

# HID<sup>®</sup> Reader Manager<sup>™</sup> Solution User Guide (iOS)

PLT-03683, A.4 May 2020



# Copyright

 $\ensuremath{\textcircled{\sc c}}$  2020 HID Global Corporation/ASSA ABLOY AB. All rights reserved.

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

# Trademarks

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

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	19/F 625 King's Road North Point, Island East Hong Kong	
Phone: +1 866 607 7339	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**.

Introduction	5
1.1 Document purpose	6
1.2 Intended audience	6
1.3 HID Reader Manager solution overview	7
1.3.1 Key authorization	
1.4 Reader and Mobile device compatibility	8
1.4.1 Readers	8
1.4.2 Mobile devices	8
HID Reader Manager App	
2.1 Mobile application setup overview	10
2.1.1 Prerequisites	
2.1.2 HID Reader Manager setup overview	
2.1.3 Download and install the Reader Manager app	
2.1.4 Register a new account within the app	12
2.1.5 Log into the HID Reader Manager app	14
2.1.6 Activate the HID Reader Manager app	
2.1.7 Display authorized keys	
2.1.8 HID Reader Manager app settings	
2.2 Reader configuration	
2.2.1 Test configuration changes	19
2.3 Basic app functionality	20
2.3.1 Create a new template	
2.3.2 Manage templates	
2.3.3 Connect to a reader	34
2.3.4 Reader inspection report	
2.3.5 Firmware upgrade	
2.3.6 View detailed reader configuration	
2.3.7 Apply configuration changes	40
2.3.8 Change reader name	41
HID Reader Manager Portal	42
3.1 Mobile Access setup	43
3.1.1 Reader Manager Portal setup	
3.2 Access the HID Reader Manager Portal	44
3.2.1 Access the HID Reader Manager Portal (HID SIS Portal)	44
3.2.2 Access the HID Reader Manager Portal (HID® Origo™ Management Portal)	47
3.3 Enroll a Reader Technician	50
3.3.1 Edit Reader Technician information	53
3.3.2 Delete an enrolled Reader Technician	55

3.4 Issue authorization keys	
3.4.1 Edit authorization key information	
3.4.2 Revoke (delete) an authorization key	61
3.5 Configure HID Reader Manager Portal settings	64
3.5.1 Export Reader Technician record settings	65
3.5.2 Invitation Email settings	65
3.5.3 Configure Delete Threshold	66
3.6 Add additional Reader Manager Admin	67
3.6.1 Add Reader Manager Admin (HID SIS Portal)	67
3.6.2 Add Reader Manager Admin (HID™ Origo® Management Portal)	70
3.7 Edit existing Admin Services and Roles	73
3.7.1 Edit Admin Services and Roles (HID SIS Portal)	73
3.7.2 Edit Admin Services and Roles (HID™ Origo® Management Portal)	75
Troubleshooting	77
4.1 Reader Manager App messages	
4.1.1 Error and warning messages	
4.1.2 Information messages	
4.1.3 Validation messages	
4.2 Contact HID Technical Support	
Reader upgrade	82
A.1 Verify reader firmware compatibility	
A.2 iCLASS SE reader upgrade	
A.2.1 iCLASS SE Bluetooth & OSDP upgrade kits	
A.2.2 iCLASS SE/multiCLASS SE Bluetooth & OSDP upgrade kit instructions	85
A.2.3 Configure reader in HID Reader Manager	
Identify HID reader models	
B.1 Physically inspect reader	
B.2 Check the product labeling	
B.3 Check the reader firmware version with Reader Manager	
Glossary	
C.1 Glossary	



# Section 01 Introduction

## **1.1 Document purpose**

Powering

**Trusted Identities** 

This document provides an overview of the HID<sup>®</sup> Reader Manager<sup>™</sup> 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<sup>®</sup>/multiCLASS SE<sup>®</sup> readers, the iCLASS SE<sup>®</sup> Express R10 reader and HID<sup>®</sup> Signo<sup>™</sup> readers.
- Update reader firmware for supported iCLASS SE/multiCLASS SE readers, the iCLASS SE<sup>®</sup> 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<sup>™</sup> 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 <u>Appendix Reader</u> 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

#### HID<sup>\*</sup> 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<sup>®</sup> Reader Manager<sup>™</sup> 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<sup>™</sup> or Mobile (MOB) key users:

- A Mobile Access account is established for the organization through the HID Global onboarding process. See <u>Mobile Access setup</u>.
- A HID Reader Manager Portal instance is available for the Organization. See <u>Reader Manager Portal</u> <u>setup</u>.
- 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:

- 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 **<u>Register a new</u>** <u>account within the app</u>.

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 <u>HID Reader Manager Portal</u>.
- 2. The Reader Technician activates the issued invitation code in the HID Reader Manager app. See **Activate the HID Reader Manager app**.
- The Reader Technician verifies key authorization has been received in the HID Reader Manager app. See <u>HID Reader Manager Portal</u>.

#### HID Powering Trusted Identities

#### 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.







#### Powering Trusted Identities

#### 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.

	10:20	\$ 66% 🔲 ·	No SIM 😤	10:20
	Login		🗸 Login	User Validation
			MY ACCOU	INT
			Email	address
				Submit
Sign in to ir	nspect, configure HID Readers.	and update		
	Email address	6		
	Password			
	Sign In			
E	orgot Password	d ?		

Note: If the entered email address is associated with an existing HID Origo<sup>™</sup> 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**.



#### Powering Trusted Identities

- 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**.

No SIM 🗢 10:20 🖇 66% 💷	No SIM 🗢	10:20	* 66% 💷	No SIM 🗢	10:20	* 66% 💷
User Validation License		Register	×		Register	×
Privacy Policy	MY ACCOUNT	r		COMPANY	NFORMATION	
License and User Agreement	Password	requirements:		Comp	any Name	
Library Copyright and Licenses	- At least 1 Upp - At least 1 Low	ercase letter ercase letter		Select	Country	
BOUNCY CASTLE	- At least 1 spec - At least 1 num	cial letter Iber		Addre	ss Line 1	
Copyright (c) 2000 - 2017 The Legion of the Bouncy Castle Inc. (https://www.bouncycastle.org)	Email ac	Idress		Addre	ss Line 2 (Option	al)
Permission is hereby granted, free of charge, to any person obtaining a copy of this software and	Passwor	rd		Addre	ss Line 3 (Option	al)
issociated documentation files (the "Software"), o deal in the Software without restriction, ncluding without limitation the rights to use,	Confirm	password		City		
opy, modify, merge, publish, distribute, ublicense, and/or sell copies of the Software, and to permit persons to whom the Software is urnished to do so, subject to the following	CONTACT INF	ORMATION		State/	Province	
	First Na	me		Zip/Pc	ostal Code	
AGREE	Last Na	me				
DISAGREE	Mobile r	hone number			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.



#### Powering Trusted Identities

### 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.



No SIM 🗢	10:20	* 66% 💷					
	Setting	s About					
MY ACC	OUNT						
	firstName lastNa demo.installer@hid	me global.com					
Reme	ember Me						
Change	e Password						
	Sign Out						
ADMINIS	TRATION KEYS						
Show	Authorized	Keys →					
Show Enter In	Authorized	Keys >					
Show Enter II Administ HID Elite iCLASS S	Authorized nvitation Code ration Keys are requ or HID Mobile Acce SE Readers.	Keys					
Show Enter In Administ HID Elite iCLASS S	Authorized nvitation Code ration Keys are requ or HID Mobile Acces SE Readers.	Keys					









#### 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.



### Powering Trusted Identities

#### 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.

No SIM 🗢	10:20	\$ 66% 💷
	Settings	About
MY ACCO	UNT	
Remer Change	firstName lastName demo.installer@hidgloba mber Me Password	al.com
	Sign Out	
ADMINIST	RATION KEYS	
Show	Authorized Key	ys >
Enter In	vitation Code	
Administra HID Elite d iCLASS SI	ation Keys are required f or HID Mobile Access® E E Readers.	to manage Enabled
Home	Templates	<b>\$</b> Settings

#### **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<sup>®</sup>/multiCLASS SE<sup>®</sup> Rev E readers (with Bluetooth & OSDP module installed), the iCLASS SE<sup>®</sup> Express R10 reader, and HID<sup>®</sup> Signo<sup>™</sup> 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 <u>Apply</u> <u>configuration changes</u>.

#### 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.

SIM 🗢	10:20	\$ 66% 💶	No SIM 🗢	10:20	\$ 44% 💷
	Templates	+		Select Reader	×
Search			READER	TYPE	
			HID SI	igno	
			Seos F	Profile	
			Soft cha	rging profile is not applic	able for
Ν	o configuratio	n	ICLASS S	SE/MUITICLASS SE reader	S.
te	emplates foun	d	Enable	ed	
			Keypad i	s not applicable for iClass	s SE
			LAPICSS :	AK	
				ŬK	
		- Q-			



#### **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.

No SIM 🕿 10:20 ≵ 44% 🔲	No SIM 🔶
Inspection Report C ×	<b>&lt;</b> Cr
CREDENTIAL DETAILS	
Credentials	NEC
Keys	BLE
READER SETTINGS	
ISO14443A UID Output Format	13.56 MHZ
Bluetooth Modes, Ranges & Power	SEOS
Communication Protocol	Seos
Audio & Vieual	ICLASS
	iClass
Optional Settings	iClass SE
Keypad Settings	iClass SR
	MIFARE DESFIRE
Save Template	MIEADE DESEiro

No SIM 🔶	10:20	* 44% 💷
<	Credentials	
	OBILE ACCESS	
NFC		
BLE		
13.56	MHZ HIGH FREQUE	ENCY
SEOS		
Seos		
ICLASS		
iClass		$\bigcirc$
iClass SE		$\bigcirc$
iClass SR		$\bigcirc$
MIFARE DESF	IRE	
MIEARE DES	SEire SIO	$\cap$

No SIM 🗢 10:20	\$ 44% 🔲
Credentials	
MIFARE DESFIRE	
MIFARE DESFire SIO	$\bigcirc$
MIFARE DESFire CSN	$\bigcirc$
MIFARE CLASSIC	
MIFARE Classic SIO	$\bigcirc$
MIFARE Classic CSN	$\bigcirc$
125 KHZ LOW FREQUENCY	
HID Proximity and	$\bigcirc$
HID Dorado Proximity	$\bigcirc$
EM Proximity	$\bigcirc$
Add to the template	



#### 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.

No SIM 🗢	10:20 Build Template	* 66% 💷	No SIM 🗢	10:20 UID OUTPUT	* 44% 🔳
CREDENTIA	L DETAILS		ISO14443A U	ID OUTPUT FORMAT	
Credenti	als		32-BIT MSE	3	~
Keys			32-BIT LSB		
READER SE	TTINGS		26-BIT with	Facility Code 1	
ISO1444	3A UID Output Format		34-BIT MSE	3	
Bluetoot	h Modes, Ranges & Pov	wer	40-BIT MSE	3	
Commun	nication Protocol		37-BIT LSB		
Audio &	Visual		56-BIT LSB		
Optional	Settings		26-BIT MSE	3	
Keypad S	Settings		56-BIT MSE	3	
	Save Template		A	dd to the template	

#### **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.

No SIM 🗢	10:20	\$ 66% 💷	No SIM 🗢	10:20	* 66% 💷	No SIM 🔶	10:20 🛪	6
	Build Template	×	<	BLE Settings		<	BLE Settings	
REDENTIA	L DETAILS		TAP			Allow Ap	op Specific	
Credentia	als		Allow Ta	р				
Keys			Adjust Ran	ge (in dBm)		Adjust Ran	ge (in dBm)	
READER SE	TTINGS			-			74 +	
ISO1444	3A UID Output Format			40 +				
Bluetooth	h Modes, Ranges & Po	wer				This option opening mo	enables/disables the entra ode specific to an opening	ince
Commun	ication Protocol		This option Tap operation mobile device	enables/disables the t on is typically used wh ce is in close proximity	ap operation. len the y to the	application mobile devi is -75dBm (displad)	(for example, widget openi ices and wearables). Defaul and minimum is -40 dBm	ng It si
Audio & \	Visual		-40 dBm. A each individ	rox. 0 to 4 in). Default djust to best suit perfo lual reader.	setting is prmance for	ENHANCED	) TAP	
Optional	Settings		TWIST AND	GO		Allow En	hanced Tap	
Keypad S	Settings		Allow Tw	ist and Go	$\bigcirc$	This option	enables/disables the enha	nce
			Adjust Ran	ge (in dBm)		operation. I used when proximity to	Enhanced Tap operation is t the mobile device is in clos o the reader (approx. 0 to 4	typi se in)
	Save Template							

- 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	Тар	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.

No SIM 🗢	10:20	* 66% 💷	No SIM 🗢	10:20	* 66% 💷	No SIM 🔶	10:20	\$ 66% 💻
	Build Template	×	<	Host Protocol		<	Host Protocol	
CREDENTIA	L DETAILS		WIEGAND			between re controller d	ader and controller. R ocumentation for req	efer to your uired
Credenti	als		Enabled		$\bigcirc$	configuratio	n	
Keys			Wiegand is	the default communic	ation	SPEC COM	PLIANCE	
DEADED CE	TIMOS		protocol use to the contr	ed by readers to send ollers.	access data	V1		
ISO1444	3A UID Output Format		OSDP			ADDRESS		
Bluetoot	h Modes, Ranges & Por	wer	Enabled			00		
Commun	vication Protocol		OSDP enabl between rea	les bi-directional com ader and controller. R	munication efer to your	MODES (OF	ILY APPLICABLE FOR	OSDP V2)
Commun	ication Protocol		controller d configuratio	ocumentation for requ on	uired	Install M	ode	
Audio &	Visual		SPEC COMP	PLIANCE		Secure N	/lode	
Optional	Settings		V1			In install mo	de the default secure	e channel key
Keypad S	Settings		ADDRESS			can be used sent over s	d. In Secure Mode, on acure channel are acc	ly commands cepted
			00				Add to the templa	te
	Save Template							

#### **Audio & Visual settings**

- 1. From the **READER SETTINGS** section, tap **Audio & Visual**.
- 2. From the AUDIO/VISUAL section, tap LED Idle Color.
- 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.

ild Template	×	AUDIO/VISU	Audio & Visual	×	<	Led Idle Color
AILS		AUDIO/VISU	IAL			
					LED IDLE C	OLOR
		LED Idle Co	blor		Re	d
		Credential I	Read LED Color		Gr	een
S					Bl	he
D Output Format					Or	ange
les, Ranges & Pov	wer				Cy	/an
n Protocol					Ma	agenta
					W	hite
ıgs					He	ost Controlled
gs						
						Add to the template
	S D Output Format des, Ranges & Po In Protocol I Ings gs gs	SS D Output Format des, Ranges & Power in Protocol l l ngs gs	SS D Output Format des, Ranges & Power in Protocol i I Ings gs	SS D Output Format des, Ranges & Power in Protocol i gs gs	S D Output Format des, Ranges & Power in Protocol i gs gs	SS BOUTPUT Format BIL D Output Format C C V In Protocol MA I Inssertion C C V Inssertion C C C C C C C C C C C C C C C C C C C

- 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.

No SIM ᅙ	10:24 Audio & Visual	¥ 66%
AUDIO/VIS	UAL	
LED Idle C	olor	
Credential	Read LED Color	

#### **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.

No SIM 🗢	10:20	* 66% 💷	No SIM 🗢	10:24	\$ 66% 💷		No SIM 🗢	10:24	\$ 66% 💻
	Build Template	×		Optional Settings	×		<b>く</b> Back	Metal Tuning	
CREDENTIA	L DETAILS		OPTIONAL S	SETTINGS			METAL TUN	IING	
Credenti	als		Intelligen	t Power Management			AIR		
Keys			Velocity of	checking			When meta	I tuning is configured t	o be on, the
READER SE	TTINGS		Metal Tur	ning			to improve   environmen	cerformance on metal ts (also resulting in re-	duced
ISO1444	3A UID Output Format								
Bluetoot	h Modes, Ranges & Po	wer						Add to the templat	e
Commun	nication Protocol								Done
Audio &	Visual								
Optional	Settings								
Keypad S	Settings					-		AIR	
								AUTO	
	Save Template								

#### **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.

No SIM 🗢	10:20	\$ 66% 💷
	Build Template	×
CREDENTIAL	DETAILS	
Credential	5	
Kevs		
ISO14443	TINGS A UID Output Format	
Pluatooth	Modes Danser & Dawer	
Didecoord	nioues, kanges & Power	
Communic	cation Protocol	
Audio & Vi	isual	
Optional S	Settings	
Keypad Se	attings	
	Save As Template	
	Care no remplate	
	Apply Selected Items	

#### 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.

No SIM 🗢	10:20	* 66% 💷
	Build Template	×
CREDENTIAL D	DETAILS	
Credentials		
Keys		
READER SETTI	NGS	
ISO14443A	UID Output Format	
Bluetooth M	lodes, Ranges & Power	
Communica	tion Protocol	
Audio & Visi	ual	
Optional Set	ttings	
Keypad Sett	tings	
WALLET SETTI	INGS	
ECD Config	uration	

#### 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.

Build Template X   REDENTIAL DETAILS   Credentials   Keys   EADER SETTINGS   ISO14443A UID Output Format   Bluetooth Modes, Ranges & Power   Communication Protocol   Audio & Visual   Optional Settings   Save Template   Save Template   Save Template   Save Template   Communication Protocol   Audio & Visual   Optional Settings   Save Template   Save Template   Save Template   Category   Adds MOB0123, Blue LED, Twist n Go   VtEGORY   emo Category   emo Category	Build Template X   Save Template   EDENTIAL DETAILS   Credentials   Keys   ADER SETTINGS   SO14443A UID Output Format   Bluetooth Modes, Ranges & Power   Communication Protocol   Audio & Visual   Optional Settings   Save Template   X   LE   s MOB0123, Blue LED, Twist n Go   TEGORY   Save Template   X   Save Template	Build Template X   Save Template   DER SETTINGS   Old443A UID Output Format   uetooth Modes, Ranges & Power   ommunication Protocol   udio & Visual   otional Settings   Save Template   X   Save Template   X   M © 10:24 * 66% ●   Save Template   X   M © 10:24 * 66% ●   Category   Adds MOB0123, Blue LED, Twist n Go   Demo Category   Adds MOB0123, Blue LED, Twist n Go   E   MOB0123, Blue LED, Twist n Go   E   MOB0123, Blue LED, Twist n Go   E   E   MoB0123, Blue LED, Twist n Go   Demo Category   Adds MOB0123, Blue LED   E   Construction   Adds MOB0123, Blue LED, Twist n Go   Demo Category   Adds MOB0123, Blue LED, Twist n Go   Demo Category   Adds MOB0123, Blue LED   E   MoB0123, Blue LED, Twist n Go	6	10:20	* 66% 💷
DENTIAL DETAILS redentials redentials redentials reges DER SETTINOS CATEGORY Demo Category Corrections Consumination Protocol udio & Visual ptional Settings Save Template A    10:24   \$ 66%   C   Save Template  A    10:24   Templates C   Search Demo Category Adds MOB0123, Blue LED, Twist n Go EGORY mo Category	DENTIAL DETAILS   redentials   ByS   DER SETTINGS   CATEGORY   Demo Category   Letooth Modes, Ranges & Power   communication Protocol   udio & Visual   ptional Settings   Save Template   No SiM © 10:24   Yearch   Carecory   A © 10:24 * 66% ●   Demo Category   A © 10:24 * 66% ●   Demo Category   A © 10:24 * 66% ●   Demo Category   A © Search   Demo Category   Adds MOB0123, Blue LED, Twist n Go   EGORY   mo Category   Adds MOB0123, Blue LED, Twist n Go	DENTIAL DETAILS redentials redentials regentials regent	Bui	ild Template	×
Adds MOB0123, Blue LED, T Adds MOB0123, Blue LED, T Save Template 10:24 \$ 66% Save Template No SIM © 10:24 Templates CATEGORY Demo Category No SIM © 10:24 Templates Category Cover Template Category Cover Template Category Cover Template Category Cover Template Cover Template	Adds MOB0123, Blue LED, T Adds MOB0123, Blue LED, T CATEGORY Demo Category	Adds MOB0123, Blue LED, /S ER SETTINGS D14443A UID Output Format retooth Modes, Ranges & Power mmunication Protocol dio & Visual tional Settings Save Template No SIM © 10:24 Templates MOB0123, Blue LED, Twist n Go GORY No Category Adds MOB0123, Blue LED Twist n Go Save Template	NTIAL DET	AILS	
eys DER SETTINGS CATEGORY Demo Category Demo Category Ceree Template Category Demo Category Ceree Template Category Ceree Template Category Ceree Template Category Ceree Template Ceree Templa	eys DER SETTINGS S014443A UID Output Format Luetooth Modes, Ranges & Power ommunication Protocol udio & Visual iptional Settings Save Template M * 10:24 * 66% Save Template M * 10:24 * 66% LE M * 10:24 * 66% Demo Category Adds MOB0123, Blue LED, Twist n Go EGORY mo Category Adds MOB0123, Blue LED, Twist n Go	E E M 10:24 \$ 66% Bave Template M 0B0123, Blue LED, Twist n Go E E E Save Template Save Template Save Template CATEGORY Demo Category No SIM 10:24 Templates Category Save Template Category Save Template Category Save Template Category Save Template Category Adds MOB0123, Blue LED Category Adds MOB0123, Blue LED	dentials		
ADER SETTINGS S014443A UID Output Format Auetooth Modes, Ranges & Power communication Protocol audio & Visual aptional Settings Save Template Save Template M * 10:24 * 66% Save Template Save Template M * 10:24 * 66% Category No SIM * 10:24 Templates Q Search Demo Category Adds MOB0123, Blue LED, Twist n Go	ADER SETTINGS S014443A UID Output Format luetooth Modes, Ranges & Power communication Protocol udio & Visual Aptional Settings Save Template Save Template M © 10:24 * 66% Save Template LE S MOB0123, Blue LED, Twist n Go LE S MOB0123, Blue LED, Twist n Go M © Category Adds MOB0123, Blue LED, TeGORY mo Category Adds MOB0123, Blue LED, Credentials AV	DER SETTINGS CATEGORY Demo Category Demo Category Demo Category Save Template CATEGORY Demo Category No SIM  10:24 10:	s		
S014443A UID Output Format  Buetooth Modes, Ranges & Power Communication Protocol  uudio & Visual  Optional Settings  Save Template  Save Template  M 10:24 * 66%  Template  M 10:24 * 66%  Demo Category  LE  SMOB0123, Blue LED, Twist n Go  FEGORY mo Category	SQ14443A UID Output Format  Bluetooth Modes, Ranges & Power Communication Protocol  Audio & Visual Deptional Settings  Save Template  M  10:24 Save Template  M  10:24 Save Template  M  10:24 Templates  C Search Demo Category Adds MOB0123, Blue LED, Twist n Go  FEGORY mo Category Save Template	O14443A UID Output Format   uetooth Modes, Ranges & Power   ommunication Protocol   udio & Visual   ptional Settings   Save Template   X   Save Template   X   E   MOBB0123, Blue LED, Twist n Go   EGORY   no Category   Adds MOB0123, Blue LED, Twist n Go   EGORY   no Category   Save Template	R SETTING	S	
Huetooth Modes, Ranges & Power Communication Protocol udio & Visual Aptional Settings Save Template M * 10:24 * 66% Save Template Save Template	siluetooth Modes, Ranges & Power Communication Protocol udio & Visual Optional Settings Save Template M  10:24  4 66%  10:24 Save Template  No SiM  10:24 Templates LE s MOB0123, Blue LED, Twist n Go Demo Category Adds MOB0123, Blue LED, TEGORY mo Category Save Template	uetooth Modes, Ranges & Power  ommunication Protocol  udio & Visual  ptional Settings  Save Template  A   10:24	14443A UII	D Output Format	t
ommunication Protocol udio & Visual ptional Settings Save Template M  10:24  \$ 66%  10:24 Save Template  10:24 Templates C Search Demo Category Adds MOB0123, Blue LED, Twist n Go	ommunication Protocol udio & Visual ptional Settings Save Template M  10:24  66% No SiM  10:24 Templates LE No SiM  10:24 Templates Cearch Demo Category Adds MOB0123, Blue LED, Tegory mo Category Save Template	adio & Visual   ptional Settings   Save Template   Save Template   M © 10:24 * 66%    Save Template   E   MOB0123, Blue LED, Twist n Go   EGORY   no Category   Save Template	tooth Mod	les, Ranges & Po	ower
udio & Visual ptional Settings Save Template M  10:24  66%  10:24 Save Template  10:24 Templates C Search Demo Category Adds MOB0123, Blue LED, Tecory mo Category	udio & Visual ptional Settings Save Template M  10:24  \$ 66%  No SIM  10:24 Templates LE s MOB0123, Blue LED, Twist n Go Demo Category Adds MOB0123, Blue LED, Credentials AV	rdio & Visual ptional Settings Save Template A ● 10:24 ★ 66% ● Save Template ★ 10:24 E E MOB0123, Blue LED, Twist n Go Demo Category Adds MOB0123, Blue LED Credentials AV	nmunicatio	n Protocol	
bptional Settings Save Template M	Apptional Settings  Save Template  M  10:24 66% 10:24 Cemplate  No SIM 10:24 Templates  Cemplate  Cemplate  Cemplate  Cemplate  Save Template	Save Template   Image: Save Template   Image: Save Template   Save Template   Image: Save Template	io & Visual	I	
Save Template  M  10:24 866% 10:24 10:24 10:24 10:24 Templates  TLE  Save Template C Search Demo Category Adds MOB0123, Blue LED, TEGORY emo Category	Save Template          M * 10:24 * 66% * 10:24         Save Template         Save Template         LE         Is MOB0123, Blue LED, Twist n Go         Demo Category         Adds MOB0123, Blue LED, Twist n Go         TEGORY         Save Template         Save Template	Save Template  A   10:24  \$ 66%  10:24  \$ 66%  10:24  Templates  E  MOB0123, Blue LED, Twist n Go  EGORY  Adds MOB0123, Blue LED  Credentials  AV  Save Template	ional Settin	ngs	
Save Template	Save Template       M Total     66%       Save Template     No SIM Total       Save Template     Templates       LE     Save Template       Is MOB0123, Blue LED, Twist n Go     Demo Category       Adds MOB0123, Blue LED, Twist n Co     Credentials       TEGORY     Av       Save Template     Av	Save Template  A   10:24  Save Template  No SIM  10:24  Templates  C  Save Template  No SIM  10:24  Templates  C  Save Template  No SIM  10:24  Templates  C  Save Template  Save Template  Save Template			
IM © 10:24 * 66% Save Template X TLE Is MOB0123, Blue LED, Twist n Go TEGORY emo Category Adds MOB0123, Blue LED, Credentials AV	M  10:24 Save Template  No SIM 10:24 Templates  Save Template  No SIM 10:24 Templates  Save Template  No SIM 10:24 Templates  No SIM 10:24 Templates 1	A  Template A  A  A  A  A  A  A  A  A  A  A  A  A	Sa	ave Template	
Image: Save Template   Save Template   TLE   ds MOB0123, Blue LED, Twist n Go   Demo Category   Adds MOB0123, Blue LED, Twist n Co	M  10:24  66%  10:24  Save Template  LE  No SiM  10:24  Templates  Q. Search  Demo Category  Adds MOB0123, Blue LED,  TEGORY  mo Category  Save Template	A © 10:24 * 66% Save Template X E MOB0123, Blue LED, Twist n Go EGORY no Category Save Template			
Save Template     X       Save Template     X       TLE     Q. Search       ds MOB0123, Blue LED, Twist n Go     Demo Category       Adds MOB0123, Blue LED, Twist n Go     Adds MOB0123, Blue LED,       VTEGORY     AV	Save Template     X       Save Template     X       LE     Q. Search       Is MOB0123, Blue LED, Twist n Go     Demo Category       Adds MOB0123, Blue LED, Twist n Co     Adds MOB0123, Blue LED,       TEGORY     Credentials       Save Template     AV	Image: No Sim P     Image: No Sim P       Save Template     X       E     Q. Search       Image: MOB0123, Blue LED, Twist n Go     Demo Category       Adds MOB0123, Blue LED, Twist n Go     Credentials       EGORY     Av       Save Template     Av	~	10:24	
TLE Q Search ds MOB0123, Blue LED, Twist n Go Demo Category Adds MOB0123, Blue LED, Ategory emo Category	LE S MOB0123, Blue LED, Twist n Go Demo Category Adds MOB0123, Blue LED, TEGORY TEGORY Save Template	E Save Template	• Sa	ve Template	×
dis MOB0123, Blue LED, Twist n Go Demo Category Adds MOB0123, Blue LED, TEGORY amo Category	Is MOB0123, Blue LED, Twist n Go Demo Category Adds MOB0123, Blue LED, TEGORY TEGORY Save Template	EGORY Save Template Building Series S			
EGORY AV	EGORY  The construction of	EGORY Adds MOB0123, Blue LED Credentials AV Save Template	лОВ0123	8, Blue LED, Tw	vist n Go
TEGORY Credentials AV	TEGORY TEGORY Save Template	EGORY Credentials AV Save Template			
emo Category	TEGORY Credentais AV	Credentials AV			
enio Category	Save Template	Save Template	ORY		
	Save Template	Save Template	Categor	es. (	
			Sa	ave Template	
			Sa	ry ave Template	
			Sa	ry ave Template	
		<i>∞</i> □	Sa	ave 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 [<].

o SIM 🗢 10:20	* 66% 💷	No SIM 🗢	10:24	\$ 66% 💷	N	o SIM 🗢	10:20	* 6
Home			Templates	+	<	<	Template Details	
Scan For Readers	>	Q Search				Adds N	/OB0123, Blue	e Ll
HEI D		Demo Cate	gory			Twist r	n Go	
ID Reader Manage	r Overview >	Adds MOB	123, Blue LED,	Twist n Go		CATEGORY		
Bluetooth and OSDF	Upgrade >	Credentials	AV	BLE		Demo Ca	tegory	
Reader Configuratio	n and Ins >					CREATED B	Y	
Reader Firmware Up	date >					in 🔒	staller@hidglobal.com	
ull User Guide	>					CREDENTIA	LS	
HARED TEMPLATES						Credenti	als and Keys	
No Shared Ter	nplates					AUDIO/VISU	JAL	
			_			Idle Led Co	lor	
Home Templates	Settings	Home	Templates	Settings		Home	Templates	Sett

- 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.

No SIM 🗢	10:20	\$ 66% 💷
	Home	
Scan For Re	aders	>
HID Reader	Manager O	verview >
Bluetooth ar		ograde
Boodor Cont	figuration a	
Reader Com	inguration a	nu ins >
Reader Firm	ware Upda	te >
Full User Gu	ide	>
SHARED TEMPL	ATES	
Test Template		
AV shared by rm.admin@g	BLE mail.com	
A		sle.
Home	Templates	Settings

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.

No SIM 🗢	10:20	* 66% 💶	No SIM 🔶	10:20	\$ 60% 💷
	Home			Templates	+
Scan For F	Readers	>	Q Search		
HELP			Demo Cate	egory	
HID Reade	r Manager O	verview >	Adds MOB	0123, Blue LED, <sup>-</sup>	Twist n Go
Bluetooth	and OSDP Up	ograde >	Credentials	AV	BLE
Reader Co	nfiguration a	nd Ins >	Lindate LE	Dicolor	
Reader Fir	mware Updat	te >	Opuate EE	Dicolor	
Full User G	Guide	>	AV		
SHARED TEME	ATES		Update Re	ad AV	
Test Template	LAILO		AV		
AV shared by	BLE				
Home	Templates	Settings			•
			Home	remplates	Settings

#### 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

- 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.

Io SIM 🗢	10:20	* 66% 💷	No SIM 🗢 🔰	0:12 * 6:	% 💷	No SIM 🗢	10:12	* 6
	Home		Nearby	Readers	×	Ne	arby Readers	
			HID Reader	-55 dBr	n >	HID Reader	-55	5 dB
an For R	eaders	>	HID Reader	-82 dBr	n >	HID Reader	-88	B dB
.P			HID Reader	-88 dBr	n >	HID Reader	-89	9 dB
) Reade	r Manager O	verview >						
uetooth a	and OSDP U	pgrade >						
ader Co	nfiguration a	nd Ins $ ightarrow$						
ader Firr	mware Upda	te >	Signal strength va	lues closer to 0		Sele	ect Operation	
ll User G	uide	>	physically closest	indicate a reade . Eg. A signal	r is			
ARED TEMP	LATES		indicates a reader	is physically clo	ser	1	. Inspect	
No	Shared Templa	ates	signal strength	ider with -100 d	BW		2. Locate	
			Sto	o Scan			Start Scan	<u> </u>
*		\$					Cancel	

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.



HID<sup>®</sup> Reader Manager<sup>™</sup> Solution User Guide (iOS)

HID

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



No SIM 🗢	10:18	∦ 5	9% 💷
	Inspection Report	G	×
_			
Inspe	cting		
			- 1
-			- 1
			- 1
		_	

No SIM 🗢	10:20	* 60% 💷
Шар	ection Report	<u> </u>
CONFIGURE R	EADER	
Apply Temp	ate	
Change Rea	der Name	
ADMINSTRATI	ON CONFIGURATIO	DN
Reader Adn	nin	Standard
Mobile Adm	nin	Standard
SOFTWARE C	ONFIGURATION	
Detailed Co	onfiguration	>
FIRMWARE IN	ORMATION	
Loaded Rel	ease is R10.0.0	.30 >
Available Re	elease is R10.0.	0.30 >

#### Powering Trusted Identities

#### 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 <u>View detailed reader configuration</u>.
- 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 <u>Change reader name</u>.
     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 <u>Contact</u>
  HID Technical Support.

×

Inspection Report     C     ×       CONFIGURE READER
CONFIGURE READER Apply Template Change Reader Name
Apply Template Change Reader Name
Change Reader Name
ADMINSTRATION CONFIGURATION
Reader Admin Standard
Mobile Admin Standard
SOFTWARE CONFIGURATION
Detailed Configuration >
FIRMWARE INFORMATION
Loaded Release is R10.0.0.30
Available Release is R10.0.0.30


# 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.

o SIM 🗢 10:20	∦ 6	0% 🔲	No SIM 🗢	10:28	\$ 59% 💶	No SIM 🗢	10:30	\$ 59
Inspection Rep	ort C	×	< 1	nspection Report	C	<	Inspection Report	G
IRMWARE UPGRADE			Firmware Up	grade		Firmwal	re Upgrade	
There is an optional fir available for this reade	mware upg r.	rade	There is an opt	tional firmware upgrade ava	ilable for this	There is	an optional firmware upgrade av	ailable fo
Upgrade Firr	nware		Reader Upgra	de		Reader	Upgrade	
CONFIGURE READER				Performing Firmware Upgrade		c		
Apply Template				Packet 26 of 334 (2min 9s)			✓	
ADMINSTRATION CONFIGU	RATION		Upgra	ade Phase 2 of 5	_		Reader was successfully upgra	ded !
Reader Admin	Stan	dard			_			
Mobile Admin	Stan	dard	A	a een gelenen.		k	J	_
SOFTWARE CONFIGURATIO	N		Reader Admin		Standard	Reader A	ldmin	Sta
Detailed Configurati	on	>	Mobile Admin		Standard	Mobile A	dmin	Sta
			Software Cor			Softwar	e Configuration	

**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.

No SIM		\$ 60% 💷
	Inspection Report	G X
CONFI	IGURE READER	
Apply	(Tomplate	
Apply	remplate	
Chan	ge Reader Name	
ADMIN	STRATION CONFIGURATI	ON
Read	ler Admin	Standard
nead		Standard
Mobi	le Admin	Standard
SOFT	WARE CONFIGURATION	
Detai	iled Configuration	>
	-	
FIRMW	VARE INFORMATION	
Load	ed Release is R10.0.0	.30 >
Availa	able Release is R10.0.	0.30 >

# **Credential details**

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

- Credentials, see <u>Credential settings</u>.
- Keys, see <u>Add Mobile Keys</u>.

#### **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 <u>Communication Protocol settings</u>.
- Audio & Visual, see <u>Audio & Visual settings</u>.
- Optional Settings, see <u>Optional Settings</u>.
- Keypad Settings, see Keypad Settings.
- Wallet Settings, see <u>Wallet Settings</u>.

#### 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 <u>Apply configuration changes</u>.

No SIM 🗢	10:20	* 66% 💷
<	Inspection Report	c
CREDENTIAL	DETAILS	
<ul> <li>Credential</li> </ul>	5	
Keys		
READER SET	TINGS	
ISO14443	A UID Output Format	
Bluetooth	Modes, Ranges & Power	
Communic	cation Protocol	
<ul> <li>Audio &amp; Vi</li> </ul>	isual	
Optional S	ettings	
Keypad Se	ettings	
	Save As Template	
	Apply Selected Items	

# 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.

No SIM 🗢 10:20	*	60% 🔲	No SIM	<b>?</b>	10:20	\$ 60% 💷		No SIM 🗢	10:21	* 40% 💶
Inspection Report	C	×			Templates	+		<	Templates	+
CONFIGURE READER			Q Se	earch				Q Search		
Apply Template			Dem	no Catego	ry			Demo Cat	egory	
Change Reader Name			Adds	s MOB012	23, Blue LED, 1	wist n Go		Adds MOB	0123, Blue LED, Twis	st n Go
ADMINSTRATION CONFIGURAT	TION		Cre	dentials	AV	BLE		Credentials	AV	BLE
Reader Admin	Sta	ndard					J			
Mobile Admin	Sta	ndard	Upda	ate LED c	olor			Update LED	) color	
SOFTWARE CONFIGURATION				AV					Select Operatio	n
Detailed Configuration		>	Upda	ate Read	AV				View	
FIRMWARE INFORMATION				AV						
Loaded Release is R10.0.	0.30	>						lost temple	Apply	
Available Release is R10.0	0.0.30	>	4	*	Ē	÷		r -	Cancel	
			Но	ome	Templates	Settings				
				~						
Templates	*	37% 💶		≂ Ins∣	10:28 pection Repo	* 42% <b>⊡</b> rt C				
Q. Search			• Pro	atocols/Mo	hile Kevs					
Domo Cotonomi				0100010,1110	bile rego					
Demo Category			AUDI	O/VISUAL						
Adds MOB0123, Blue LED, T	wist n G	0		D Idle Colo	T	_				
Changing Configuration		×	Cha	anging Co	onfiguration	×				
		- 1								
Please power cycle yo	ur read	er	~	Template	was successful	ly applied !				
Update Read AV			Co	ontroller/Ho	st Protocol					
AV				6.5						
Test Template				Sa	ve As template					
AV BLE				Appl	y Selected Iter	ns				

**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.

# **HID**<sup>\*</sup> Powering **Trusted Identities**

# 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.

No SIM 🗢	10:20	* 60	0% 💶
Inspe	ction Report	С	×
CONFIGURE REA	ADER		
Apply Templa	to		
другу теттріа			
Change Read	er Name		
ADMINSTRATIO	N CONFIGURATIO	N	
Reader Admi	n	Stan	dard
Mobile Admir	n	Stan	dard
SOFTWARE CON	NFIGURATION		
Detailed Con	figuration		>
FIRMWARE INFO	JRMATION		
Loaded Relea	ase is R9.0.0.4		>
Available Rele	ease is R9.0.0.	4	>

No SIM 🗢	10:21	* 40% 💷
Ins	pection Repo	rt C' X
Change I	Reader Name	×
Reader	)1	
		Apply
Mobile Adr	nin	Standard
1 2 2		
123	400	<u> </u>
- / :	; ( )	£ & @ "
#+=	, ?	! ′ 🗵
авс 🌐	⊈ space	e return

No SIM 🤝	•	10:21					40%	
	Insp	pecti	ion F	Repo	ort	G		×
Chan	ge R	eade	er Na	ame			3	\$
Rea	der0'	1						
						Ap	ply	D
Mobile	Adm	iin				St	tanda	ard
1 2	3	4	5	6	7	8	9	0
- /	:	;	(	)	£	&	@	"
#+=	•	,	1	?	!	'		$\otimes$
АВС	•	2	5	spac	е		retu	rn



# Section 03 HID Reader Manager Portal

Powering Trusted Identities

# **HID** Powering Trusted Identities

This section provides the required steps and procedures to be performed by the HID<sup>®</sup> Reader Manager<sup>™</sup> 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<sup>®</sup> Origo<sup>™</sup> 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

# **HID**<sup>\*</sup> Powering Trusted Identities

# 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.

<section-header></section-header>	The Trusted Source for Secure Identity Solutions		
ID Secure Identity Services Portal   If the provide of the provi	ome > Secure Identity Services		
Control	ID Secure Identity	Services Portal	
Log in to manage your HID Mobile Access™ User Name Password Admin@hidglobal.com Forgot your password?	ID Global offers industry expertise and a co	mprehensive suite of services to assist customers and channel partners to creat	Support Please visit the HID Technical Support to submit a case online or find the Technical Support contact information in your region.
User Name Password Admin@hidglobal.com ••••••••••••••••••••••••••••••••••••	Log in to manage your HID N	lobile Access™	
Forgot your password?	User Name	Password	NEED HELP?
Forgot your password?	Admin@hidglobal.com		
Difficulties leasing in 2 Click here	Differentian language in 2 Click he	Forgot your password?	



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

Home > Secure Identity Services

# **HID Secure Identity Services Portal**



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



Powering Trusted Identities

HID

ASSA ABLOY

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

HID	
Home HID Reader Manager Portal	
Manage authorization of reader technicians for your HID Elite and HID Mobile Access readers	Need Assistance? Please visit HID Global Technical Support to submit a case online or find the Technical Support contact information for your region. Research Knowledge Base >>
Log in to manage your HID Readers. User name Admin@hidglobal.com Password LOGIN	Forgot your password? Visit the HID Secure Identity Services Portal, enter your user name and click "Forgot your password?".

**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**.

© 2019 HID Global Corporation/ASSA ABLOY AB All Rights Reserved | Reader Manager Privacy Notice | HID Origo Service Status

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

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

# **HID**<sup>\*</sup> Powering Trusted Identities

# **3.2.2** Access the HID Reader Manager Portal (HID<sup>®</sup> Origo<sup>™</sup> 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.

HID I HID Origo Management Portal	0 B i
Dashboard Services	
Mobile Identities Manage the administration mobile credential users.	Reader Manager           Manage reader key authorization as well as access to reader installation and configuration.
© 2019 HID Global Corporation/ASSA ABLOY AB. All Rights Reserved   Privacy Notice	Terms of Use   Service Status

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

HID <sup>®</sup>   HID Origo Management Portal	9 <b>8</b>	•
Services   Mobile Identities   Manage the administra   Cancel Continue Cancel Continue	ader	
© 2019 HID Global Corporation/ASSA ABLOY AB. All Rights Reserved   Privacy Notice   Terms of Use   Service Status		

Powering Trusted Identities

HID

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

HID	
Home HID Reader Manager Portal	
Manage authorization of reader technicians for your HID Elite and HID Mobile Access readers	Need Assistance? Please visit HID Global Technical Support to submit a case online or find the Technical Support contact information for your region. Research Knowledge Base >>
Log in to manage your HID Readers. User name Admin@hidglobal.com Password LOGIN	Forgot your password? Visit the HID Secure Identity Services Portal, enter your user name and click "Forgot your password?".

2019 HID Global Corporation/ASSA ABLOY AB All Rights Reserved | Reader Manager Privacy Notice | HID Origo Service Status

ASSA ABLOY

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

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

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<sup>®</sup> Reader Manager<sup>™</sup> 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 [

	admin@hidglobal.com - HID Global   Logout
HID	
Keys and Reader Technicians Keys and Reader Technicians	C \$
HID Global Keys	
Test 123 Test 456	
Reader Technicians	<b>2</b> +
Select Operation V APPLY O	Search
Name 🕲 🔻 Email 💌 Company 🔻 Keys Authorized 🕲 🔻	Alert 🔻 Last Updated 🔻 View Detail
No Reader Technicians available.	
KI K 1 2 H 🗰 25 🔻 items per page	1 - 0 of 0 results 🛛 🧲
VIEW DELETED READER TECHNICIANS	

Powering Trusted Identities

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

		admin@hidglobal.com - HID Global   Logout
HID	HID Administration	
Keys and Reader Technicians > E	nroll Reader Technician	
<b>Enroll Reader</b>	Technician	
Deader Technicia	n Information	
Reader Technicia	mmormation	
Name	Demo	
Email address	demo.installer@hidglobal.com	
Company	HID Global	

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

HID

Invitation & Key Auth	orization	
How do you want to proceed?	• Send only invitation to Reader Technician. Key Authorization(s) will need to be issued later.	
	Send invitation and Key Authorization(s) to Reader Technician.	
CANCEL	ENROL	

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 <u>Activate the HID</u> <u>Reader Manager app</u>. When the Reader Manager app is activated the administrator can issue key authorization. See <u>Issue authorization keys</u>.

# 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.

ecord(	s) selected						<u> </u>
Select (	Operation	V APPLY O			Search		Q
	Name 🕐 🔻	Email 🔻	Company 🔻	Keys Authorized 👔 🔻	Alert 🔻	Last Updated 🔻	View Detail
•	Demo Installer	demo.installer@hidglobal.com	HID Global			Feb 02, 2018	

3. Click EDIT in the Reader Technician Information section.

Keys and Reader Technicians > Reader Technician Detail

Reader Tec	hnician Detail	2
Reader Technician Information		<i>I I I I I I I I I I</i>
Name	Demo Installer	
Email address	demo.installer@hidglobal.com	
Company	HID Global	

#### D<sup>\*</sup> Powering Trusted Identities

4. Edit Reader Technician Information and click SAVE.

On the **Keys and Reader Technicians** page the updated Reader Technician information appears in the **Reader Technicians** list.

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

Keys and Reader Technicia	ans 🦻 Reader Technician Detail		
<b>Reader Te</b>	chnician Detail		2
Deeder Teeks			
Reader Techn	ician information		
Namo	Demo	Installer	
Name			
Email address	demo.installer@hidglobal.com		
Company	HID Global		



# 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.

ecord(	s) selected						<u> </u>
Select (	Operation	V APPLY O			Search		Q
	Name 🕲 🔻	Email 🔻	Company 🔻	Keys Authorized 🕘 🔻	Alert 🔻	Last Updated 🔻	View Detail
	Demo Installer	demo installer@bidglobal.com	HID Global			Feb 02, 2018	

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

Mobile Devices		
Current Mobile Devices	Deleted Mobile Devices	
No deleted devices found.		
DELETE READER TEC	CHNICIAN	RETURN

Powering Trusted Identities

- 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.

Delete Reader Technician
You are about to delete the selected Reader Technician. Mobile devices and assigned key authorisations will be deleted permanently from the HID Reader Manager. The Reader Technician will be moved to the Deleted Reader Technician's list.
Reason for deletion
Do you want to delete the selected Reader Technician?
NO

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

# HID<sup>\*</sup> Powering Trusted Identities

# 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.

Read	der Technician	S					<b>2</b> +
Select 0	Operation				Search		Q
	Name 🝘 🔻	Email 🔻	Company 🔻	Keys Authorized 😨 🔻	Alert 🔻	Last Updated 🔻	View Detail
	Demo Installer	demo.installer@hidglobal.com	HID Global	-		Feb 02, 2018	
4	П2 и и	25 🔻 items per page				1 - 1 of 1	results 📿

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

	Current Ke		
		ys Revoked / Expired Keys	
Apple IPhone X OS 13.3.1 Sluetooth; READERMANAGER-1.4.0 (249 nvitation code: Endpoint ID:	0)	No current keys to display for this device as of now.	>
Primary Device	O AL	THORIZE ADDITIONAL KEYS	

## HID<sup>\*</sup> Powering Trusted Identities

- 4. On the Authorize Additional Keys page select a key reference from the Key drop-down menu.
- 5. As an option set a authorization validity period.

**Note:** If the validity period for authorization is not set the default period is five years.

6. Click SAVE.

		admin@hidglobal.com - HID Global   Logout
HID		
Keys and Reader Technicians > Reader Technicia	an Detail > Authorize Additional Keys	
<b>Authorize Addition</b>	al Keys	2
Available RM Testing Orga	anization Keys	
ios 13.3.1	Кеу	M0B0001
Bluetooth; READERMANAGER-1.4.0 (249.0) Invitation code: Endpoint ID:	Validity period for authorization (Optional)	2 Years V
• Primary Device		
Status Ready for Key		
CANCEL		SAVE



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

Current Mobile Devices	Deleted Mobile Devices	8
Apple IPhone X iOS 13.3.1 Bluetooth; READERMANAGER-1.4.0 Invitation code: - Endpoint ID: Primary Device Status Ready for Key	(249.0) 	Irrent Keys Revoked / Expired Keys MOBAOAQ Issuing Key Valid till Feb 02, 2023 09:18:50 UTC Revoke Key Authorization
		AUTHORIZE ADDITIONAL KEYS     DELETE DEVICE

- 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**.

Current Mobile Devices Deleted	Mobile Devices
Apple IPhone X iOS 13.3.1 Bluetooth; READERMANAGER-1.4.0 (249.0) Invitation code: Endpoint ID: Primary Device Status Ready for Key	Current Keys Revoked / Expired Keys MOBAOAQ Key authorized Valid till Feb 02, 2023 09:18:50 UTC Revoke Key Authorization
	AUTHORIZE ADDITIONAL KEYS     DELETE DEVICE

# 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**.

Key reference ICE65789		
Friendly name of key	,	
Test123		
Description (Optiona	I)	
Description (Optiona	l)	
Description (Optiona	1)	

## **HID**<sup>\*</sup> Powering Trusted Identities

# 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.

Reader Technicians					<b>&amp;</b> +	
Select Operation V APPLY O				Search		Q
🔲 Name 🕡 🔻	Email 🔻	Company 🔻	Keys Authorized 🛛 🔻	Alert 🔻	Last Updated 🔻	View Detail
Demo Installer	demo.installer@hidglobal.com	HID Global	-		Feb 02, 2018	

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

Current Mobile Devices	Deleted Mobile Devices
Apple IPhone X iOS 13.3.1 Bluetooth; READERMANAGER-1.4.0 (2. Invitation code: - Endpoint ID: Primary Device Status Ready for Key	(9.0) MOBAOAQ Issuing Key Valid till Feb 02, 2023 09:18:50 UTC Revoke Key Authorization
	AUTHORIZE ADDITIONAL KEYS     DELETE DEVICE

Powering Trusted Identities

- 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.

Revoke Key Authorization				
You are about to revoke the se Authorization will be deleted p Manager.	elected Key Authorization. The Key permanently from the HID Reader			
Do you want to revoke the Key Authorization?				
l	NO Yes			

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

Current Mobile Devices Deleted	Mobile Devices
Apple IPhone X iOS 13.3.1 Bluetooth; READERMANAGER-1.4.0 (249.0) Invitation code: Endpoint ID: Primary Device Status Ready for Key	Current Keys Revoked / Expired Keys
	AUTHORIZE ADDITIONAL KEYS     DELETE DEVICE

## HID<sup>\*</sup> Powering Trusted Identities

- 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.

Current Mobile Devices	Deleted Mobile Devices			
	Curr	rent Keys Revoked / Expired Keys		
Apple IPhone X IOS 13.3.1 Bluetooth; READERMANAGER-1.4.0 (2) Invitation code: Endpoint ID: O Primary Device Status Ready for Key	49.0) 	MOBAOAQ Key revoked On Feb 02, 2018 09:29:33 UTC		
		AUTHORIZE ADDITIONAL KEYS	DELETE DEVICE	



# 3.5 Configure HID Reader Manager Portal settings

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

			admin@hidgi	obal.com - HID G	ilobal   Logout
HID					
Keys and Reader Technicians	icians			<b>C</b>	٢
HID Global Keys					
Test123 Test 456					
Reader Technicians					<b>&amp;</b> +
Select Operation V APPLY O			Search		Q
Name 🐌 🔻 🛛 Email 🔻	Company 🔻	Keys Authorized 🛞 🔻	Alert 🔻 L	ast Updated 🔻	View Detail
No Reader Technicians available.					
K K 1 2 K ₩ 25 ▼ items	per page			1 - 0 of 0	results C
VIEW DELETED READER TECHNICIANS					

# **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.

Export Settings When Reader technician records are exported, they will include					
Reader Technician	🗹 Email	Company	☑ Alert	☑ Last updated	
Device ✓ Make	☑ Model	Device status	✓ End point ID	✓ Invitation code	
Key Authorization	Description	☑ Key reference			

# 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.

Invitation Email Settings When invitation email messages are sent, this template will be used



#### **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.

Configure	Delete	Thresho	ld	
When attempting to d retry the delete opera After the time configu	elete a mobile tion. ired below, the	device or Revoke K system automatica	ey Authorizati Ily completes	on, if the mobile device is not reachable (e.g turned off or out of range), the system will periodically the delete operation and places the Key Authorization in a revoked state.
Delete threshold	2	Hours	~	



# 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.

The Trusted Source for Secure Identity Solutions			
Home > Secure Identity Services	Services Portal		
Hib Secure identity	Services Fortai		
HID Global offers industry expertise and a c and manage secure identities.	omprehensive suite of services to assist of	ustomers and channel partners to create, use	Support Please visit the HID Technical Support to submit a case online or find the Technical Support contact information in your region.
User Name	Password		NEED
Admin@hidglobal.com	•••••	LOGIN	HELP?
	Forgot your password?		
Difficulties logging in? Click h	ere.		

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





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

	D		The Trusted Source Secure Identity Solut	for lions						
lome >	Secure	ar	tity Services > Adminit	stration > Users and	d Contacts				rmtesting orga RM Testing Orga My Account   Log	nization nization g Out
IY HID		HID	) Mobile Access	Administration						
User	Con	sole			First Provinue	1 Novi	Lacta	Showing 1 - 12	of 12	
User	cons	sole		« Q Search	First ← Previous	1 Next	→ Last »	Showing 1 - 12 o	of 12	+ Add
User Se Actior	constanch	sole	Last name	« Q Search First name	First ← Previous	1 Next	→ Last »	Showing 1 - 12 of	of 12 Services	+ Add Roles
User Se Action	cons earch	sole	Last name rmadminprodus	« Q Search First name hidold	First ← Previous	1 Next Status ACTIVE	→ Last » Portal User Y	Showing 1 - 12 of Ship Contact	of 12 Services Reader Manager	+ Add Roles RM Administrato
User Se Action	earch	sole	Last name rmadminprodus utilityadminpro	Q Search       First name       hidold	First ← Previous User ID / Email hidoldrmadminpro hidoldutilityadminp	1 Next Status ACTIVE ACTIVE	→ Last » Portal User Y Y Y	Showing 1 - 12 of Ship Contact	of 12 Services Reader Manager Utility Service	+ Add Roles RM Administrato Utility Admin
User Se Action C C	earch	sole	Last name rmadminprodus utilityadminpro rmtestuser	Q Search       First name       hidold       hidold	First ← Previous User ID / Email hidoldrmadminpro hidoldutilityadminp hidrmtestuser@grr.la	1 Next Status ACTIVE ACTIVE ACTIVE	→ Last » Portal User Y Y Y Y Y	Showing 1 - 12 of Ship Contact N N N	Services Reader Manager Utility Service Reader Manager	+ Add Roles RM Administrato Utility Admin RM Administrato

- 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.

mtestuser1	Sanvica	Pole
1110-304-301	Card Services	
irst name	Gard Services	Full access to all functionality.
nid		CS Operator
ser ID / Email		Partial access to funtionality. Able to request badges, confirm production and download return files, but cannot perform configuration constitues.
nidrmtestuser1@grr.la		operationa
	Mobile	MA Administrator
onfirm User ID / Email	Access	Full access to all functionality.
nidrmtestuser1@grr.la		<ul> <li>MA Reviewer Read only access. Can not add or edit data nor issue or revoke Mobile IDs.</li> </ul>
ortal User (optional)		MA Operator
Yes 🔹		Partial access to funtionality. Able to add mobile users and issue and revoke Mobile IDs, but cannot perform configuration operations.
hip Contact (optional)	Organization	Org Admin
Select One 🔻	Administration	Enables the 'Administration' feature. Able to add, edit, delete portal users and perform password resets on their accounts.
	RMA & Web order search	OM Admin
	Reader Manager	RM Administrator Service for the Reader Manager, Full access to all the RM activity
	Utility Service	Utility Admin

#### D Powering Trusted Identities

- 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.

Password		Support
Your new password must contain -		Please visit the HID Technical Support to submit a case online
Minimum 8 characters		or find the Technical Support contact information in your
Uppercase and lowercase letters		region.
Minimum one number		NEED
Minimum one special character (e.g. 1&%)		HELP?
Should not use your email address		
New Password	Confirm Password	
······		
Additional Security  If you opt for additional security, we will send a va  If you are unable to receive the validation code or  I would like to enable additional security for hyperbolic security fo	word has been created.	
Privacy Statement Agreement		
I have read and agree to the HID Global Corporation Private	cy Statement	
SAVE		

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)**.

69

## 3.6.2 Add Reader Manager Admin (HID<sup>™</sup> Origo<sup>®</sup> 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 [1] on the **Dashboard** screen, then select **Organization Administration**.



Powering Trusted Identities

HID

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

Administrative Users						ADD ADMIN USER
↑ Administrative Person's Name	↑ Email Address	Phone Number	↑ Status		↑ Roles	Actions @
Adminuser1	Adminuser1@gmail.com		Active	Mobile Identities, Reader Manager	MI Administrator, RM Administrator	🖻 C 🔌
Adminuser2	Adminuser2@gmail.com		Active	Mobile Identities, Reader Manager	MI Administrator, RM Administrator	n C 🔌
Adminuser3	Adminuser3@gmail.com		Active	Mobile Identities, Reader Manager	MI Administrator, RM Administrator	n C 🔌
<< First < Previous 1 2 Next	Last >> Last >> 10	er page			Showing	1 - 3 of 3 results C

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

Jser Information					
Name	Admin		User4		
Business email address (this will be used as the user ID)	Adminuser4@gmail.com				
Confirm email address	Adminuser4@gmail.com				
Phone number	Country		Country code		Phone (Area code + Phone number)
	United States of America	$\sim$	1		
Select the services and roles to be assigned to this administrative user	Service	Role			
	Mobile Identities	None MI Review Read only IDs. MI Operati Partial ac revoke M MI Admin Full acces	ver access. Can not add or edit tor cess to funtionality. Able to obile IDs, but cannot perforn <b>istrator</b> iss to all functionality.	t data nor issue add mobile use n configuration	t or revoke Mobile ers and issue and operations.
	Organization Administration	Org Admi Enables th and perfo	<b>n</b> he 'Administration' feature. A rm password resets on their	Able to add, edit r accounts.	t, delete portal users
	Reader Manager	RM Admin Service fo	<b>nistrator</b> r the Reader Manager,Full a	ccess to all the	RM activity

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

HID <sup>*</sup>   HID Origo Managem	ent Portal			?	<b>8</b> I
Administration Dashl	board				
New Administrative user has been added succession	essfully!				
Organization Summary					
Organization name	HID Origo Demo	Services	Mobile Identities, Organization Administration, Reader Manager		
Organization ID	5551859	Status	Active		
Organization Address	Tech Ridge Austin, TX 78753				
	United States of America				
				SETTINGS	EDIT

#### HID<sup>®</sup> Reader Manager<sup>™</sup> Solution User Guide (iOS)

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.

Powering

**Trusted Identities** 

 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.

		Help
HID		
Set Up Account	t	
Login & Security		
Control your password and account acco	ess. Your password protects your account. You can also add a second layer of protection with 2-Step Authentication, which sends a one-time-verification code to your phone for you to enter when you sign in.	
Password		
Password guidelines -		
<ul> <li>Minimum 8 characters</li> <li>Upper case and lower case letters</li> <li>Minimum one number</li> <li>Minimum one special character</li> <li>Should not use your email address</li> </ul>		
New password		
Confirm password		
Multi-Factor Authentication If you opt for Multi-Factor authentication, If you are unable to receive the validation If you are unable to receive the validation Turn on the Multi-Factor authent	, each time you login to SIS Portal Account, you'll need your password and a verification code. We will send a validation code via text message to your mobile phone. n code on your mobile phone, the system will offer an alternative. ication	
Privacy Agreement		
I have read and agree to the HID Glo	bal Corporation Privacy Statement.	
CANCEL	SAV	/E

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<sup>®</sup> Origo<sup>™</sup> 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  $[\mathscr{I}]$  associated with a listed user.

ome > Se	ecure l	dentity Services > Admi	nistration > Users and	d Contacts				rmtesting orga	nization
		and Contr	octe				RM Testing Organization		
1561	50							My Account   Log	g Out
Y HID		HD Mobile Access	Administration						
	villa.	ne							
	01150	ne	ĸ	First ← Previous	1 Next	Last »	Showing 1 - 12 of	of 12	
Sear	ch		« Q Search	First ← Previous	1 Next	→ Last »	Showing 1 - 12 e	of 12	+ Add
Sear	ch	Last name	Q Search First name	First ← Previous	1 Next	→ Last »	Showing 1 - 12 of Ship Contact	of 12 Services	+ Add Roles
Sear Actions	ch	Last name madminprodus.	Q Search First name . hidold	First ← Previous	1 Next Status ACTIVE	E→ Last »	Showing 1 - 12 of Ship Contact	of 12 Services Reader Manager	+ Add Roles RM Administrate
Sear Actions	ch Q 1	Last name rmadminprodus. utilityadminpro	<ul> <li>Q Search</li> <li>First name</li> <li>hidold</li> </ul>	First ← Previous	1 Next Status ACTIVE ACTIVE	E→ Last » Portal User Y Y Y	Showing 1 - 12 of Ship Contact	Services Reader Manager Utility Service	+ Add Roles RM Administrat Utility Admin
Sear Actions	ch 	Last name rmadminprodus. tulityadminpro	Q Search     First name     hidold     hid	First ← Previous	1 Next Status ACTIVE ACTIVE ACTIVE	→ Last » Portal User Y Y Y Y Y	Showing 1 - 12 of Ship Contact N N N	of 12 Services Reader Manager Utility Service Reader Manager	+ Add Roles RM Administrat Utility Admin RM Administrat

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

rmtestuser1	Service	•	
	Card Services	CS Administrat	or
hist name		Full access to al	li functionality.
nia		CS Operator	funtionality. Able to request hadnes, confirm
Iser ID / Email		production and operations	download return files, but cannot perform configuration
hidrmtestuser1@grr.la			
	Mobile	MA Administrat	tor
onfirm User ID / Email	Access	Full access to al	II functionality.
hidrmtestuser1@grr.la		MA Reviewer	
		Read only acces IDs.	ss. Can not add or edit data nor issue or revoke Mobile
ortal User (optional)		MA Operator	
Yes 🔻		Partial access to revoke Mobile II	o funtionality. Able to add mobile users and issue and Ds, but cannot perform configuration operations.
hip Contact (optional)	Organization	Ora Admin	
Select One 🔻	Administration	Enables the 'Ad users and perfo	ministration' feature. Able to add, edit, delete portal rm password resets on their accounts.
	RMA & Web	OM Admin	
	order search		
	Reader	RM Administrat	tor
	Manager	Service for the F	Reader Manager, Full access to all the RM activity
	Utility Service	Utility Admin	

 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 <u>Access the HID Reader</u> <u>Manager Portal (HID SIS Portal)</u>. <sup>\*</sup> Powering **Trusted Identities** 

HID

#### **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 [1] on the **Dashboard** screen, then select **Organization Administration**.

HID Origo Management Portal	@ <b>8</b> ]
Dashboard Services	HID Origo Services Organization Administration
Mobile Identities Manage the administration mobile credential users.	norization as well as access to reader ation.
© 2019 HID Global Corporation/ASSA ABLOY AB. All Rights Reserved   Privacy Notice   Terms of Use   Service Status	

Powering Trusted Identities

3. In the **Administrative Users** section, click the on the edit icon  $[\mathscr{I}]$  associated with a listed user.

Administrative Users						ADD ADMIN USER
Administrative Person's Name	1 Email Address	Phone Number	↑ Status			Actions @
Adminuser1	Adminuser1@gmail.com		Active	Mobile Identities, Reader Manager	MI Administrator	🔊 🕈 🗎
Adminuser2	Adminuser2@gmail.com		Active	Mobile Identities, Reader Manager	MI Administrator, RM Administrator	1 C N
Adminuser3	Adminuser3@gmail.com		Active	Mobile Identities, Reader Manager	MI Administrator, RM Administrator	🖋 🏷 🗎
<< First < Previous 1 2 Next	t> Last>> 10 🗸 ite	ms per page			Showir	ig 1 - 3 of 3 results 🛛 C

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

dd Administrative User			CANCEL SAVE
User Information			
Name	Admin	User1	
Business email address (this will be used as the user ID)	Adminuser1@gmail.com		
Confirm email address	Adminuser1@gmail.com		
Phone number	Country	Country code Phone (Area code + Phone nu	mber)
	United States of America	✓ 1	
Select the services and roles to be assigned to this administrative user	Service	Role	
	Mobile Identifies	<ul> <li>None</li> <li>MI Reviewer         Read only access. Can not add or edit data nor issue or revoke Mobile IDs.     </li> <li>MI Operator         Partial access to funtionality. Able to add mobile users and issue and revoke Mobile IDs, but cannot perform configuration operations.     </li> <li>MI Administrator         Full access to all functionality.     </li> </ul>	
	Organization Administration	Org Admin Enables the 'Administration' feature. Able to add, edit, delete portal users and perform password resets on their accounts.	
	Reader Manager	RM Administrator Service for the Reader Manager,Full access to all the RM activity	

6. The RM Administrator can now log back into the HID Origo Management Portal and select the **Reader Manager** option to be redirected to HID Reader Manager. For detailed information, see **Access the HID Reader Manager Portal (HID**<sup>®</sup> **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
<i>"There does not seem to be an internet connection."</i>	Internet connectivity is not available for the mobile device. Check the mobile device Settings > Connections.
"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.
<i>"Failed to register the user."</i>	The user tries to register when HID Reader Manager servers are down. Please periodically try again and check your email for any service distribution notification.
"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
<i>"You are not authorized to configure this reader."</i>	The user does not have authorization keys/credentials to access the reader. Please request key authorization for this reader from the Reader Manager Portal Administrator.
"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.
<i>"This module can not be used to upgrade the Reader. Use the module with the latest firmware."</i>	The BLE smart module firmware/hardware version is unsupported by the Reader Manager app. Please ensure the module used for the upgrade is from an Bluetooth and OSDP Upgrade Kit. See <u>iCLASS SE Bluetooth &amp; OSDP upgrade kits</u> .
"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
<i>"New Password is not compliant to requirements"</i>	The new Password entered has not met the password requirement rules. Please use a password which meets the requirements detailed on the screen.
"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.

Powering

**Trusted Identities** 

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



Electrical tape



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



Expansion slot



Module from upgrade kit

- D Powering Trusted Identities
- 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.

IM 🗢 10:2	0	* 44	% 💶	No SIM	Ŷ	10:20	
Inspection R	eport	G	×	<		Credentials	
EDENTIAL DETAILS				0	HID MC	BILE ACCESS	
Credentials					THE MC		
evs				NFC			
- / -				BLE			
DER SETTINGS					10 50 1		-NO
014443A UID Outpu	ut Forma	t			13.50 N	IHZ HIGH FREQU	ENC
uetooth Modes, Ran	ges & P	ower		SEOS			
	-			Seos			
mmunication Proto	COI			ICLAS	S		
dio & Visual				iClass	5		
otional Settings				Class	05		
whad Settings				IClass	5 SE		
iypuu ooxiiigo				iClass	s SR		
Save Ten	nlato			MIFAR	RE DESFI	RE	
Save len	ipiate			MIFAR		Fire SIO	

#### iCLASS SE / multiCLASS SE

\* 66%

sim 😨

CREDENTIAL DETAIL Credentials Kevs

READER SETTINGS

#### HID<sup>®</sup> Reader Manager<sup>™</sup> Solution User Guide (iOS)

- 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.

**Trusted Identities** 

Powering



- 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.

o SIM 😤	10:24	* 44% 💷	No SIM 🗢	10:20	* 66% 💷
<	Inspection Report	C	<	Host Protocol	
CREDENTIA	L DETAILS		WIEGAND		
Credentia	ls		Enabled	1	$\bigcirc$
Keys			Wiegand is	s the default communic	cation
054050.053	1100		protocol u to the con	sed by readers to send trollers.	l access data
ISO14443	3A UID Output Format		OSDP		
Bluetooth	Modes, Ranges & Power		Enabled	i	
Communi	cation Protocol		OSDP enal between re	bles bi-directional com eader and controller. R	imunication efer to your
Audio & V	fisual		controller configurat	documentation for req ion	uired
Optional	Settings		SPEC COM	IPLIANCE	
Keypad Settings			V1		
	Save As Template		ADDRESS		
			00		
	Apply Selected Items				

#### Powering Trusted Identities

- 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:

- Check the size of the reader to identify the reader as an R10 model. iCLASS/multiCLASS SE<sup>®</sup> readers and HID<sup>®</sup> Signo<sup>™</sup> readers are available in different form factors for various installation environments, however the iCLASS SE<sup>®</sup> 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





HID Signo 20



#### HID Powering Trusted Identities

## **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<sup>®</sup> 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<sup>®</sup> Signo<sup>™</sup> reader.

iCLASS SE Express R10

#### iCLASS/multiCLASS SE Rev E R10 10:20

Inspection Report C

ADMINSTRATION CONFIGURATION

SOFTWARE CONFIGURATION Detailed Configuration

FIRMWARE INFORMATION Loaded Release is R8.6.0.4 Available Release is R8.6.0.4

No SIM 🗢

CONFIGURE READER Apply Template Change Reader Name

Reader Admin

Mobile Admin

Powering

**Trusted Identities** 

	No SIM 🗢	10:20	\$ 60% 🗖
	Insp	ection Report	c ×
	CONFIGURE F	READER	
	Apply Temp	late	
	Change Rea	der Name	
	ADMINSTRAT	ION CONFIGURATIO	N
	Reader Adr	nin	Standar
	Mobile Adn	nin	Standar
	SOFTWARE C	ONFIGURATION	
	Detailed Co	onfiguration	
	FIRMWARE IN	FORMATION	
	Loaded Rel	ease is R9.0.0.4	
	Available Re	elease is R9.0.0.	4

	HID Signo	)	
No SIM 🗢	10:20	* 6	0% 🔲
In	spection Report	G	×
CONFIGUR	E READER		
Apply Ten	nplate		
Change R	eader Name		
ADMINSTR	ATION CONFIGURATIO	лс	
Reader A	dmin	Star	ndard
Mobile A	dmin	Star	ndard
SOFTWARE	CONFIGURATION		
Detailed	Configuration		>
FIRMWARE	INFORMATION		
Loaded R	elease is R10.0.0.	.30	>
Available	Release is R10.0.	0.30	>



# 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.
МА	HID Mobile Access <sup>®</sup> . 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	<ul> <li>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:</li> <li>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).</li> <li>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.</li> <li>App Specific:This entrance opening mode is specific to an application, for example, widget opening from a wearable such as a smartwatch.</li> </ul>
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.		A.3
	<ul> <li>Section 2.3.6 View detailed reader configuration.</li> </ul>	
	<ul> <li>Appendix A - Configure reader in HID Reader Manager.</li> </ul>	
July 2019	<ul> <li>Updates implemented:</li> <li>Section 2.3.1 Create a new template. Updated section for the select reader option and select charging profile option for iCLASS SE Express.</li> <li>Section 2.3.6 View detailed reader configuration. Updated section for enable/disable Mifare &amp; Desfire UID and Priority options for iCLASS SE Express.</li> <li>Section A.2.2.1 Configure reader in HID Reader Manager. Updated section for enable/disable Mifare &amp; Desfire UID and Priority options for iCLASS SE Express.</li> <li>Section 2.3.5 Update reader firmware and Section 2.3.7 Apply configuration changes. Added note relating to "SNMP Authentication Failed" message.</li> <li>Section 4.1.1 Error and warning messages. Updated Error and warning message table for "SNMP Authentication Failed" message.</li> </ul>	A.2
January 2019	<ul> <li>Updates implemented for Reader Manager 1.1.0 and support for the iCLASS SE Express R10:</li> <li>Section 2.3 Basic app functionality. Updated sections for new and changed template configuration settings.</li> <li>Section 3.5.2 Enroll Reader Manager Admin (HID Origo Management Portal)</li> <li>Appendix A - Configure reader in HID Reader Manager. Updated section for new settings.</li> <li>Appendix B - Identify HID reader models. New section.</li> </ul>	A.1
September 2018	Initial release for Reader Manager 1.0.	A.0



## Powering **Trusted Identities**

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

#### PLT-03683, A.4

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