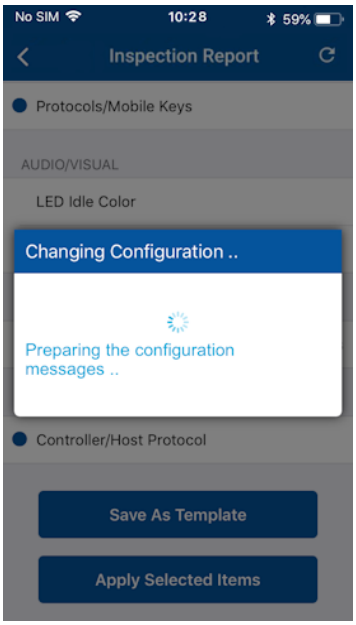


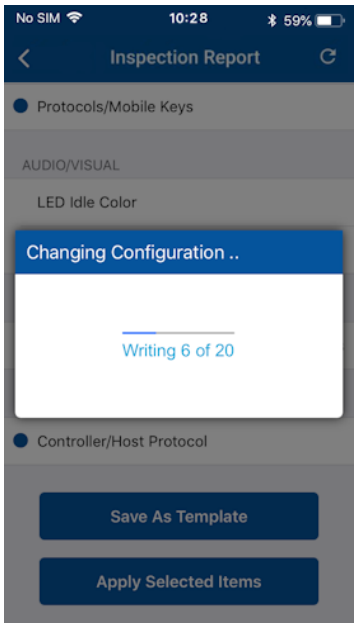


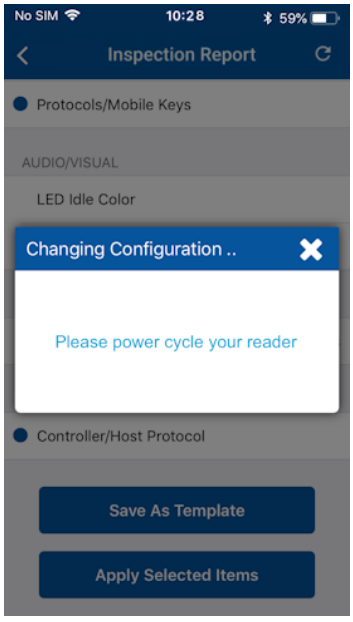
11. On the **Inspection Report** screen, tap **Apply Selected Items**. The selected configuration settings are applied to the reader.

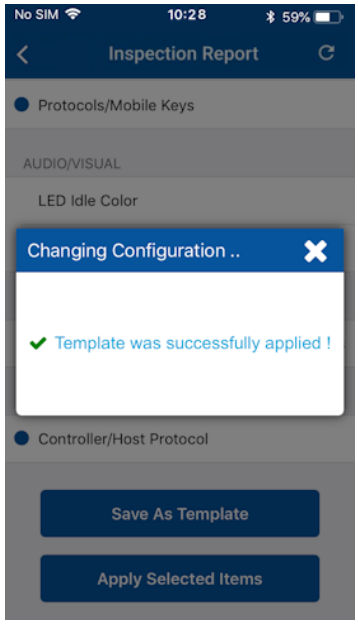
    Note: If the reader is a Standard enabled reader you will be prompted to power cycle the reader. For ICE/MOB enabled readers no reader power cycle is required.











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

Appendix **B**

Identify HID reader models

Powering
Trusted Identities

B.1 Physically inspect reader

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

1. Check the size of the reader to identify the reader as an R10 model. iCLASS/multiCLASS SE® readers and HID® Signo™ readers are available in different form factors for various installation environments, however the iCLASS SE® Express R10 reader is only available in the mini-mullion form factor, 1.9" x 4.1" x 0.9" (4.8 cm x 10.3 cm x 2.3 cm).
2. Once the reader model is identified check the reader front product labeling:
   - iCLASS/multiCLASS readers have a blue HID label with “iCLASS SE” or "multiCLASS SE".
   - iCLASS SE Express R10 reader only has the blue HID label.
   - HID Signo readers have grayscale HID labels.

iCLASS/multiCLASS SE R10

iCLASS SE Express R10

HID Signo 20

B.2 Check the product labeling

The HID reader model is printed on the product labeling. The product label is located on:

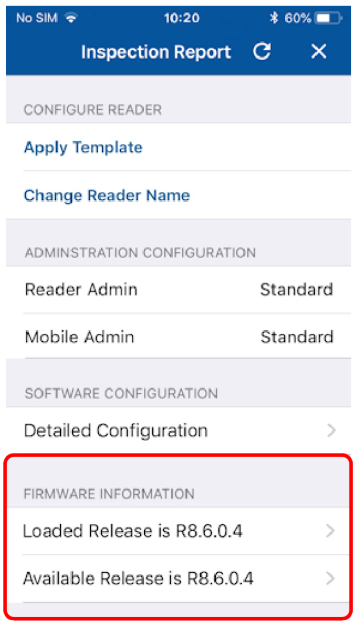
- The original box packaging in which the reader was supplied.
- The back of the reader.

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

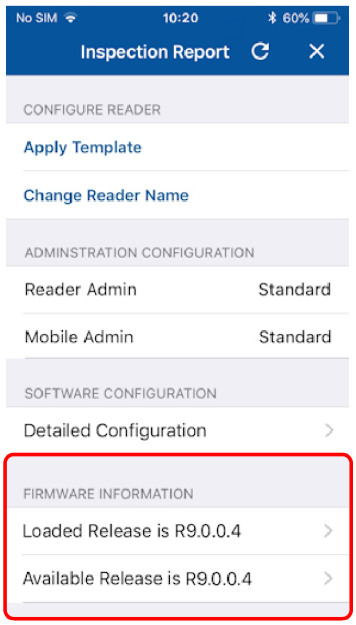
B.3 Check the reader firmware version with Reader Manager

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

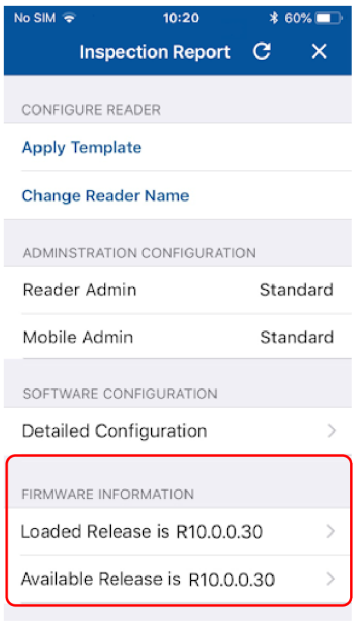
iCLASS/multiCLASS SE Rev E R10



iCLASS SE Express R10



HID Signo



Appendix C
Glossary

Powering
Trusted Identities

C.1 Glossary

Term	Description
BLE	Bluetooth Low Energy (formerly marketed as Bluetooth Smart) is a wireless personal area network technology.
Credential Container	A mobile device which holds a credential.
End customer	The Organization that uses HID products and services.
Invitation code	Invitation codes are issued to users as the first step in registering a new device. Invitation codes consist of a 16-character alphanumerical sequence and are used to authenticate devices and associate them with the relevant user.
MA	HID Mobile Access®. Mobile access is the use of a mobile device, such as a smartphone, tablet or wearable, to gain access to secured doors, gates, networks, services and more.
MFA	Multi-Factor Authentication. A security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login or other transaction.
Mobile credential/Mobile ID	Virtual credentials that are stored on a mobile device. Mobile IDs are issued and/or revoked via the HID Mobile Access portal. Mobile IDs are unique to each device and cannot be copied. If a user switches devices, a new Mobile ID must be issued.
Mobile-enabled readers	Mobile-enabled readers are fully activated and personalized to support an organization's specific Mobile ID's. These readers can only be ordered after the organization has completed registration for HID Mobile Access or HID Elite program. MOB or ICE Mobile Keyset will be required at time of order.
Mobile-ready readers	Mobile-ready readers are prepared to support HID Mobile Access but lack the personalized configuration (Mobile Keyset) to read an organization's specific Mobile ID's. These readers can be ordered at any time but will require field activation after the organization has completed registration for HID Mobile Access. To support a specific organization's Mobile IDs, these readers need to be personalized (Mobile Keyset loaded) using the HID Reader Manager App or a Mobile Key Card.
Mobile Keyset (MOB or ICE)	Mobile Keyset is a reference number for a set of cryptographic keys loaded into a reader. Mobile IDs, Mobile Key cards, and Mobile Admin cards will securely authenticate only with readers programmed with a matching keyset. An organization is assigned a Mobile Keyset upon registration into either the HID Elite™ (ICE) or HID Mobile Access (MOB) programs. The correct Mobile Keyset must be supplied when ordering mobile-enabled readers, Mobile IDs, Mobile Key cards, and Mobile Admin cards.
Opening modes	The following opening modes can be enabled/disabled using the HID Reader Manager App. When approaching a reader these interactions can be performed with a mobile device for access: ■ Tap (including Enhanced Tap): The mobile device is brought very close to, or touching, the reader (a similar user experience to using a physical credential). ■ Twist and Go:The mobile device holder initiates access by twisting the mobile device in a sharp 90 degree rotation in either direction (a similar motion to using a physical door handle). Typically used when the mobile device is at a longer distance from the reader. ■ App Specific:This entrance opening mode is specific to an application, for example, widget opening from a wearable such as a smartwatch.
Organization Administrator	User with sufficient privileges to add new Reader Manager Administrator users.

Term	Description
Organization ID	Organization ID is a reference number for a unique account within the Mobile Access Portal. It is assigned at the conclusion of account registration. The correct Organization ID must be supplied when ordering Mobile IDs and Mobile Admin cards.
OSDP	Open Supervised Device Protocol (OSDP) is an access control communications standard developed by the Security Industry Association (SIA) to improve interoperability among access control and security products.
Reader Manager Administrator	User with full access to all HID Reader Manager 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.

Revision history

Date	Description	Revision
September 2019	Updated the following sections for the functionality to enable/disable High Frequency and Low Frequency credentials for iCLASS SE readers: ■ Section 2.3.1.1 Credential and Keys settings. ■ Section 2.3.6 View detailed reader configuration. ■ Appendix A - Configure reader in HID Reader Manager.	A.3
July 2019	Updates implemented: ■ Section 2.3.1 Create a new template. Updated section for the select reader option and select charging profile option for iCLASS SE Express. ■ Section 2.3.6 View detailed reader configuration. Updated section for enable/disable Mifare & Desfire UID and Priority options for iCLASS SE Express. ■ Section A.2.2.1 Configure reader in HID Reader Manager. Updated section for enable/disable Mifare & Desfire UID and Priority options for iCLASS SE Express. ■ Section 2.3.5 Update reader firmware and Section 2.3.7 Apply configuration changes. Added note relating to “SNMP Authentication Failed” message. ■ Section 4.1.1 Error and warning messages. Updated Error and warning message table for “SNMP Authentication Failed” message.	A.2
January 2019	Updates implemented for Reader Manager 1.1.0 and support for the iCLASS SE Express R10: ■ Section 2.3 Basic app functionality. Updated sections for new and changed template configuration settings. ■ Section 3.5.2 Enroll Reader Manager Admin (HID Origo Management Portal) ■ Appendix A - Configure reader in HID Reader Manager. Updated section for new settings. ■ Appendix B - Identify HID reader models. New section.	A.1
September 2018	Initial release for Reader Manager 1.0.	A.0

Powering
Trusted Identities

PLT-03683, A.4

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

Support: 866-607-7339
Fax: 949-732-2120

Asia Pacific 19/F
625 King's Road
North Point
Island East
Hong Kong
Support: 852-3160-9833
Fax: 852-3160-4809

Europe, Middle East & Africa
Phoenix Road
Haverhill, Suffolk
CB9 7AE
United Kingdom
Support: 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