

HID Mobile Access[®]

Frequently Asked Questions

Support Documentation for Portal Administrators

PLT-02085, C.0
August 2023



Copyright

© 2014 - 2023 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 Origo, HID Reader Manager, HID Elite, iCLASS SE, multiCLASS SE, and Seos are trademarks or registered trademarks of HID Global, ASSA ABLOY AB, or its affiliate(s) in the US and other countries and may not be used without permission. All other trademarks, service marks, and product or service names are trademarks or registered trademarks of their respective owners.

Contacts

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

What's new

Date	Description	Revision
August 2023	Sections 5.2.3 Upgrade an existing pre-paid subscription and Section 5.2.4 Multiple channel partners. Added information for upgrading from a MID-SUB-T053 to a MID-SUB-T103 subscription.	C.0

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

Introduction	8
1.1 HID Mobile Access	9
General Questions	10
2.1 When was HID Global established?	11
2.2 How long has HID Global been providing the Mobile Access solution?	11
2.3 Does HID Global rely on third parties to provide services to the End Customer?	11
2.4 Does HID Global have a formal Business Continuity policy in place?	11
2.5 Who is responsible for establishing and testing HID Global's Business Continuity arrangements?	11
2.6 Does HID Global have an incident management process?	11
2.7 Does HID Global have a formal change management process in place?	11
2.8 Does HID Global comply with ISO27001?	11
2.9 Can HID Global demonstrate compliance with non-national legislation and regulations, for example SOX, PCI-DSS?	11
HID Mobile Access	12
3.1 What is HID Mobile Access?	13
3.2 What is Seos?	13
3.3 How is the HID Mobile Access solution different from other solutions available today?	13
3.4 Does HID Global Mobile Access support both BLE and NFC?	13
3.5 What are the differences between using BLE and NFC for reader to mobile device communication?	14
3.6 How do I onboard for the Mobile Access service?	14
3.7 How do I order user licenses for the first time?	15
3.8 Which Service Levels are available for the HID Origo Management Portal?	15
3.9 What technical support is available for HID Mobile Access?	15
HID Mobile Access Portal	16
4.1 Are there any best-practice policies I should implement within the Enterprise environment?	17
4.2 Which browsers are supported by the HID Origo Management Portal?	17
4.3 What roles are available in the Portal?	18
4.4 How can I reset my HID password?	19
4.5 Why can't I see the HID Mobile Access web application after I log into the Portal?	19
4.6 Where can I check the HID Origo Service status?	19
4.7 Can I try Mobile Access free of charge?	20
4.8 How do I redeem an invitation using a QR Code?	23
4.9 How do I allow additional administrators to use the Portal?	24
4.10 How do I configure the time zone setting in the Portal?	25
4.11 How can I see information about my purchased user licenses for Mobile Access?	28
4.12 How do I control how many user licenses I consume?	28
4.13 I am using all purchased user licenses, how do I buy additional user licenses?	29
4.14 How can I find out which users are inactive?	29

4.15 How do I enable the Site field and Phone Number field in the Portal?	31
4.16 How do I enroll users and issue a Mobile ID to their mobile device?	33
4.17 How do I assign a photo image to an individual enrolled user?	34
4.17.1 Edit/delete newly enrolled user photo	35
4.17.2 Edit/delete existing user photo	35
4.18 How do I change the badge image to my corporate logo?	37
4.19 How do I configure an invitation link?	39
4.19.1 Remove invitation code from email	39
4.19.2 Configure invitation email distribution	39
4.20 How do I change the invitation email template?	40
4.21 How many times can an invitation code be used?	40
4.22 How do I configure a custom mail server?	41
4.23 Why can't I delete users?	44
4.24 How can I revoke Mobile IDs from a user's mobile device?	44
4.25 How do I manage obsolete or duplicate Mobile IDs (MIDs)?	45
4.25.1 Delete a Mobile ID (MID)	45
4.25.2 Set a MID type as default	46
4.25.3 Check for duplicate MIDs and remove duplicates	47
4.25.4 Remove a range of credentials	49
4.26 What should I do if the Mobile Access Portal displays "Delivering Mobile ID" for an extended period?	51
4.27 How do I enable Enterprise Policy Enforcement?	52
4.28 How are MIDs replenished?	53
4.29 How do I activate auto-replenishment?	54
4.29.1 Activate auto-replenishment	55
4.30 What subscription contract renewal notifications are communicated?	56
4.31 What happens if my subscription contract is on manual renewal and I don't place a renewal order before my subscription expires?	56
4.32 How do I activate Delegated Authorization functionality?	57
4.32.1 Approve a Delegation Request	57
4.32.2 Perform Organization administration actions	59
4.32.3 Perform Mobile Identities actions	60
4.32.4 Delegated Authorization limitations	62
4.33 What role does a Service Provider have for Delegated Authorization?	62
4.34 Certificate-based Authentication	63
4.34.1 Prerequisites	63
4.34.2 Base64 encoding	64
HID Mobile Identities Subscriptions	65
5.1 What Mobile Access Subscription contracts are available?	66
5.1.1 Pre-paid subscription user licenses	66

5.1.2 Activation based subscription user licenses	66
5.2 How do I change my Subscription model?	67
5.2.1 Activation based subscription to a pre-paid subscription model	67
5.2.2 Pre-paid to an activation based subscription model	67
5.2.3 Upgrade an existing pre-paid subscription	67
5.2.4 Multiple channel partners	67
5.3 What subscription contract renewal notifications are communicated?	67
5.4 What happens if my subscription contract is on manual renewal and I don't place a renewal order before my subscription expires?	68
HID Mobile IDs	69
6.1 What are Mobile IDs?	70
6.2 How can I buy additional Mobile IDs?	70
6.3 Is a Mobile ID more secure than a physical card credential?	71
6.4 How many Mobile IDs can be issued to a device?	72
6.5 Can the Mobile ID be transferred to a new device?	72
6.6 Can one user's Mobile ID be accessed from multiple devices?	72
6.7 What if I factory-reset my device, or uninstall the Mobile Access App	72
6.8 Can Mobile IDs be utilized beyond access control in the future?	72
6.9 If a Mobile ID has been disabled, does this free up a Mobile ID that I can then use for another phone?	72
HID Mobile Access App	73
7.1 Which mobile devices and operating systems are supported?	74
7.2 Where can users download the HID Mobile Access App?	74
7.3 How do I open a door using HID Mobile Access?	74
7.3.1 Using HID Mobile Access with BLE on iPhone or Android with BLE	74
7.3.2 Using HID Mobile Access with NFC on an Android device	75
7.4 Does HID Mobile Access work without network coverage?	75
7.5 Does HID Mobile Access work without a battery?	75
7.6 What impact does HID Mobile Access have on battery life?	75
7.7 Should the user regularly update their mobile device to the latest operating system?	75
7.8 Should the user regularly update their mobile device to the latest HID Mobile Access App?	75
7.9 What is the average data usage by the HID Mobile app?	76
7.9.1 iOS mobile devices	76
7.9.2 Android mobile devices	76
7.10 Does the app collect private data?	76
HID Mobile-enabled readers	77
8.1 Why doesn't the reader recognize my mobile device?	78
8.2 Why do I get vibration or sound from the device before the reader LED shows green?	78
8.3 What happens when Twist and Go is used and there are multiple readers in range of the mobile device?	78
8.4 Why is the door opening experience slower with mobile than with a physical card?	78

8.5 How does the user know when to Tap vs. Twist and Go?	78
8.6 Can you have both Tap and Twist and Go enabled at the same time?	79
8.7 Is the power consumption and wiring different to standard readers?	79
8.8 Can I control the reading range?	79
8.9 What are possible starting dBm values for BLE reader locations?	79
8.10 What is Enhanced Tap door opening mode?	80
Automated onboarding	81
9.1 How do I submit a self onboarding request?	82
9.2 What is automated onboarding?	83
9.3 How long does the automated onboarding process take?	84
9.4 Can I change the Organization name after onboarding?	84
9.5 Can I start using the Mobile Access service right after the onboarding process?	84
9.6 Why am I asked for HID Elite Program in Step 1 of the onboarding process?	84
9.7 Does automated onboarding include ordering Readers and Mobile IDs	84
9.8 What is needed to place the order?	84
9.9 What is an organization ID?	84
9.10 What is a Mobile Keypad?	84
9.11 How can I find my organization ID and Mobile Keypad?	84
Legacy support	85
10.1 Are legacy parts being discontinued?	86
10.2 If I use the automated onboarding process, am I obliged to place an order? Will my organization ID and Mobile Keypad be reserved forever even though I am not ordering?	86
10.3 If I am a HID Partner, how can I ensure that Mobile Admin cards are sent to me as opposed to the end user?	86
10.4 Are there any issues about shipping the Mobile Admin cards internationally?	86
10.5 What formats are allowed when booking an order for a MOBILE-ID?	86
10.6 Can I use new part numbers to order for a legacy customer?	86
Security	87
11.1 What happens if I lose my device?	88
11.2 What is the security level on the mobile device?	88
11.3 How is security maintained?	88
11.4 When someone downloads the HID Mobile Access App, can they automatically use it?	88
11.5 What should I do before re-issuing a device to another user?	88
11.6 How do you protect the privacy of the information I provide?	88
11.7 What if I want to associate an existing Mobile Keypad to a newly created Org?	89
11.8 Can the end user restrict which partners can order Readers and Mobile IDs with their Mobile Keypad or ICE?	89
11.9 What happens if there is no Mobile Keypad for a given end user?	89
11.10 Does HID Global perform penetration testing of your Mobile Access solution?	89
11.11 Is there a defined Information Security role within HID Global?	89
11.12 Is education / training given to provide HID Global staff with an awareness of information security?	89

11.13 Where does HID Global store and process End Customer data? 89

11.14 How does HID Global monitor your network for unauthorized devices? 89

11.15 Is HID Mobile Access GDPR compliant? 89

Section **01**

Introduction

1.1 HID Mobile Access

Congratulations! Your company has migrated to a new methodology for managing secure identities for physical access. The adoption of the HID Mobile Access® service now enables staff to securely access locations using Android and iOS mobile devices. Your role as Enterprise or End User Administrator is to manage your company's users, and issue or revoke Mobile IDs via a cloud-based portal. You are also likely to be the first point of contact if employees have any questions about HID Mobile Access.

This guide will serve as a reference and to provide you with the information you need to support your company in a knowledgeable manner.

Note: For reference purposes HID Global recommends that customers retain Technical Support contact information for their authorized HID Channel Partner or Direct Integrator.

Section 02

General Questions

2.1 When was HID Global established?

HID Global was established in 1991 as Hughes Identification Devices, a subsidiary of Hughes Aircraft. The company was acquired by ASSA ABLOY in 2006 and is now part of the Global Technologies division of ASSA ABLOY.

2.2 How long has HID Global been providing the Mobile Access solution?

HID Global has been providing HID Mobile Access® since 2014.

2.3 Does HID Global rely on third parties to provide services to the End Customer?

Yes, HID Global relies on Amazon Web Services and ViaWest.

2.4 Does HID Global have a formal Business Continuity policy in place?

HID Global has a Business Continuity plan in place. The Business Continuity Management System is modeled after the ISO22301 standard.

2.5 Who is responsible for establishing and testing HID Global's Business Continuity arrangements?

The Business Continuity Management System is modeled after the ISO22301 standard. The maturity level in terms of implementation and testing is different at different local sites. BCM Plans are decentralized. On the top level the Compliance Core team is providing guidance.

2.6 Does HID Global have an incident management process?

Yes, HID Global has an Incident Management Process that follows the ITIL Incident Management Standard.

2.7 Does HID Global have a formal change management process in place?

Yes, HID Global has a Change Management process based on the ITIL framework in place.

2.8 Does HID Global comply with ISO27001?

The HID Origo Cloud Platform has been certified for compliance with ISO 27001. For additional details please refer to:

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

2.9 Can HID Global demonstrate compliance with non-national legislation and regulations, for example SOX, PCI-DSS?

SOX is not relevant as HID Global/ASSA ABLOY is not listed in the US Stock Exchange. PCI-DSS is not applicable to Mobile Access, as the solution does not process Credit Card Transactions.

Section **03**

HID Mobile Access

3.1 What is HID Mobile Access?

HID Mobile Access® complements your existing access control solution; instead of using cards or fobs to access the building, the Mobile IDs are stored on the employee's mobile device.

The HID Mobile Access service, powered by Seos®, consists of the following components:

- HID Origo™ Management Portal. A managed service that allows you to manage users and securely issue or revoke Mobile IDs to the user's mobile device.
- HID Mobile Access App for Android and iOS devices.
- HID Mobile Access SDK for Android and iOS devices.
- HID Mobile Access API.
- Mobile Access compatible readers.
- Mobile IDs with integrated Seos technology for management of trusted identities.

3.2 What is Seos?

Seos® is a technology platform created by HID Global which provides a secure, portable, adaptable, device agnostic way of managing secure identity information and applications. Seos technology is what enables the use of a mobile device as a trusted credential for physical access control.

HID Global has created an open ecosystem of Seos-interoperable products and services, including credentials, readers, and a backend infrastructure to issue and revoke credentials. The use of Seos technology on a mobile device, loaded with a secure identity, enables the use of that mobile device to securely open doors to homes, hotels, hospitals, universities, and commercial buildings.

3.3 How is the HID Mobile Access solution different from other solutions available today?

HID Mobile Access provides the industry's only mobile access solution that offers native support for iOS and Android mobile devices in both wired and wireless locks.

Our solutions are powered by Seos, a breakthrough credential technology that manages secure identity solutions and represents a new way of thinking about the end-user experience. The best-in-class security and privacy protection offered by HID Mobile Access is a scalable solution that can evolve to meet your secure identity needs. For more information visit:

<https://www.hidglobal.com/solutions/access-control/hid-mobile-access-solutions>

For more information about breakthrough credential technologies, please contact your access control integrator or the vendor where you purchased HID Mobile Access.

3.4 Does HID Global Mobile Access support both BLE and NFC?

HID Global Mobile Access supports BLE (Bluetooth Low Energy, formerly marketed as Bluetooth Smart) on both iOS and Android. NFC (Near-field Communication) is only supported on Android due to the restrictions from Apple on NFC usage on iOS. For more information on Mobile Access supported devices and BLE/NFC compatibility, refer to:

<https://www.hidglobal.com/mobile-access-compatible-devices>

3.5 What are the differences between using BLE and NFC for reader to mobile device communication?

Whether your mobile device uses BLE (Bluetooth Low Energy) or NFC (Near Field Communication) to communicate with the reader depends on the installed readers and the mobile devices that are compatible for use with Mobile Access. HID recommends the use of both BLE and NFC in the Mobile Access solution to provide optimal opening experience for a variety of devices. For information on supported devices and BLE/NFC compatibility, refer to, **Which mobile devices and operating systems are supported?**

For Android devices, tap opening using NFC gives the shortest possible opening time. For iOS devices, Tap always utilizes BLE. For Android and iOS, both Twist and Go and opening with a widget from a phone or wearable, use BLE.

To make it easier for you to use this guide, we have listed the key differences between the solutions:

	NFC	BLE
Supported mobile network operators	All mobile operators	All mobile operators
Supported device operating systems	Any Android device with NFC capability	All Android devices with Android 4.4 (or higher) iOS devices with support for Bluetooth 4.0
Supported readers	HID Signo™ readers, iCLASS SE®/multiCLASS SE® readers (Rev E or newer, shipped after Q1 2013) or readers upgraded with a BLE upgrade kit	HID Signo™ readers, iCLASS SE®/multiCLASS SE® that have a BLE module (that is, readers with a part number starting with 9nnnB or 9nnnM)
Transaction experience	Tap (short range) Quick transaction if user is aware of the “sweet spot” where the NFC antenna is located within the mobile device	Tap (short range) Twist and Go (long range) App Specific, for example widget opening from mobile device or wearable (long range)

3.6 How do I onboard for the Mobile Access service?

1. Visit the HID Origo Management Portal site at <https://portal.origo.hidglobal.com> and click **CREATE ACCOUNT**.
2. Enter your user and organization details and click **SUBMIT**.
3. After registration you will receive an email. Follow the instructions in the email to change the password and get started.

Once the onboarding process is complete you will be taken through a guided tour of the HID Origo Management Portal, together with the option to enable a free of charge trial subscription. For further details see, **Can I try Mobile Access free of charge?**

3.7 How do I order user licenses for the first time?

To purchase additional user licenses after first purchase of user licenses, see: [How can I buy additional Mobile IDs?](#)

If you are a new customer to HID Mobile Access, follow the onboarding flow referenced in the [How do I onboard for the Mobile Access service?](#) section. Send in your purchase order to your HID Channel Partner and include the following information:

- Organization ID (created during onboarding)
- Organization name
- Mobile Keypad
- Format Information (if required)
- HID Mobile Access Part Number for user licenses: MID-SUB-T100

If you are already a customer of HID Mobile Access and wish order user licenses, please contact HID Customer Service for your region via the contact details provided at:

<https://www.hidglobal.com/customer-service>

3.8 Which Service Levels are available for the HID Origo Management Portal?

HID Global will use commercially reasonable efforts to:

- Make the service available at least 99.5% of each calendar month, excluding maintenance.
- Provide notice to customers within 30 minutes of a significant service disruption.
- Provide at least 7 days advance notice for any maintenance activity.

For additional information, please refer to the following:

- [HID Global Corporation Product-Specific Support Terms Physical Access \(PACS\)](#)
- [HID Origo Services Status information](#)

3.9 What technical support is available for HID Mobile Access?

For technical support questions about HID Mobile Access, contact your access control integrator or the vendor where you purchased HID Mobile Access. HID Global provides technical support to your integrator.

Section **04**

HID Mobile Access Portal



4.1 Are there any best-practice policies I should implement within the Enterprise environment?

HID Global recommends implementing the following policies within your Enterprise environment, in combination with HID Mobile Access, as part of your IT or HR policy:

- Install a reporting process for the loss of mobile devices and the subsequent revocation of the Mobile ID(s) and disabling of the associated Mobile ID(s) within the Access Control System.
- Ban jail-broken mobile devices where the operating system has been compromised. A jail-broken mobile device is a device that has been modified to remove the restrictions imposed by the manufacturer or operator allowing access to the entire file system. This access allows for changes that are not supported by the mobile device in its default state.
- Mandate the use of a passcode, fingerprint scan, or facial recognition as additional security mechanism against the loss of a mobile device (setting within the application).
- Use a mobile device management system to manage company mobile devices (useful not only for Mobile Access, but also to secure company email and other vital company information). HID Mobile Access will work with most leading device management software.
- As Mobile Access portal administrators are transferring user data to the portal on behalf of the enterprise, you should provide a privacy policy to your users covering the transfer and storage of this data. The minimum data required to set up a user is first name, last name, and email address.
- Enable Enterprise Policy Enforcement feature via the HID Origo Management Portal. This will enforce the requirement that users within the organization have their mobile devices unlocked in order to open a door.

Note: This setting triggers an update of all credentials in your system and may cause a high load on the platform if the feature is frequently toggled on and off.

4.2 Which browsers are supported by the HID Origo Management Portal?

The following browsers have been fully tested with the HID Origo Management Portal:

- Internet Explorer x.x and above
- Chrome 68.0.3440.106 and above
- Firefox 32.0.1 and above
- Safari 5.1.7 and above

Note: The HID Origo Management Portal can be accessed using a laptop or tablet, however, access using a mobile phone is not supported.

4.3 What roles are available in the Portal?

The HID Origo Management Portal is role-based. The functional abilities for each role are listed below:

Role	Functional abilities
Organization Administrator	<ul style="list-style-type: none"> • Edit Organization settings • Manage administrative users and assign services and roles to users • Administration of mobile credential users and Reader Manager Technicians • Add/edit/delete portal users and perform password resets on their accounts. • Full access to Mobile Identities Service and Reader Manager Service functionality
Mobile Identities Service Administrator	<ul style="list-style-type: none"> • Edit Mobile Identities Service settings • Edit the invitation email sent to users • Full edit, add, and delete privileges to all users • Issue/revoke Mobile IDs and delete mobile devices
Mobile Identities Service Operator	<ul style="list-style-type: none"> • Partial access to functionality. Able to add mobile users and issue and revoke Mobile IDs. • Cannot perform configuration operations
Mobile Identities Service Reviewer	<ul style="list-style-type: none"> • Read only access • Cannot add/edit data or issue/revoke Mobile IDs
Reader Manager Service Administrator	<ul style="list-style-type: none"> • Edit Reader Manager Service settings • Add/delete Reader Manager Technicians • Issue/edit/revoke reader key authorization • Edit Reader Manager Technician information

4.4 How can I reset my HID password?

1. On the HID Origo Management Portal login page (<https://portal.origo.hidglobal.com>) enter your **Username** and click **NEXT**.

Note: Your **Username** is the email address used to create your account.

2. Click the **Forgot Password?** link.
3. In the **Password Request** dialog, click **SUBMIT**.

Password Request

If the user name you provided is correct, a temporary password will be sent to your email address upon submitting this request.

Do you want to submit this request?

4. Check your email for a **HID Origo Mobile Identities Portal Account - Temporary Password** message and follow the password reset instructions.

Note:

- If you do not see the temporary password email, check your spam or junk folder. For further assistance please visit the [HID Global Customer Support Center](#) to find the HID Technical Support contact information in your region.
- To enhance security, notification messages are now sent to the registered email address of the user for the following:
 - Modified HID Origo Mobile Identities Portal Account Password.
 - Modified HID Origo Mobile Identities Portal Authentication Factor.

4.5 Why can't I see the HID Mobile Access web application after I log into the Portal?

Your login identity has not yet been granted access to this service. Your application and account setup are most likely still in process. You should expect to see the HID Mobile Access® link on the landing page within 72 hours of completing the authentication setup. If it does not appear after that time, please visit the [HID Global Customer Support Center](#) to find the HID Technical Support contact information in your region.

4.6 Where can I check the HID Origo Service status?

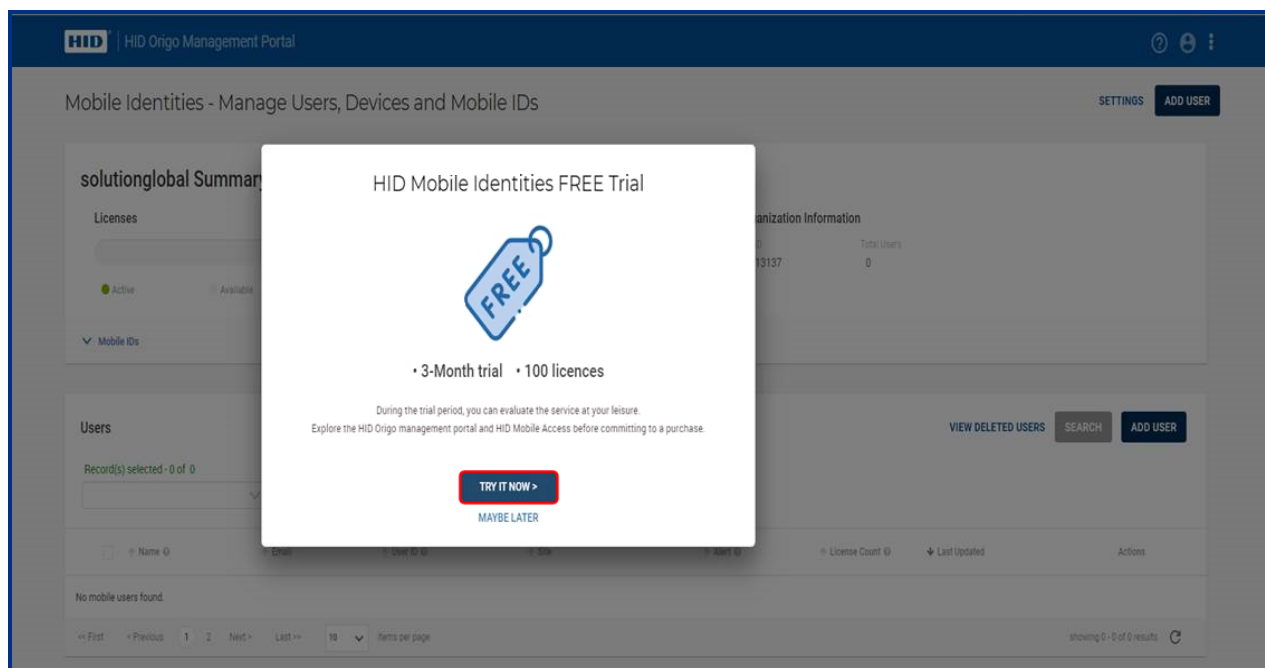
HID Origo Service status information, planned maintenance, and Incident history for the HID Origo services is available at: <https://status.origo.hidglobal.com/>.

4.7 Can I try Mobile Access free of charge?

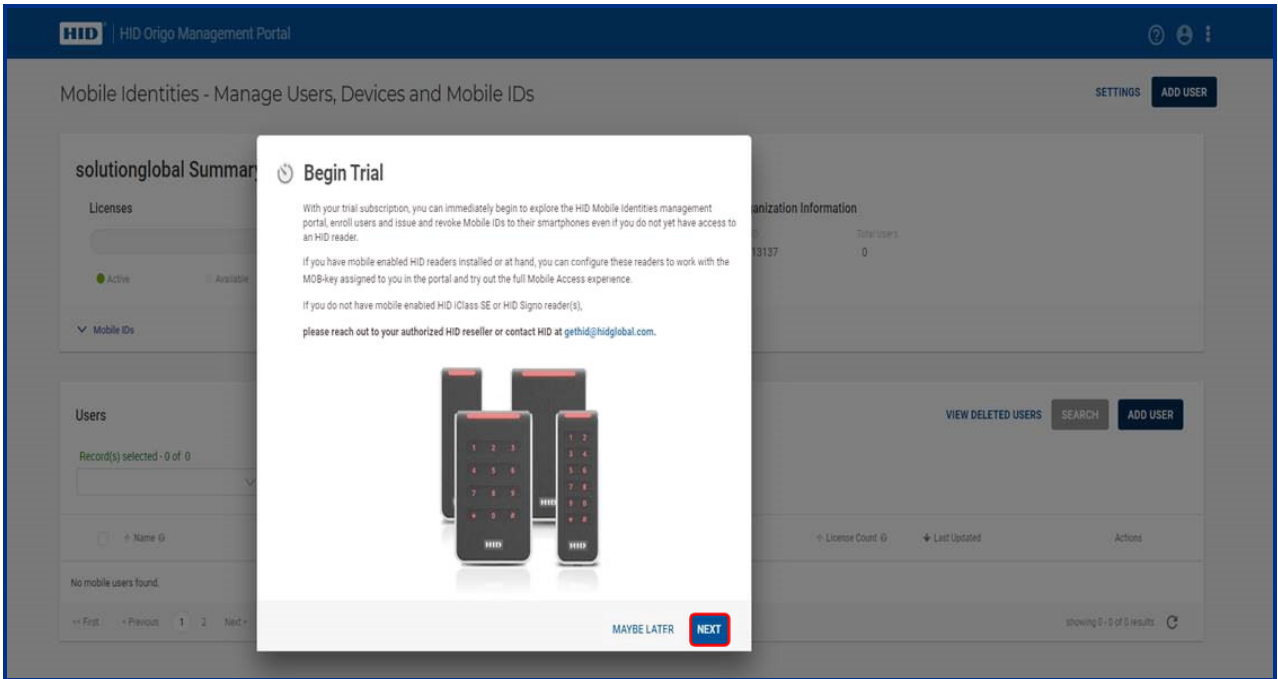
Yes, new customers have the option to try the HID Mobile Access solution, free of charge through a Trial Subscription, when they log into the HID Origo Management Portal for the first time.

Note:

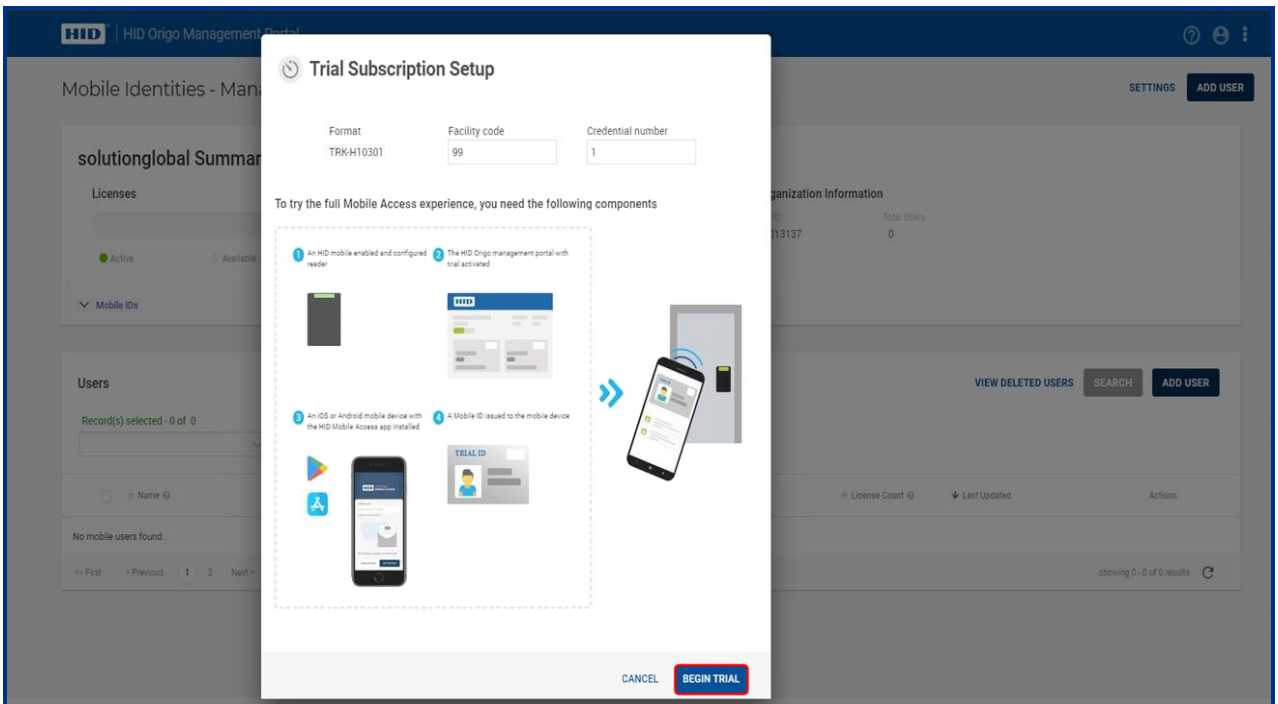
- To be able to use Trial subscription the customer must have Mobile-Ready HID readers installed. HID Mobile Access is supported by any HID Signo reader and HID iCLASS SE Mobile-Ready readers, with the Bluetooth module installed. If you do not currently have HID Mobile-Ready readers installed, please reach out to an authorized HID Channel Partner.
 - Once the Trial has started, the customer must load a MOB key into their readers and ensure the readers are configured with the correct settings for BLE communication using HID Reader Manager. If assistance is required, HID recommends that they contact an authorized HID Channel Partner.
1. Log into the HID Origo Management Portal and on the portal dashboard page select **Mobile Identities**.
 2. In the **Mobile Identities FREE Trial** dialog, click **TRY IT NOW**.



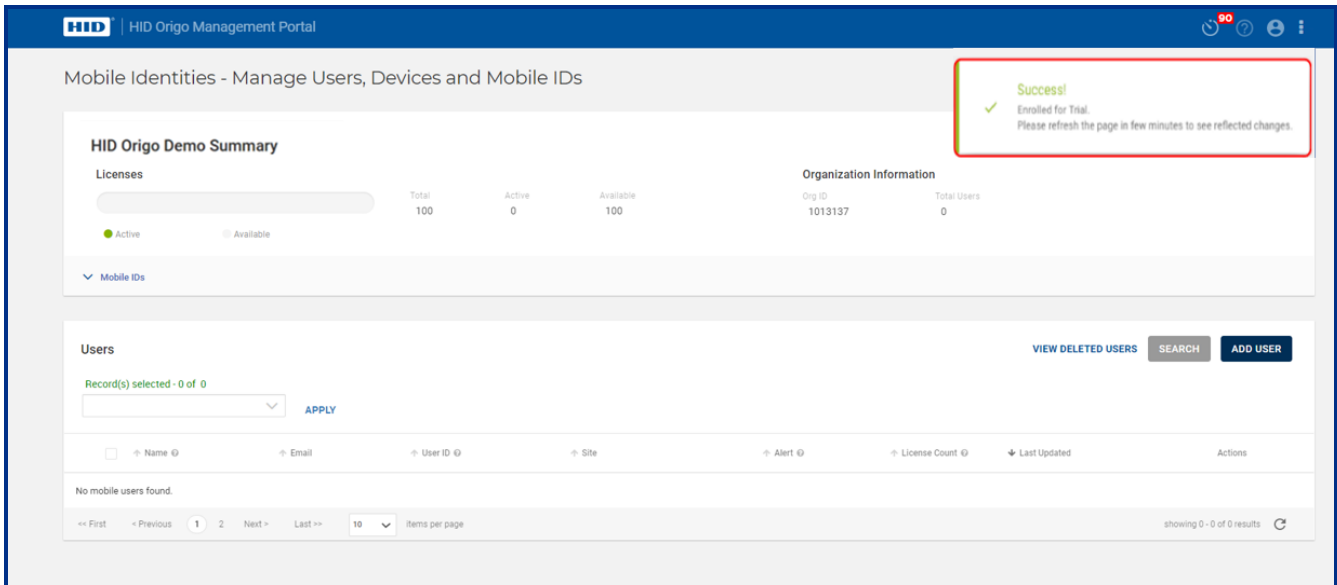
3. In the **Begin Trial** dialog, click **NEXT**.




4. Currently **TRK-H10301** is the only format supported for Trial Subscription, however, if required, you can change the **Facility code** and **Credential number**. Click **BEGIN TRIAL**.



A message is displayed to confirm that your Trial Subscription has been successfully initiated.



The following are some common questions and answers relating to the Trial Subscription feature.

Question	Answer
I have successfully opted-in for a Trial Subscription and have received the trial confirmation message, however, I do not see any Mobile IDs yet?	It can sometimes take up to 10 minutes for the trial to start. Make sure to refresh the page.
How many times can I use the Trial Subscription?	The Trial Subscription includes 100 licenses for a period of 90 days, and you can log in as many times as you want during this period.
How do I place a regular contract?	Contact an authorized HID Channel Partner to place a purchase order.
What notifications are received relating to Trial Subscription?	There are three notification types: <ul style="list-style-type: none"> • A Trial Subscription opt-in confirmation (sent after the Admin opts into the trial) • An advanced reminder about the trial expiry date (sent 30 days before the trial expiry date) • A trial expiration notification (sent after the trial expiry date)
Initially I did not opt-in for Trial Subscription. Can I opt-in for it now?	Providing you have not already placed an order for subscription user licenses, you can opt-in for the Trial Subscription by clicking on the timer icon  in the Portal header bar.
I do not want a Trial Subscription. I have already placed an order for subscription user licenses. What do I need to do?	After logging into the HID Origo Management Portal, in the Trial Subscription dialog, click MAYBE LATER to close the dialog box.

4.8 How do I redeem an invitation using a QR Code?

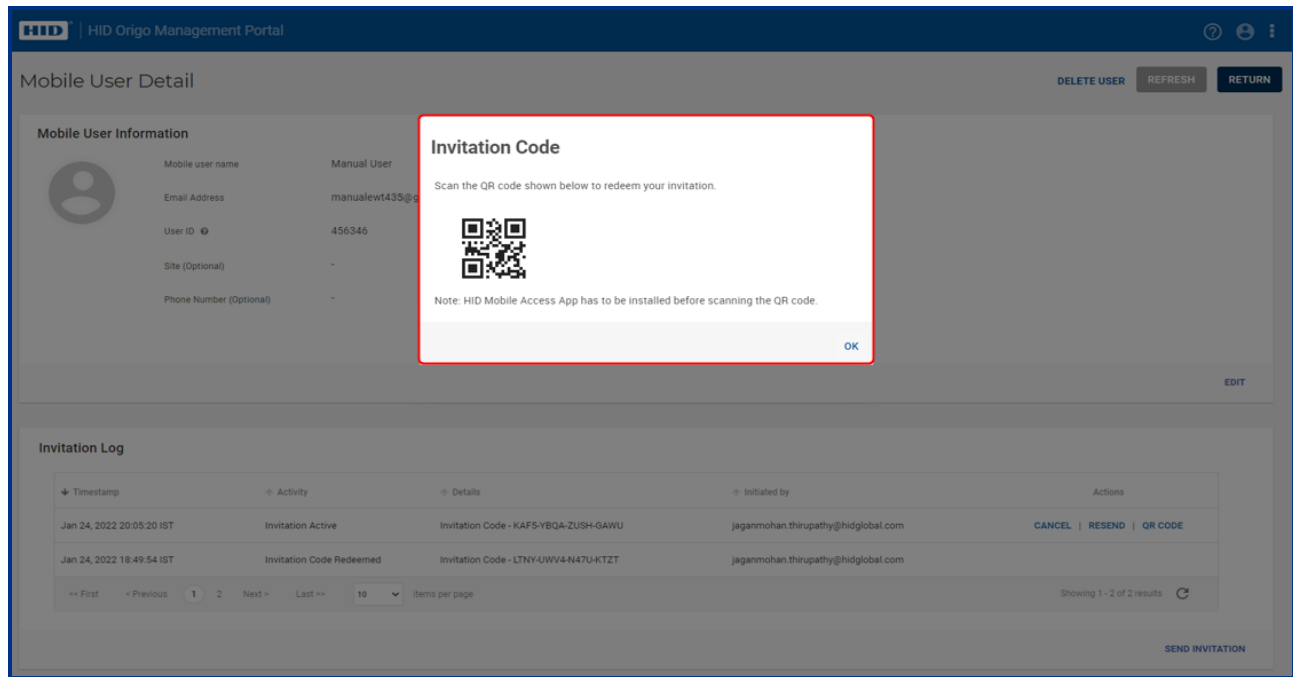
1. On the **Mobile Identities** screen, in the **Users** section, click **EDIT** associated with a displayed user.

The screenshot shows the 'Mobile Identities - Manage Users, Devices and Mobile IDs' page. At the top, there's a 'HID Origo Demo Summary' with a license progress bar (Active/Available) and organization information (Org ID, Total Users: 40). Below this is a 'Mobile IDs' section. The main 'Users' section displays a table of users. The first user is 'Manual User' with email 'manualewt435@grr.la' and User ID '456346'. The 'EDIT' button for this user is highlighted with a red box. Navigation and pagination controls are visible at the bottom of the table.

2. On the **Mobile User Detail** screen, in the **Invitation Log** section, select the **QR CODE** action.

The screenshot shows the 'Mobile User Detail' page for the user 'Manual User'. It includes 'Mobile User Information' (name, email, User ID, site, phone) and an 'Invitation Log' table. The 'Invitation Log' table has columns for Timestamp, Activity, Details, Initiated by, and Actions. The first entry is for 'Invitation Active' on 'Jan 24, 2022 20:05:20 IST' with invitation code 'KAF5-YBQA-ZUSH-GAWU'. The 'QR CODE' button in the 'Actions' column for this entry is highlighted with a red box. A 'SEND INVITATION' button is located at the bottom right of the page.

3. Scan the displayed QR Code to redeem the invitation and click **OK**.



4.9 How do I allow additional administrators to use the Portal?

If you would like to add additional users or administrators for the HID Origo™ Management Portal, the primary account administrator can add users/administrators under the **Organization Administration** menu. The primary administrator account is the account used during onboarding.

4.10 How do I configure the time zone setting in the Portal?

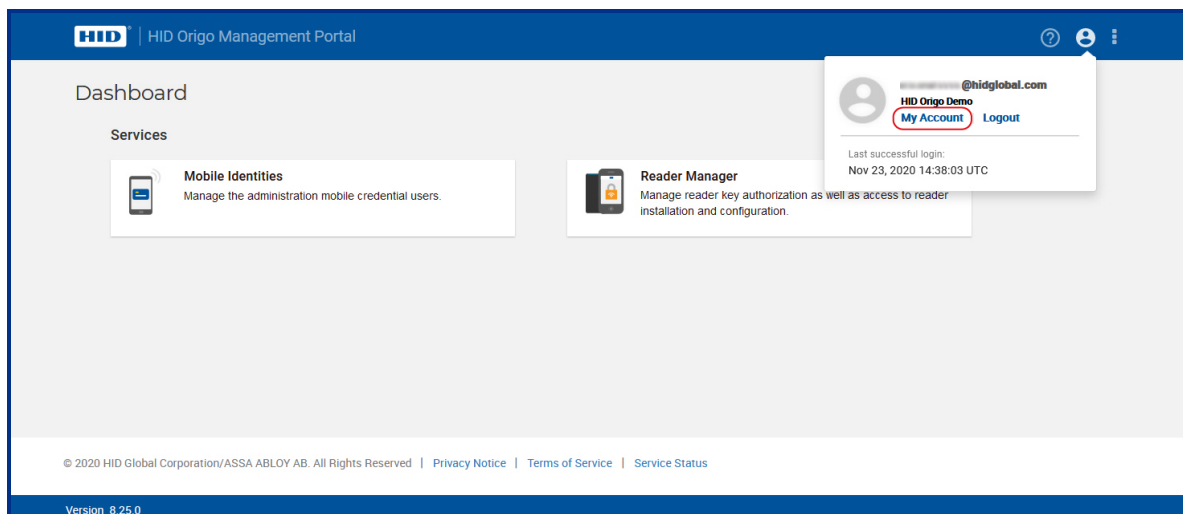
As an Enterprise or End User Administrator of a site you can configure the time zone setting in the portal. When configured, the selected time zone with a date prefix is displayed on the following portal screens:

- Mobile Identities screens:
 - Mobile Identities - Manage Users, Devices and Mobile IDs
 - Mobile ID Details
 - Mobile User Detail
 - Mobile Identities - Manage Deleted Users
 - Deleted Mobile User Detail
 - Settings > Preview Invitation Email Template
 - Export - Selected Active Users
 - Export All - All Active Users
 - Export - Deleted Users
 - Export - All Deleted Users
 - Mobile Id Inventory Export
- My Account screen
- Dashboard screen
- My Profile details pop-up

Note: Mobile Identities for a Delegation Authorization Organization, Reader Manager, End Customer Admin, and Connected Architecture do not display a configured time zone setting, only the default UTC time.

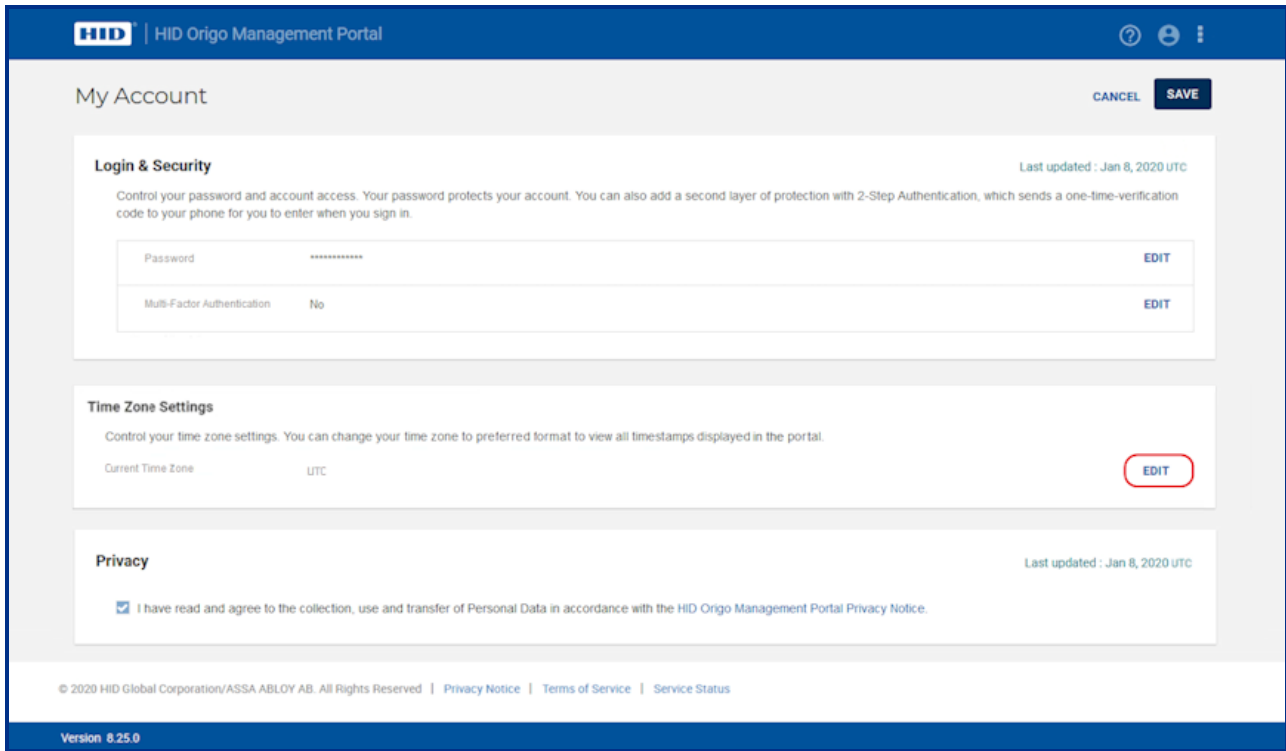
To configure the time zone setting:

1. On the HID Origo Management Portal **Dashboard** screen, click on the profile icon [👤] at the top right corner of the screen and select **My Account**.

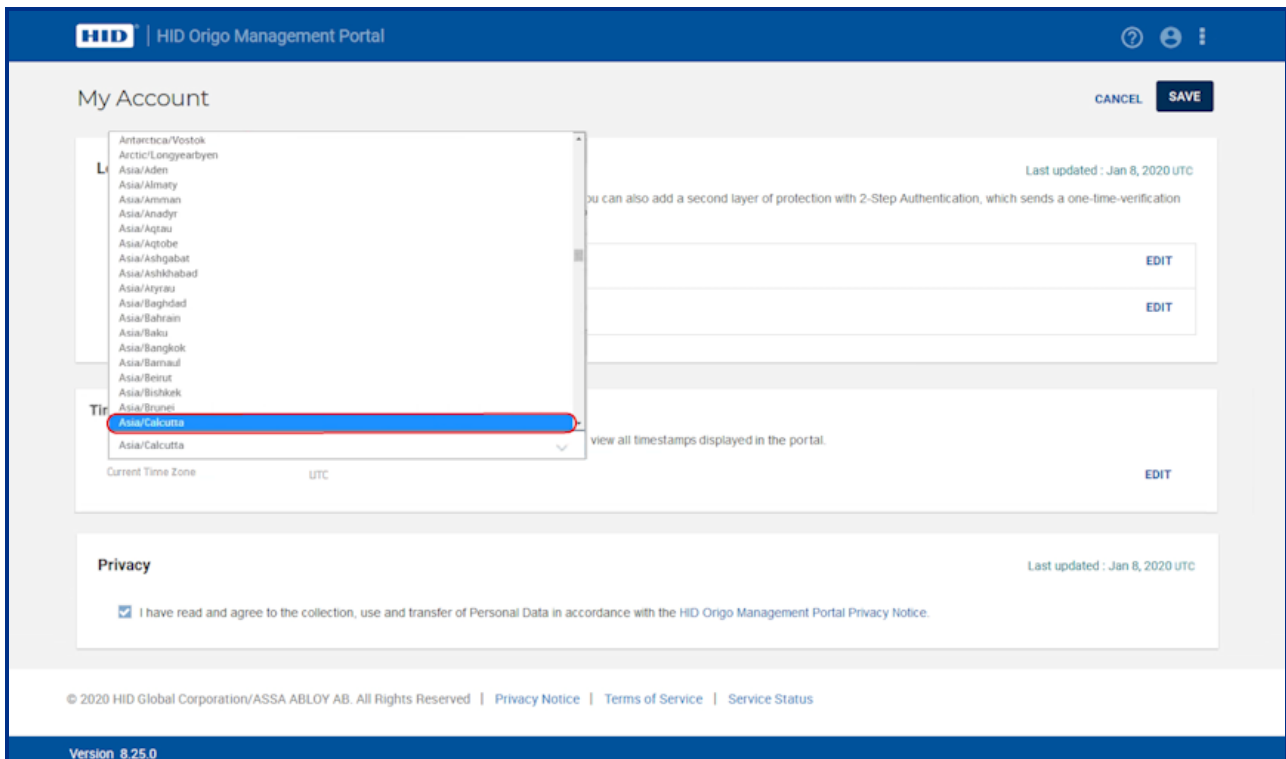


- On the **My Account** screen, scroll to the **Time Zone Settings** section and click **Edit**.

Note: The default time zone settings is **UTC**.



- Select a desired time zone from the list.



4. Click **Save**. The selected time zone, with the date prefix, will be applied across the portal.

HID | HID Origo Management Portal

My Account CANCEL **SAVE**

Personal Information Last updated : Jan 7, 2020 IST

Review your personal information. You can only update your phone number.

Name	[REDACTED]
Email address	administrator@hidglobal.com
Phone number	1 1111111 EDIT

Organizations, Services & Roles Last updated : Jan 7, 2020 IST

Review the organizations you are responsible and which roles you have been assigned for each to manage. If you have any questions, please contact your organization Admin.

Organization Name	Services	Roles
HID Origo Administrations		

Login & Security Last updated : Jan 7, 2020 IST

Control your password and account access. Your password protects your account. You can also add a second layer of protection with 2-Step Authentication, which sends a one-time-verification code to your phone for you to enter when you sign in.

Password	*****	EDIT
Multi-Factor Authentication	No	EDIT

Time Zone Settings

Control your time zone settings. You can change your time zone to preferred format to view all timestamps displayed in the portal.

Current Time Zone	Asia/Calcutta	EDIT
-------------------	---------------	-------------------

Privacy Last updated : Jan 7, 2020 IST

I have read and agree to the collection, use and transfer of Personal Data in accordance with the HID Origo Management Portal Privacy Notice.

© 2020 HID Global Corporation/ASSA ABLOY AB. All Rights Reserved | [Privacy Notice](#) | [Terms of Service](#) | [Service Status](#)

Version 8.25.0

4.11 How can I see information about my purchased user licenses for Mobile Access?

Log in to HID Origo Management Portal and select the **Mobile Identities** service option. The organization summary section displays license information.

The screenshot shows the HID Origo Management Portal interface. The main heading is "Mobile Identities - Manage Users, Devices and Mobile IDs". There are "SETTINGS" and "ADD USER" buttons in the top right. The "HID Origo Demo Summary" section includes a "Licenses" progress bar and a table:

Licenses			Organization Information	
Total	Active	Available	Org ID	Total Users
2600	2589	11	5551859	3827

Below the summary, there is a "Mobile IDs" section and a "Users" section with a "VIEW DELETED USERS" link, a "SEARCH" button, and an "ADD USER" button. A status message reads "Latest 3828 users displayed. Record(s) selected - 0 of 3828". At the bottom, a table header is visible with columns: Name, Email, User ID, Site, Alert, License Detail, Last Updated, and Actions.

- **Total:** represents the number of user licenses purchased (one user license is counted as consumed when a Mobile ID is requested for the user).
- **Active:** represents the number of active user licenses. Each unique identity record is considered a user and only active users, with at least one active mobile ID on their device, consumes a license.
- **Available:** represents the number of available user licenses.

Select **Mobile IDs** to display the Mobile IDs available for your organization. Click the view detail icon [🔍] associated with a displayed Mobile ID to view the Mobile ID specifications.

4.12 How do I control how many user licenses I consume?

A user license is counted as consumed when a Mobile ID has been requested for the user. If the Mobile ID has not been delivered to the user within the validity period set in the portal, the user license returns to the inventory of available user licenses in portal. If not delivered, for security reasons invitation codes to HID Mobile Access will, by default, expire after 48 hours.

Note: To set the invitation validity period in the portal, select **Settings** and expand the **Invitation Email & Notification Settings** option. Select **VIEW / EDIT INVITATION EMAIL TEMPLATE** and enter a period setting (hours or days) in the **Validity period for invitation** field.

4.13 I am using all purchased user licenses, how do I buy additional user licenses?

To purchase additional user licenses please contact your HID Channel Partner and provide the following information:

- Organization ID (available in the HID Management Portal on the **Mobile Identities** landing page)
- Organization name
- Contact ID
- HID Mobile Access Part Number for add on-licenses: MID-SUB-T100-ADD

Ordering information and part numbers for Mobile Access can be found in the *Readers and Credentials How to Order Guide* (PLT-02630), available from: <https://www.hidglobal.com/documents>.

Note: In certain circumstances, for example if a renewal order is placed for a lower number of user licenses than the number of active users, the account will end up in over-usage. This means that no additional users can be added or credentials can be issued until more user licenses have been purchased, or enough credentials have been revoked to free up available user licenses.

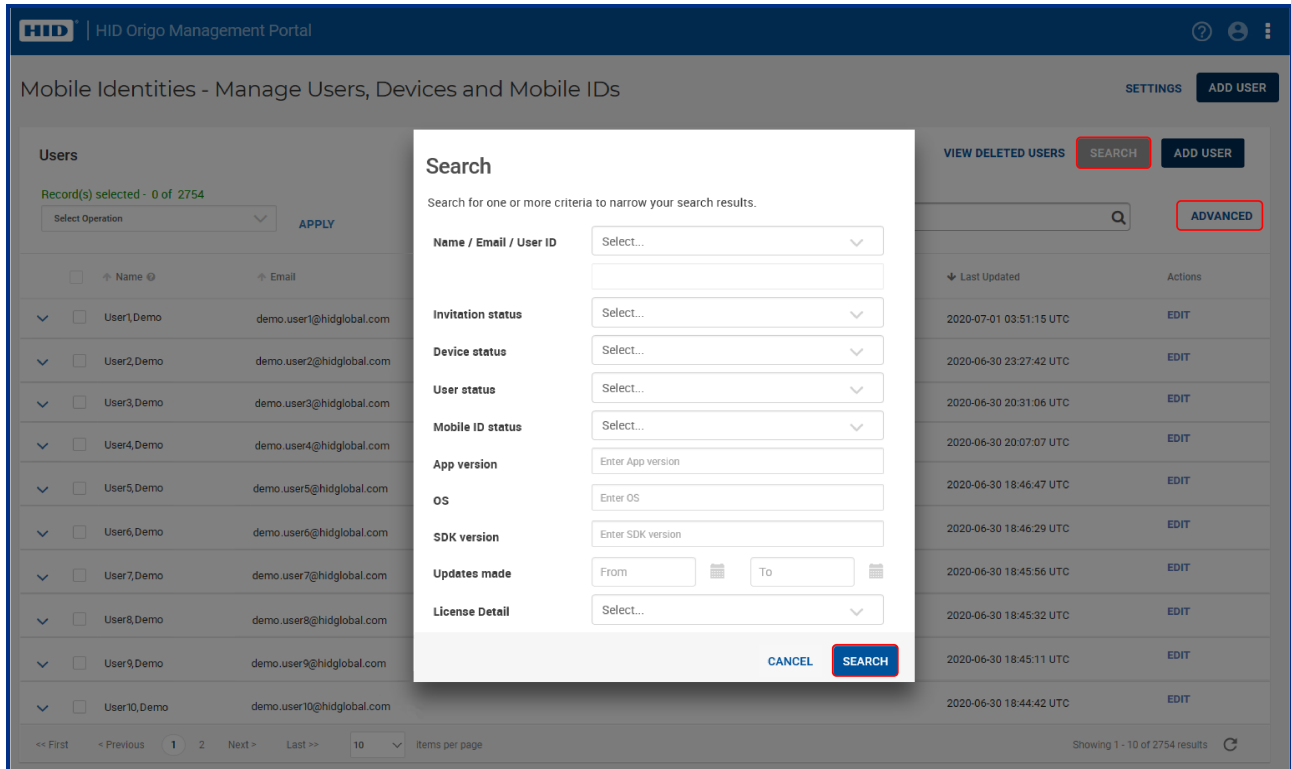
4.14 How can I find out which users are inactive?

Note: A quick search only performs a user search across the first set of 5000 users that have recently been created or modified. Therefore, if the Organization has more than 5000 users, an advanced search criteria should be used as this will search across all the user records irrespective of the size (as the user record may not be available in the first set of 5000 users).

There is no direct filter available to identify inactive users however this can be achieved by using filter options in advanced search function.

1. On the **Mobile Identities** main page, scroll to the **Users** section.
2. Click **SEARCH** and click **ADVANCED**.
3. In the **Search** dialog, select one or several listed criteria to narrow the search results.

4. Click **SEARCH** to return the search results.



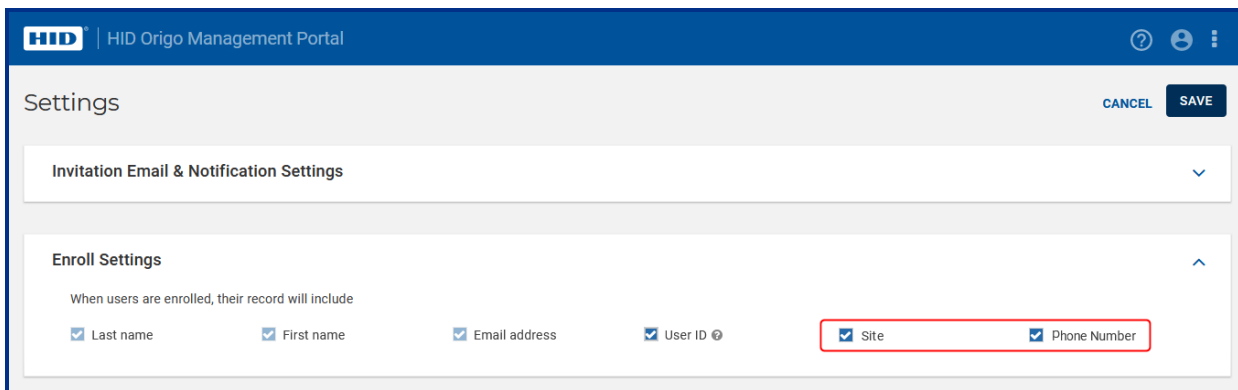
4.15 How do I enable the Site field and Phone Number field in the Portal?

For countries where there is a requirement to include site information and phone number as part of a user record, these fields can be enabled within the Mobile Identities application for user enrollment and for when mobile user records are exported.

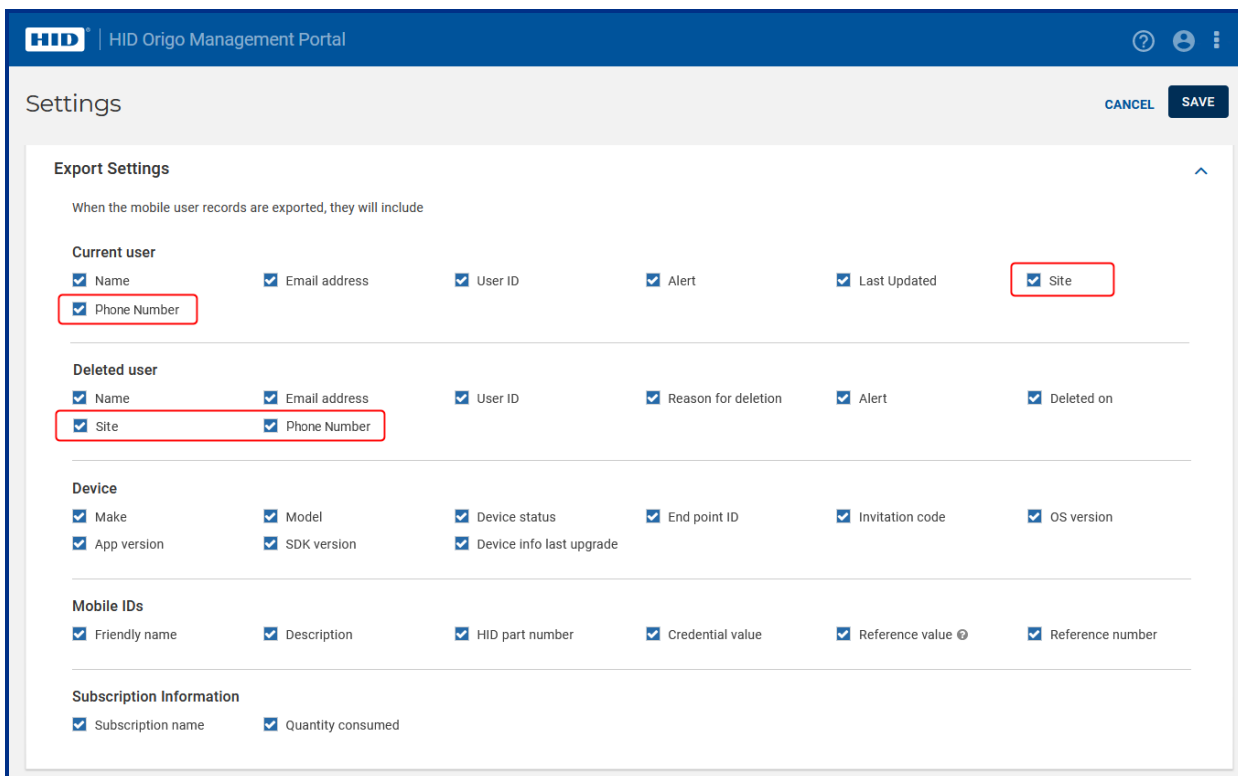
Note: As a default the **Site** field and **Phone Number** field are disabled.

To enable the **Site** field and **Phone Number** field for user enrollment and user record export:

1. On the **Mobile Identities** main page, select **Settings**.
2. To enable the **Site** field and **Phone Number** field for user enrollment expand the **Enroll Settings** section and select the **Site** and **Phone Number** options.



3. To enable the **Site** field and **Phone Number** field for when mobile user records are exported, expand the **Export Settings** section, and select the **Site** and **Phone Number** options.



If enabled the **Site** and **Phone Number** fields are available for **Single User** enrollment and in the sample upload file for **Multiple Users** enrollment.

Note: When enabled these fields are optional for **Single User/Multiple Users** enrollment. The **Site** field supports a maximum of 50 characters. The **Phone Number** field supports a maximum of 30 characters (including space, hyphen, and the plus symbol).

The screenshot shows the 'Enroll Mobile User' interface. At the top, there's a header with the HID logo and 'HID Origo Management Portal'. Below that, the title 'Enroll Mobile User' is displayed with 'CANCEL' and 'ENROLL' buttons. The main content area is titled 'Mobile User Profile' and has two tabs: 'Single User' (selected) and 'Multiple Users'. On the left, there's a user profile icon. The form fields are as follows:

- Email address:** testuser007@grr.la
- Name:** Prefix (optional), Test, User007, Suffix (optional)
- User ID:** 1004329
- Site (Optional):** Chennai
- Phone number (Optional):** +33 345-758-456

 A red rectangular box highlights the 'Site' and 'Phone number' fields.

If enabled **Site** and/or **Phone Number** information is displayed and available on the following screens:

- **Users** screen: Site information column is displayed in the active users and deleted users tables. Phone Number information is not displayed.
- **Mobile User Detail** screen: Site and Phone Number information displayed.
- **Delete Mobile User Detail** screen: Site and Phone Number information displayed.
- **Enroll Multiple Users Status** screen: Site and Phone Number information displayed.
- **Enroll Multiple Users Summary** screen: Site and Phone Number information displayed.

4.16 How do I enroll users and issue a Mobile ID to their mobile device?

As an Enterprise or End User Administrator of a site, you can add users either one-by-one or via file import.

1. On the **Mobile Identities** screen, click **ADD USER**.
2. On the **Enroll Mobile User** screen select either the **Single User** or **Multiple Users** option.

Note: To enroll multiple users, you need to create a **.csv** or **.xls** file which contain the columns “Last Name, First Name, Email Address, User ID” and upload it using the upload function provided.

3. Enter the information of the single user or select the file to upload (for multiple users).
4. Select the desired enrollment option (send invitation only or send invitation and reserve Mobile ID).
5. Click **ENROLL**.

Note:

- HID recommends sending registration codes via the corporate email system and not to insecure email addresses, such as “free mail” accounts.
- Each email address can only be enrolled once. However, when the user is enrolled, you can assign up to 10 Mobile IDs to each user’s device or add up to 5 devices per user. A user can only have one Mobile ID with a specific MOB Key reference, so therefore, you cannot issue two Mobile ID(s) of the same MOB Key to one device.

6. The user(s) are added to the user list with the status **Invitation Active**. The user receives an email which contains a link to download the HID Mobile Access Application from the Application Store links, and an invitation code.
7. After a user has downloaded the Mobile Access App and entered the invitation code, the status will change to **Invitation Code Redeemed** and now you can issue a Mobile ID to this user if you did not select the option to **Select and Reserve a Mobile ID** when you did the enrollment above.
8. To issue a Mobile ID to a user, in the **Users** section click on the **EDIT** action associated with a displayed user record.
9. On the **Mobile User Detail** window, click **Issue Mobile ID**.
10. Manually select a Mobile ID from the available Mobile IDs pool or issue a Mobile ID in an automatic sequence.

Note: You can automate this process by pre-assigning the Mobile ID at the time of enrolling the user by selecting the option, **Select and reserve Mobile ID(s) that will be issued when this user accepts the invitation code to register his or her device option**.

4.17 How do I assign a photo image to an individual enrolled user?

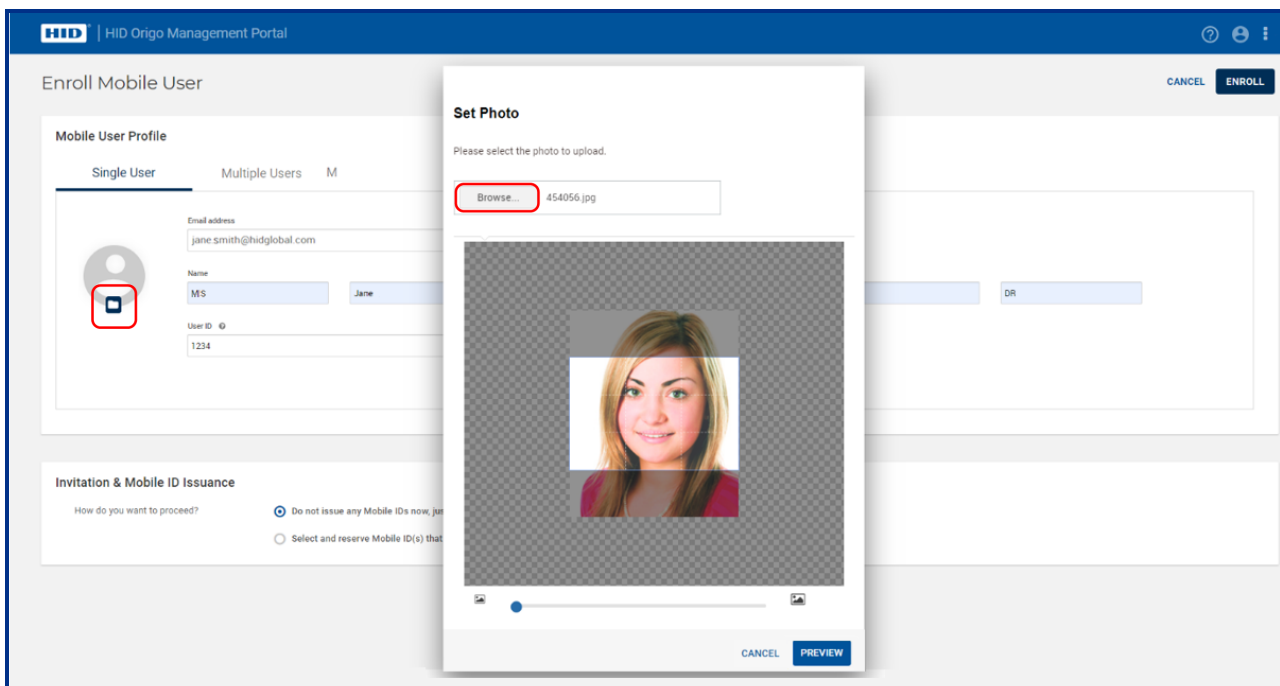
As an Enterprise or End User Administrator of a site, you can upload and assign a photo image to an individual enrolled user and subsequently edit/delete the user photo.

To upload and assign a photo when enrolling a user:

1. On the **Mobile Identities** screen, click **ADD USER**.
2. On the **Enroll Mobile User** screen select the **Single User** option.
3. In the **Mobile User Profile** section enter the user information.

Note: Two new optional fields, **Prefix** and **Suffix**, have been added to **Name**.

4. To upload and assign a photo image, click on the browse icon [📁] in the image placeholder area.
5. In the **Set Photo** dialog click **Browse** and select an image to upload. The following image criteria applies:
 - The recommended optimal photo aspect ratio is 2:3.
 - Supported images dimensions in the **Set Photo** pane is 240 x 160 pixels.
 - Supported image formats are **JPG** and **PNG**.

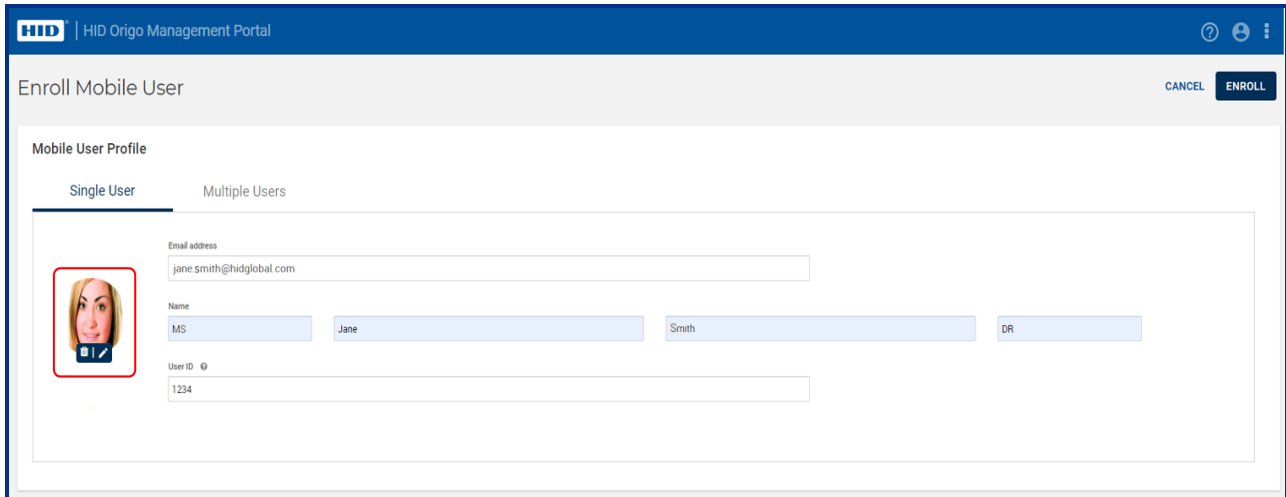


6. Click **PREVIEW** to preview the image for the user profile.
7. If the image appears correctly click **ENROLL** to save the user details with photo.

4.17.1 Edit/delete newly enrolled user photo

To edit or delete a user photo image on the **Enroll Mobile User** screen:

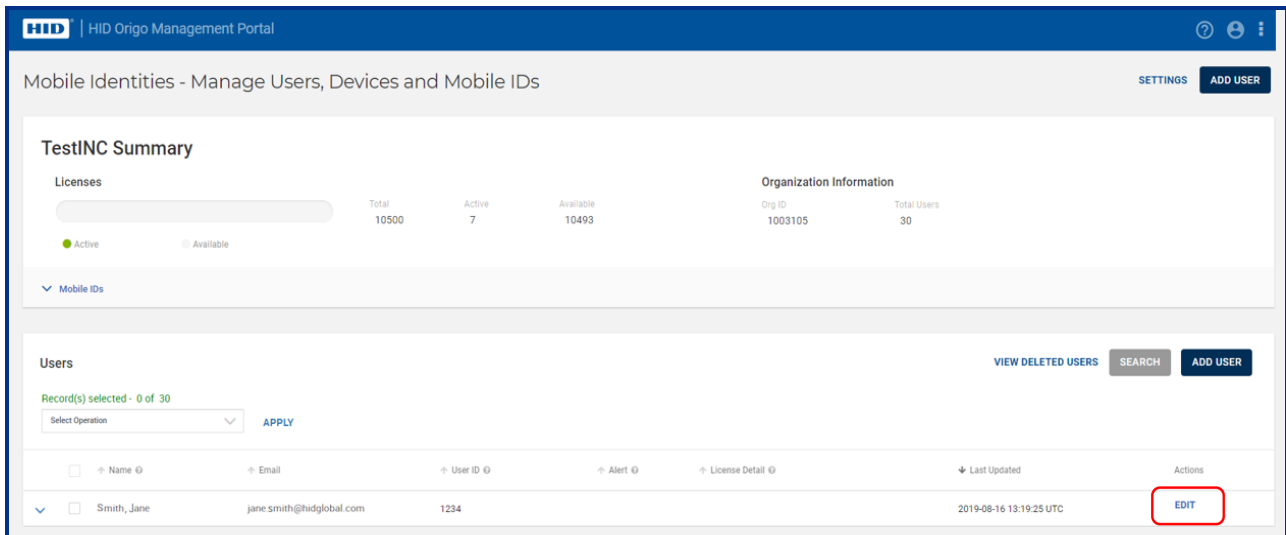
1. Hover the mouse cursor over the user photo.
2. Select the edit icon [📎] and make the required changes in the **Set Photo** dialog, or select the delete icon [🗑️] to delete the user image.



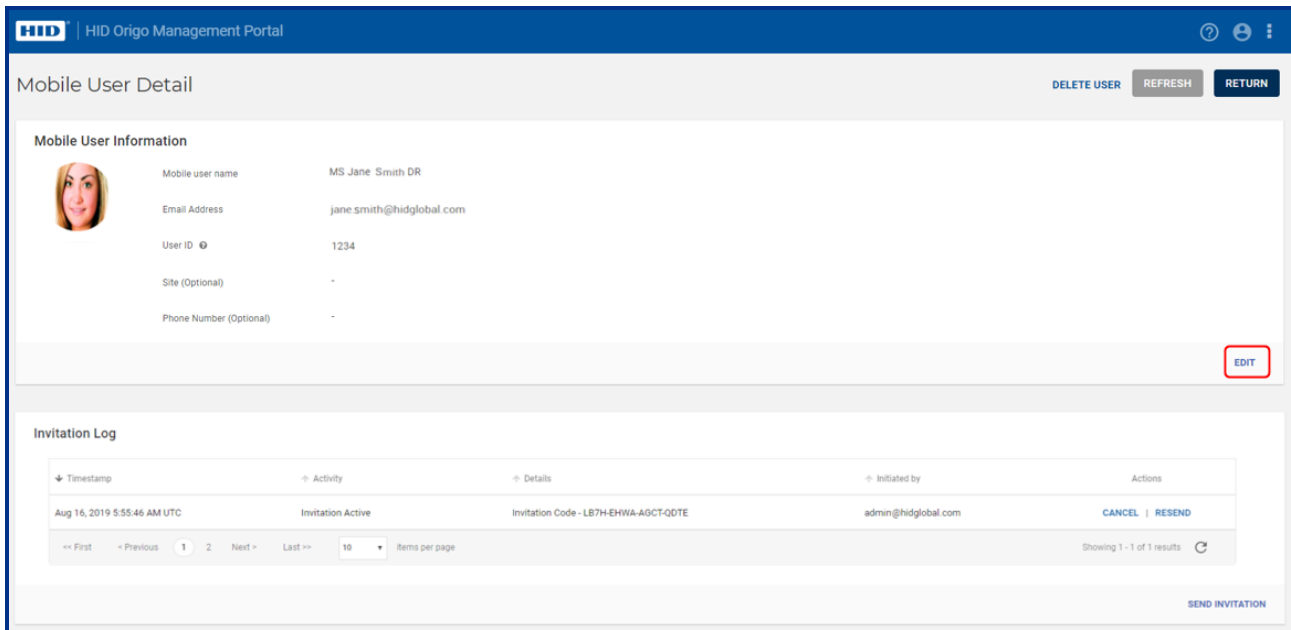
4.17.2 Edit/delete existing user photo

To edit or delete a photo image of an existing user on the **Enroll Mobile User** screen:

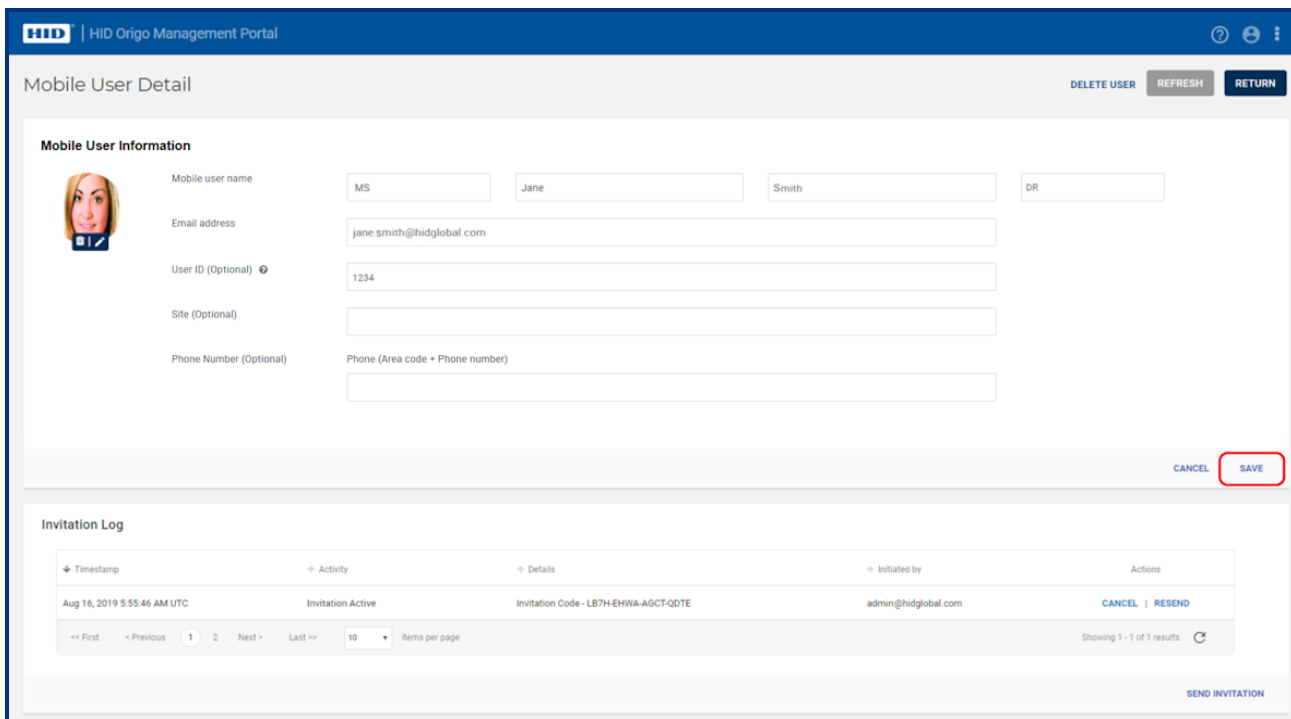
1. On the **Mobile Identities** screen, in the **Users** section, click **EDIT** associated with a displayed user.



- On the **Mobile User Detail** screen, in the **Mobile User Information** section, click **Edit**.



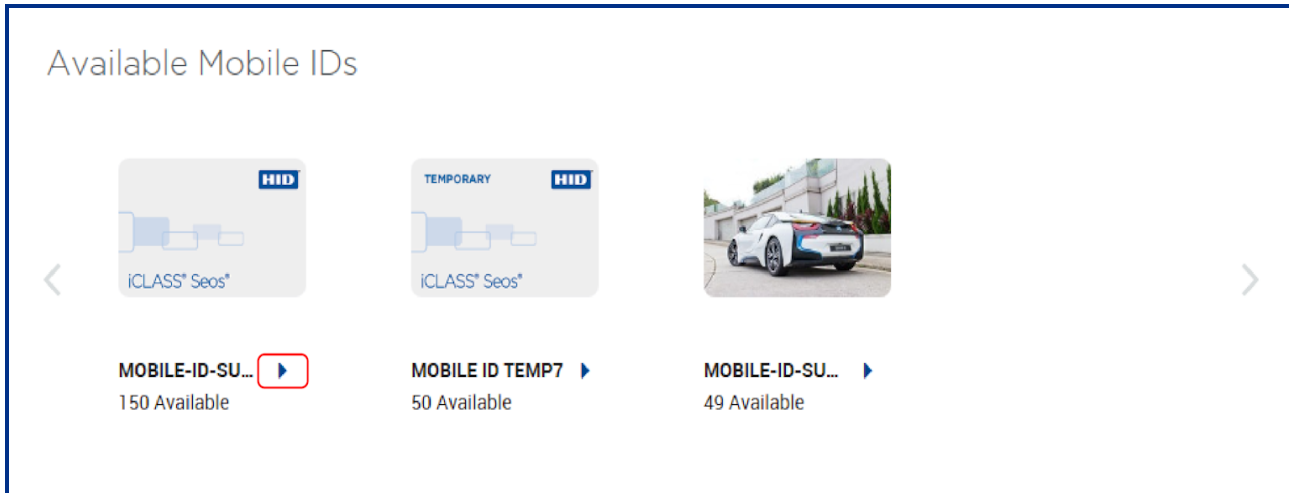
- Hover the mouse cursor over the user photo.
- Select the edit icon [📎] and make the required changes in the **Set Photo** dialog or select the delete icon [🗑️] to delete the user image.
- When the required changes have been made, click **SAVE**.



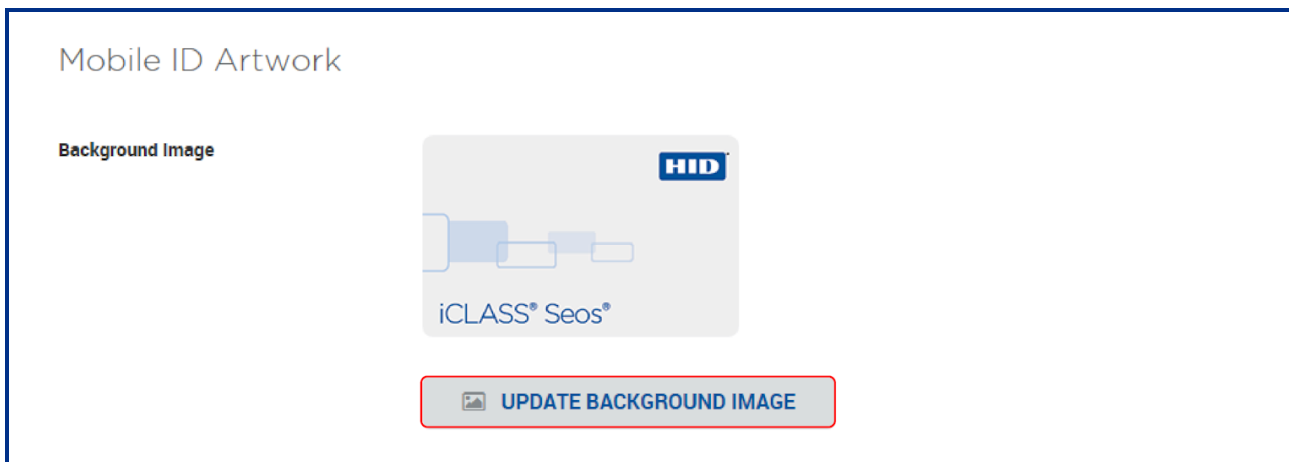
4.18 How do I change the badge image to my corporate logo?

Instead of using the default HID Global badge image, you can upload an image with your corporate logo and color scheme. This is then pushed to the mobile devices and is visible within the user's HID Mobile Access app on issuing new Mobile IDs.

1. On the **Mobile IDs & User** page, scroll to the **Available Mobile IDs** section.
2. Click the edit icon [▶] associated with a displayed Mobile ID.

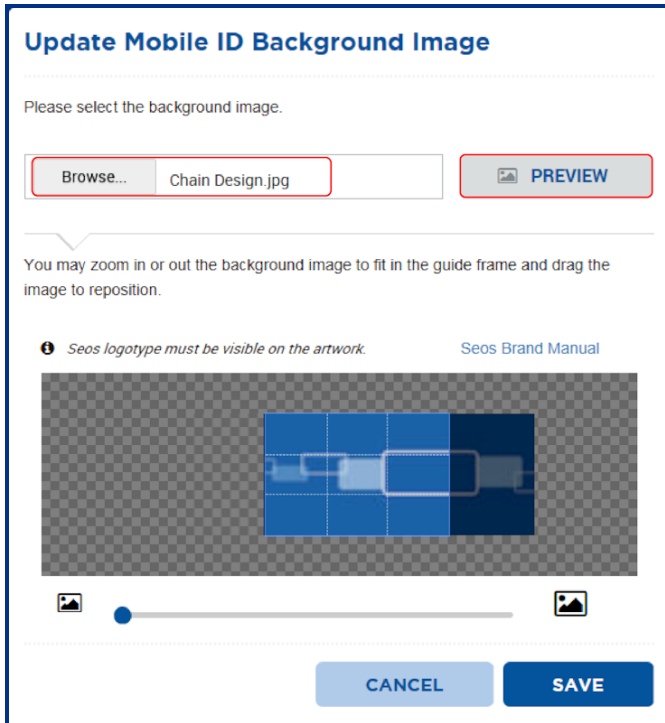


3. In the **Mobile ID Artwork** section click **UPGRADE BACKGROUND IMAGE**.



- Click **Browse** and select a new image from your computer. The image must comply with the following specifications:
 - File format: **.png** or **.jpg**
 - File size up to maximum of 1 MB
 - Dimensions: 240 pixels wide by 160 pixels high
 - Seos logo type must be visible on the artwork (information on this can be found within the portal)
- Click **SAVE** to update the Mobile ID background image.

Note: Before saving the image, click **PREVIEW** to resize and reposition the image in the guide frame.



4.19 How do I configure an invitation link?

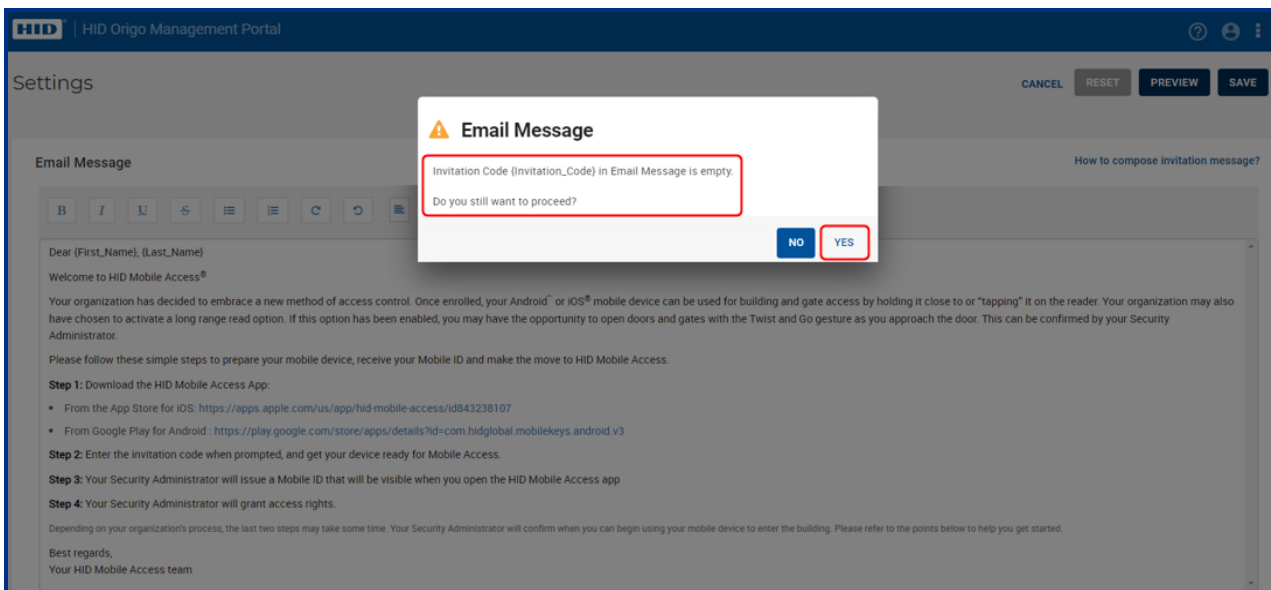
1. On the **Mobile Identities** page, click **Settings**.
2. Expand the **Invitation Email and Notification Settings** option.
3. Under **Configure invitation link** enter a link in the field. For example: **myapp://company.org?invitationCode**

For any outgoing invitation code emails, the Invitation Code is appended to the end of whatever link was configured, replacing the **invitationCode** part. When a user selects the received link, they will be prompted to open it in a given app.

4.19.1 Remove invitation code from email

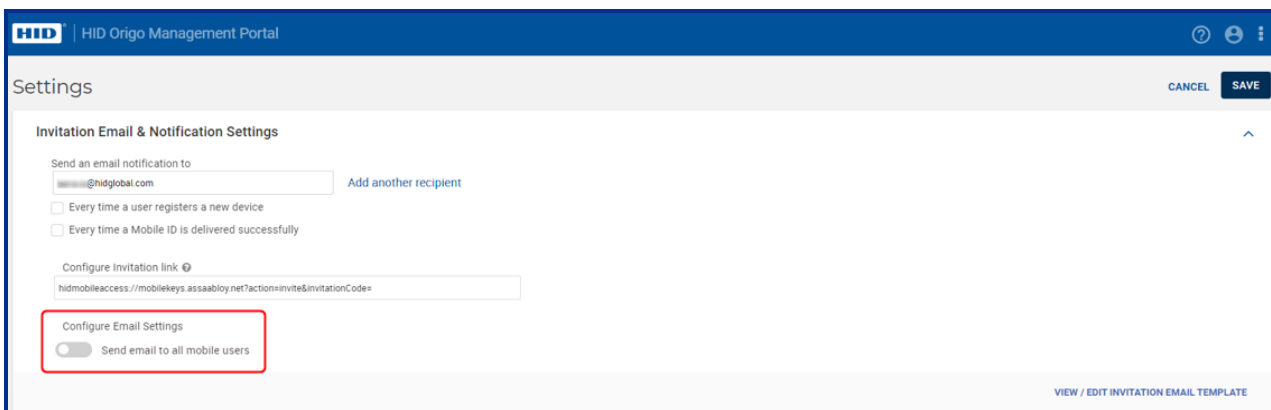
The portal provides the Org Admin with the ability to remove the invitation code from the invitation email.

Note: If the invitation code is removed from the email, the only option to redeem the code is through manual input or consuming the QR code in the portal (see [How do I redeem an invitation using a QR Code?](#)).



4.19.2 Configure invitation email distribution

The portal provides the Org Admin with the ability to disable the distribution of the invitation email to all mobile users.




4.20 How do I change the invitation email template?

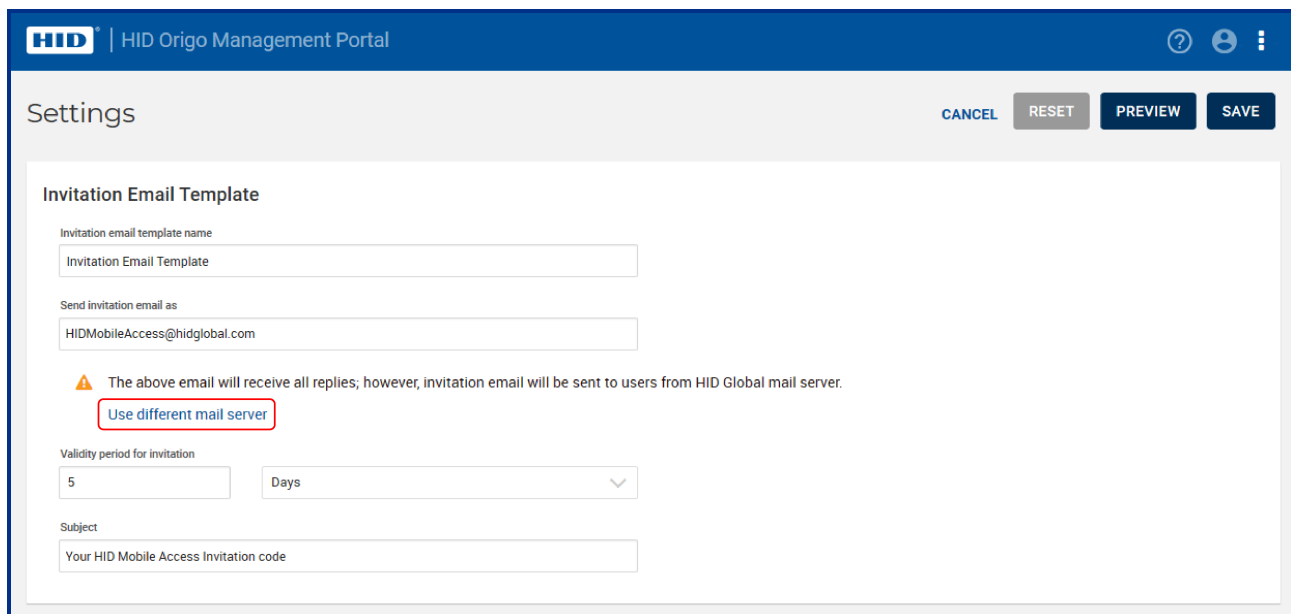
1. On the **Mobile Identities** page, click **Settings**.
2. Expand the **Invitation Email and Notification Settings** option.
3. Click **VIEW/EDIT INVITATION EMAIL TEMPLATE**.
4. Modify the following fields as required:
 - **Invitation email template name:** Enter a custom name for the email template.
 - **Send invitation email as:** Enter an email address (where the response to this invitation email will be sent).
 - **Validity period for invitation:** Enter the number of hours or days until this invitation will expire.

Note: Allow enough time for a response. A minimum of four to five days is recommended.

- **Subject:** The subject of this email can be customized to your needs.
5. In the **Email Message** section modify the text of the invitation email as required.

Note: On the Email Message section icon bar there is a hyperlink icon [] that allows you to insert and remove links to websites.

6. Once your message modifications are complete, click **PREVIEW** to review your changes.
7. Click **SAVE** to save your changes.



The screenshot shows the 'Settings' page in the HID Origo Management Portal. The 'Invitation Email Template' section is active, displaying several input fields: 'Invitation email template name' (containing 'Invitation Email Template'), 'Send invitation email as' (containing 'HIDMobileAccess@hidglobal.com'), 'Validity period for invitation' (set to '5' days), and 'Subject' (containing 'Your HID Mobile Access Invitation code'). A warning message states: 'The above email will receive all replies; however, invitation email will be sent to users from HID Global mail server.' Below this message is a red-bordered button labeled 'Use different mail server'. At the top right of the settings area are buttons for 'CANCEL', 'RESET', 'PREVIEW', and 'SAVE'.

4.21 How many times can an invitation code be used?

Invitation codes are unique and can be redeemed only once. If user attempts to redeem the same invitation code a second time it becomes an invalid invitation code and a **Please verify the code is correct** error message is displayed.

4.22 How do I configure a custom mail server?

1. On the **Mobile Identities** page, click **Settings**.
2. Expand the **Invitation Email and Notification Settings** option.
3. Enter an email address in the **Send an email notification to** field.
4. Click **VIEW/EDIT INVITATION EMAIL TEMPLATE**.

HID Origo Management Portal

Settings

Invitation Email & Notification Settings

Send an email notification to

@hidglobal.com

@grr.la Remove

Every time a user registers a new device

Every time a Mobile ID is delivered successfully

Configure Invitation link

hidmobileaccess://mobilekeys.assaabloy.net?action=invite&invitationCode+

Configure Email Settings

Send email to all mobile users

VIEW / EDIT INVITATION EMAIL TEMPLATE

5. Click **Use different mail server**.

HID Origo Management Portal

Settings

Invitation Email Template

Invitation email template name

Invitation Email Template

Send invitation email as

HIDMobileAccess@hidglobal.com

⚠ The above email will receive all replies; however, invitation email will be sent to users from HID Global mail server.

Use different mail server

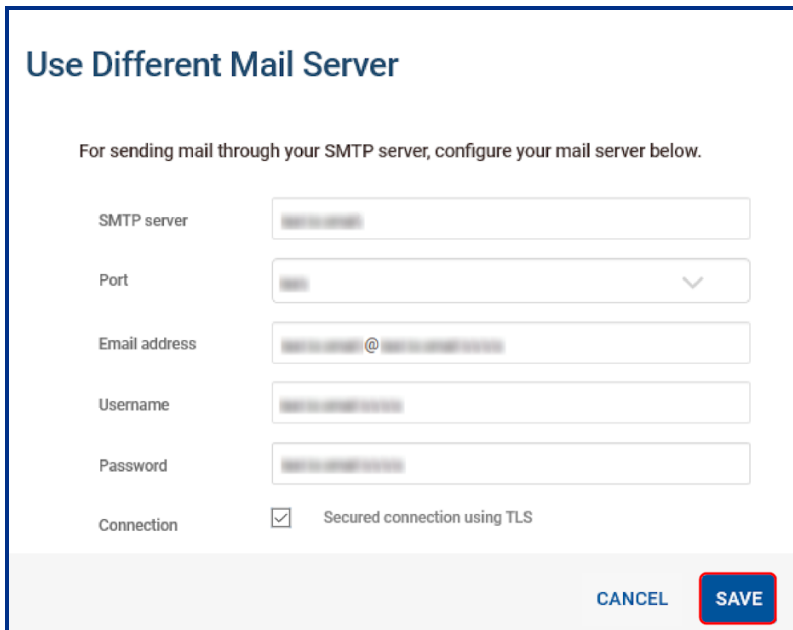
Validity period for invitation

5 Days

Subject

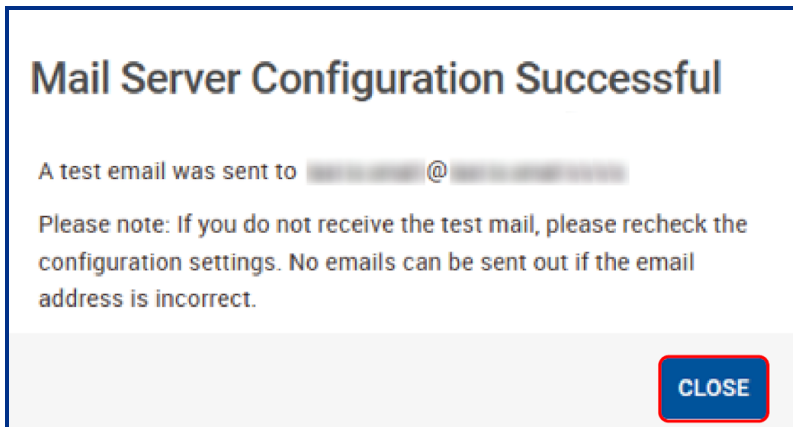
Your HID Mobile Access Invitation code

6. Enter your custom mail server details and click **SAVE**.



The screenshot shows a web form titled "Use Different Mail Server". Below the title is a sub-header: "For sending mail through your SMTP server, configure your mail server below." The form contains several input fields: "SMTP server" (text), "Port" (dropdown menu), "Email address" (text), "Username" (text), and "Password" (text). There is also a checkbox labeled "Connection" with the text "Secured connection using TLS" next to it. At the bottom right of the form are two buttons: "CANCEL" and "SAVE".

If the mail server configuration is successful, the following notification is displayed. Click **CLOSE**.



The screenshot shows a notification box with the title "Mail Server Configuration Successful". The text inside reads: "A test email was sent to [redacted] @ [redacted]". Below this is a note: "Please note: If you do not receive the test mail, please recheck the configuration settings. No emails can be sent out if the email address is incorrect." At the bottom right of the notification box is a "CLOSE" button.

7. To validate the mail server settings, check that you receive an email containing the following details.

From: <<Email address entered in Step 6>>

To: <<Email address entered in Step 3>>

Subject: Your HID Mobile Access® Portal Account - Mail Server Configuration Successful

Body:

Dear <<Local-part of email address entered in Step 6>>,

Your mail server configuration is successful. This test email is to acknowledge that your configuration settings are correct.

© HID Global Corporation/ASSA ABLOY AB HID Secure Identity Services Privacy Policy

Note: If you do not receive an email after approximately five minutes then the mail server configuration is unsuccessful. This will result in users not receiving their invitation emails. To resolve this issue, you can either click **Delete Mail Server**, which will result in mails being triggered from the default HID mail service or click **Edit Mail Server** and modify the settings so that mails are received at the next attempt.

The screenshot shows the 'Settings' page for 'Invitation Email Template' in the HID Origo Management Portal. The page includes a header with the HID logo and 'HID Origo Management Portal', and navigation buttons for 'CANCEL', 'RESET', 'PREVIEW', and 'SAVE'. The main content area is titled 'Invitation Email Template' and contains the following fields and options:

- Invitation email template name:** A text input field containing 'Invitation Email Template'.
- Send invitation email as:** A text input field containing 'HIDMobileAccess@hidglobal.com'.
- Warning:** A yellow triangle icon followed by the text: 'The above email will receive all replies; however, invitation email will be sent to users from HID Global mail server.' Below this is a red-bordered button labeled 'Edit Mail Server | Delete Mail Server'.
- Validity period for invitation:** A dropdown menu with '5' selected in the first part and 'Days' in the second part.
- Subject:** A text input field containing 'Your HID Mobile Access Invitation code'.

Possible items to check when a mail server configuration is unsuccessful:

- The provided SMTP server details may be incorrect.
- Incorrect Port and TLS setting.
- The mail server you have configured may only be allowing requests from whitelisted IPs, therefore white list the HID server's IP to allow the request.
- When using free generic SMTP services, for example Gmail, Outlook, these services may have Captcha enabled for the user login. Therefore automated services might be blocked by these providers.

4.23 Why can't I delete users?

The ability to delete users is limited by a **Max number of users deleted per day** threshold.

1. On the main page, click **Settings**.
2. Open the **Configure Delete Threshold** option.
3. Enter a value for **Max number of users deleted per day**.
4. If required enter a **Delete threshold** value. This is a time threshold after which the system automatically completes the delete operation and places the mobile device or ID in a deleted state.

The screenshot shows the 'Settings' page in the HID Origo Management Portal. The 'Configure Delete Threshold' section is highlighted with a red box. It contains two input fields: 'Max number of users deleted per day' with the value '50' and 'Delete threshold' with the value '10' and a unit dropdown set to 'Minutes'. A warning message states: 'For security reason, any changes to delete threshold will take effect after 24 hours.' Below this, a note explains: 'When attempting to delete a mobile device or ID, if the mobile device is not reachable (e.g turned off or out of range), the system will periodically retry the delete operation. After the time configured below, the system automatically completes the delete operation and places the mobile device or ID in a deleted state.'

4.24 How can I revoke Mobile IDs from a user's mobile device?

1. On the main page, select a displayed user by clicking on the icon next to the user name.
2. Click **Delete Mobile ID** to remove a single Mobile ID. You can also use **Delete Device** to remove the complete device or **Delete Mobile ID User** to remove the user and all devices and Mobile IDs of that user.

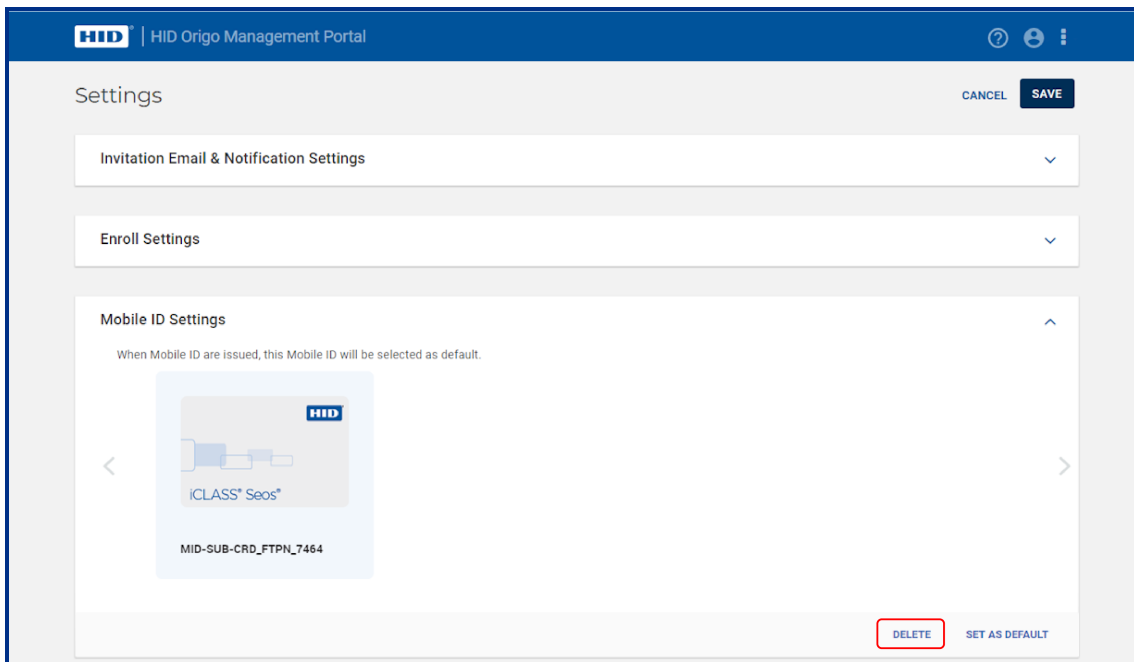
Note: Revoking a Mobile ID is not possible when the mobile device is roaming without a data connection, in flight mode or switched off. Therefore always make sure that you revoke the access rights associated with this Mobile ID within your Access Control System.

4.25 How do I manage obsolete or duplicate Mobile IDs (MIDs)?

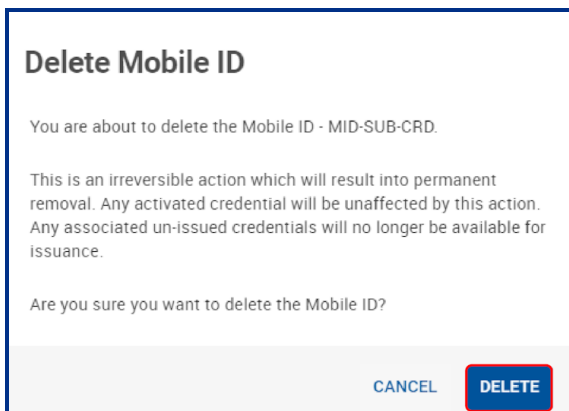
As a HID administrator or a Mobile Identities administrator you can delete obsolete MIDs (the MIDs that are not used within the allocated MID range), check for and remove duplicate MIDs, and select and remove a range of MIDs.

4.25.1 Delete a Mobile ID (MID)

1. Log into the HID Origo Management Portal and on the portal dashboard page select the **Mobile Identities** option.
2. If you are a HID administrator select an Organization and click **Go**. If you are a Mobile Identities administrator you will be automatically directed to the Mobile Identities page for your organization.
3. On the **Mobile Identities** page, select **Settings**.
4. On the **Settings** page, in the **Mobile ID Settings** section, select a MID type and click **Delete**.

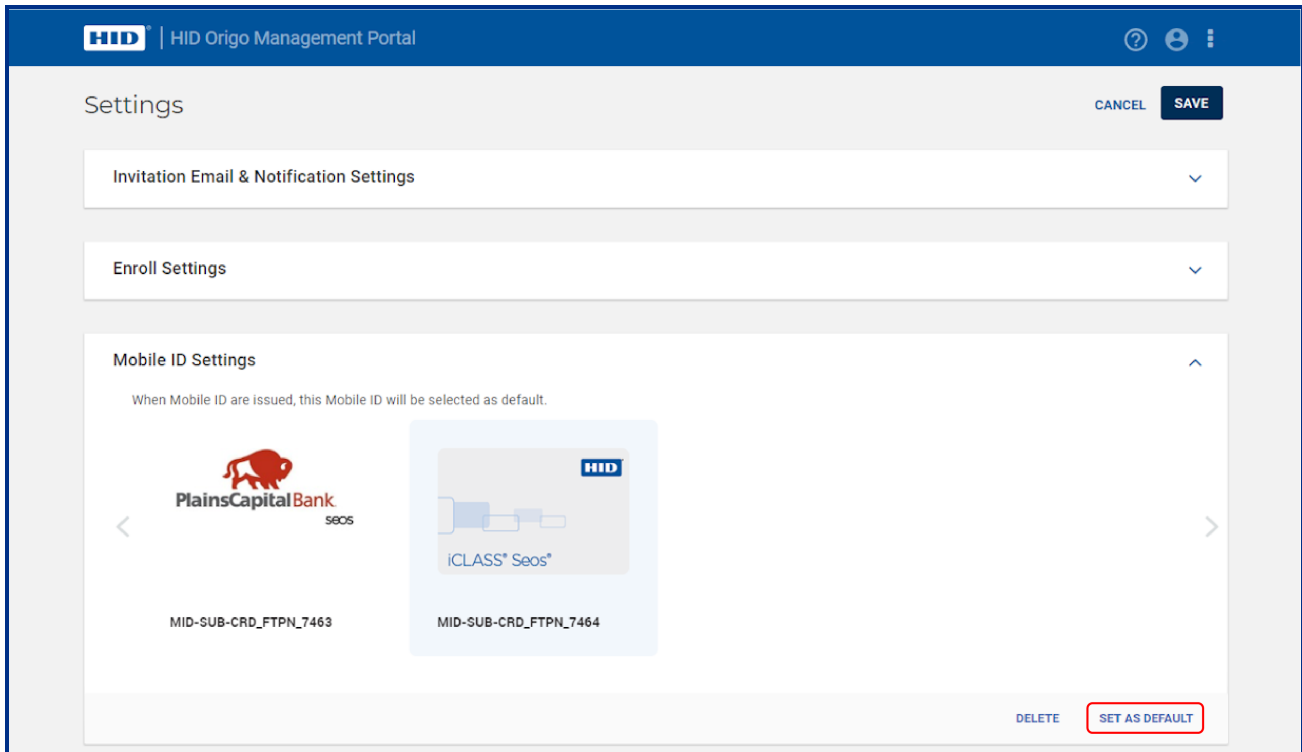


5. In the **Delete Mobile ID** confirmation dialog, review the displayed information and click **DELETE** to carry out the delete action. When the Mobile ID is deleted a success message is displayed.



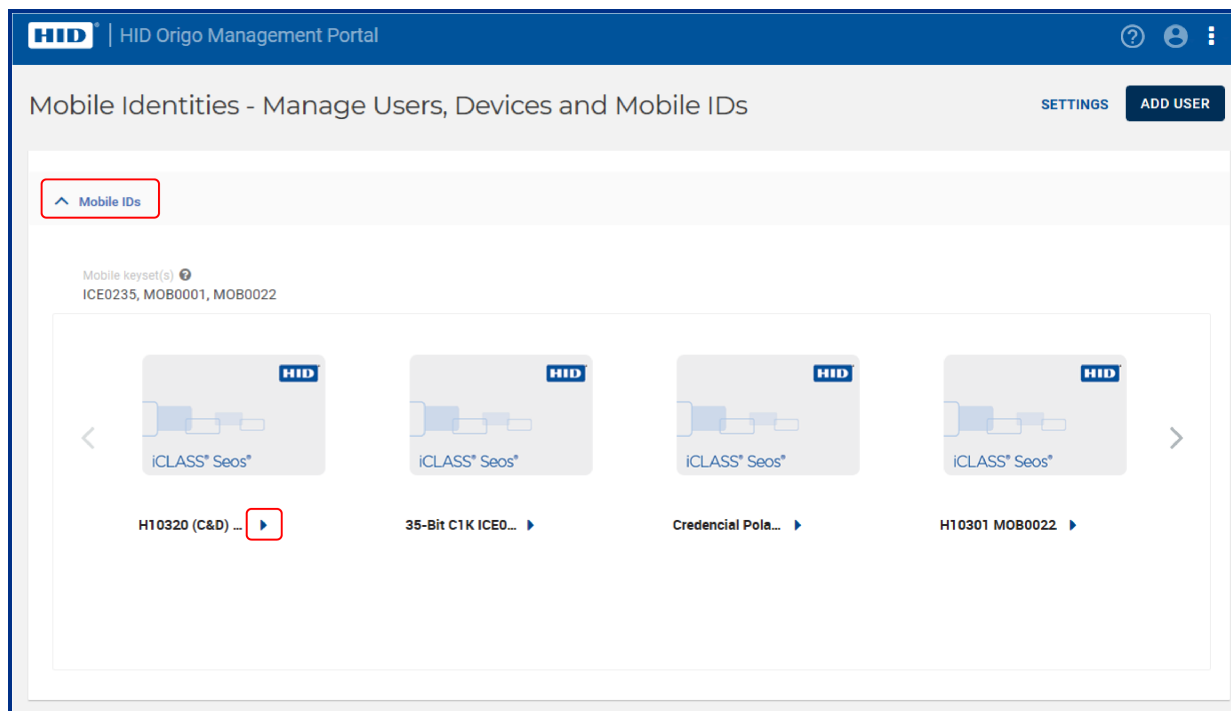
4.25.2 Set a MID type as default

1. Log into the HID Origo Management Portal and on the portal dashboard page select the **Mobile Identities** option.
2. If you are a HID administrator select an Organization and click **Go**. If you are a Mobile Identities administrator you will be automatically directed to the Mobile Identities page for your organization.
3. On the **Mobile Identities** page, select **Settings**.
4. On the **Settings** page, in the **Mobile ID Settings** section, select the appropriate MID type and click **SET AS DEFAULT**.

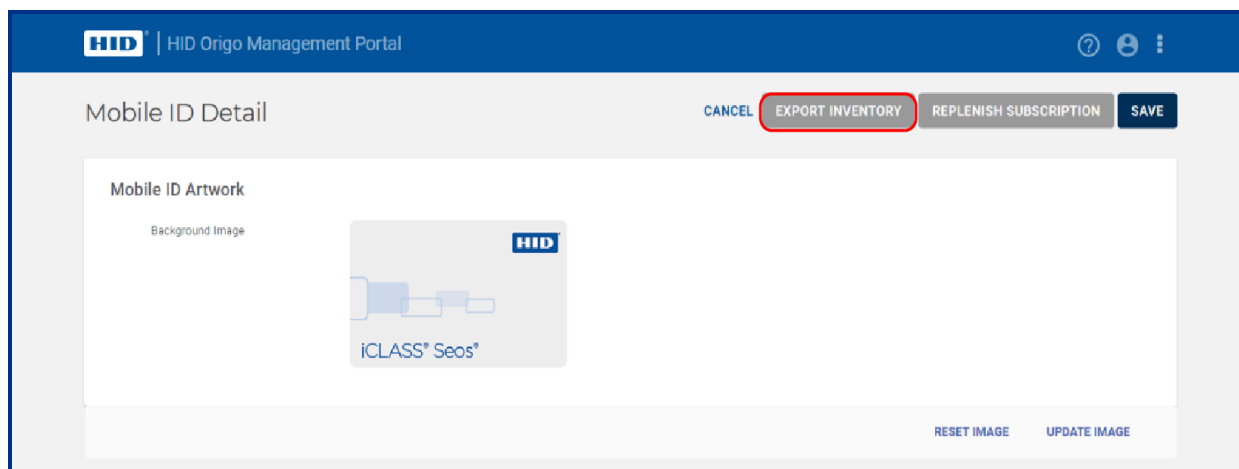


4.25.3 Check for duplicate MIDs and remove duplicates

1. Log into the HID Origo Management Portal and on the portal dashboard page select the **Mobile Identities** option.
2. If you are a HID administrator select an Organization and click **Go**. If you are a Mobile Identities administrator you will be automatically directed to the Mobile Identities page for your organization.
3. On the **Mobile Identities** page, open the **Mobile IDs** option.
4. Click the edit icon [▶] associated with a displayed Mobile ID.



5. On the **Mobile ID Detail** page, click **EXPORT INVENTORY**.



6. The system will display an excel file containing all the available credentials. Check this file to identify any duplicate Mobile IDs.
7. To remove a duplicate MID, navigate back to the **Mobile Identities** page and select the **Edit** icon associated with a specific MID type.

8. In the **Mobile ID Specifications** section, click **REMOVE DUPLICATES**.

Mobile ID Specifications

Mobile ID friendly name	MID-SUB-CRD
Description (Optional)	
HID part number	MID-SUB-CRD
Mobile keyset	MOBA481
Format	TRK-H10301
Facility code	1
Current Inventory	
Quantity	2 available
Next credential value ⓘ	1
Highest credential value ⓘ	2
Latest series added ⓘ	1 - 2 on Apr 12, 2019 08:00:33 UTC
Replenish status ⓘ	Not needed
Reference Value ⓘ	
Display ID on credential ⓘ	<input checked="" type="checkbox"/>
Marking offset ⓘ	0
Prefix (Optional)	
Suffix (Optional)	

REMOVE RANGE REMOVE DUPLICATES

9. In the **Remove Duplicates** confirmation dialog, review the displayed information and click **REMOVE** to carry out the remove action.

Note: You are notified if no duplicates are found.

Remove Duplicates

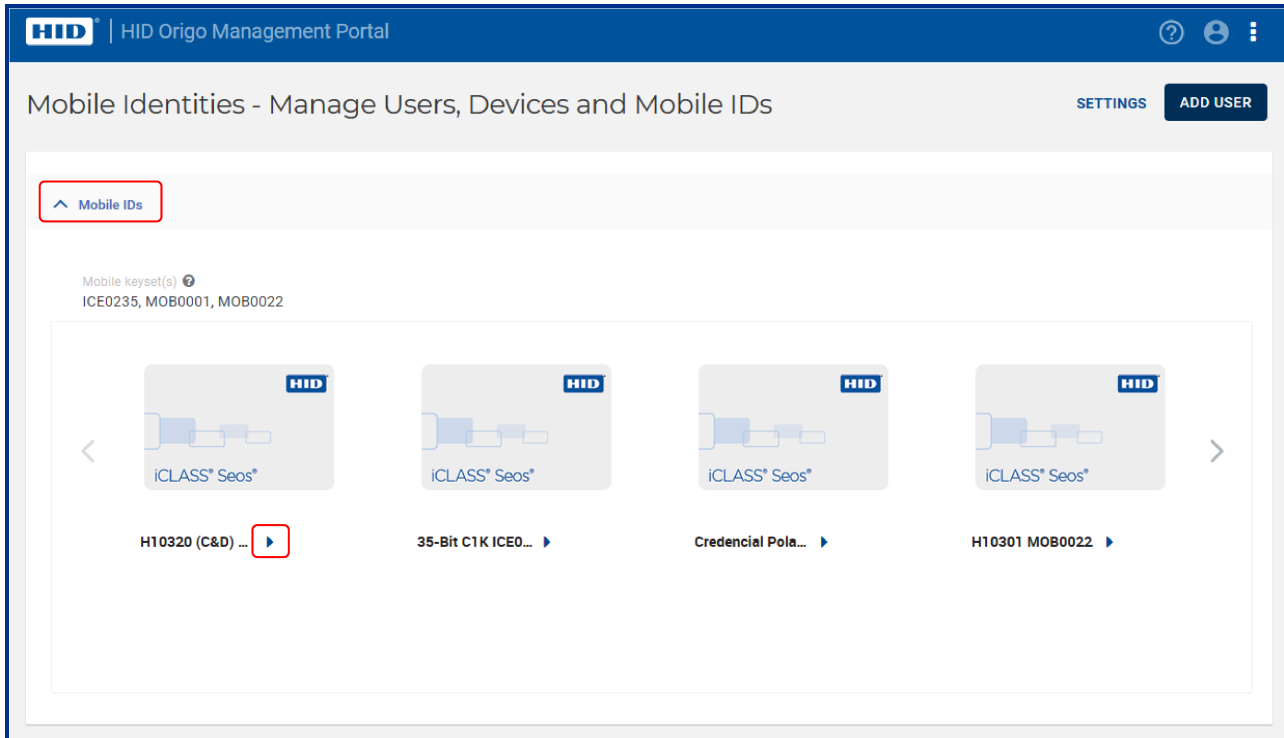
20 duplicates are found among un-issued credentials. Only the duplicates in un-issued credentials will be removed. The already issued credentials will not be effected by this action.

Are you sure you want to remove 20 duplicates?

CANCEL REMOVE

4.25.4 Remove a range of credentials

1. Log into the HID Origo Management Portal and on the portal dashboard page select the **Mobile Identities** option.
2. If you are a HID administrator select an Organization and click **Go**. If you are a Mobile Identities administrator you will be automatically directed to the Mobile Identities page for your organization.
3. On the **Mobile Identities** page, open the **Mobile IDs** option.
4. Click the edit icon [▶] associated with a displayed Mobile ID.



- On the **Mobile ID Detail** page, in the **Mobile ID Specifications** section, click **REMOVE RANGE**.

Mobile ID Specifications

Mobile ID friendly name: MID-SUB-CRD

Description (Optional):

HID part number: MID-SUB-CRD

Mobile keyset: MOBA481

Format: TRK-H10301

Facility code: 1

Current Inventory

Quantity: 2 available

Next credential value: 1

Highest credential value: 2

Latest series added: 1 - 2 on Apr 12, 2019 08:00:33 UTC

Reprint status: Not needed

Reference Value

Display ID on credential:

Marking offset: 0

Prefix (Optional):

Suffix (Optional):

REMOVE RANGE REMOVE DUPLICATES

- In the **Remove Range** dialog enter the range to be removed (**Starting credential** and **Ending credential** values) and click **REMOVE**.
- In the **Remove Range** confirmation dialog, review the displayed information and click **REMOVE** to carry out the remove action.

Remove Range

Please select the range to be removed.

Starting credential: 1

Ending credential: 10

CANCEL REMOVE

Remove Range

You have chosen to remove the credentials in the range 1 to 10. The already issued credentials will not be affected by this action. All associated un-issued credentials in the range will be removed. Once removed, they will no longer be available for issuance.

Are you sure you want to continue?

CANCEL REMOVE

4.26 What should I do if the Mobile Access Portal displays “Delivering Mobile ID” for an extended period?

This usually occurs because the user was not in a good cell area when the ID was being delivered. After a few retries our server will stop re-attempting the delivery operation.

To try and force delivery, **do not issue a new invitation** (as this changes the endpoint ID of the phone and thus the ID will never deliver). Firstly check the mobile device is compatible for use with mobile access, see [HID Mobile Access - Compatible Devices](#).

Next have the user attempt the following:

1. Reboot the phone.
2. Once the phone is back up, make sure it is in a location with good cell service.
3. Open the HID Mobile application and swipe to refresh. A refresh icon will display in the app as it contacts the server.

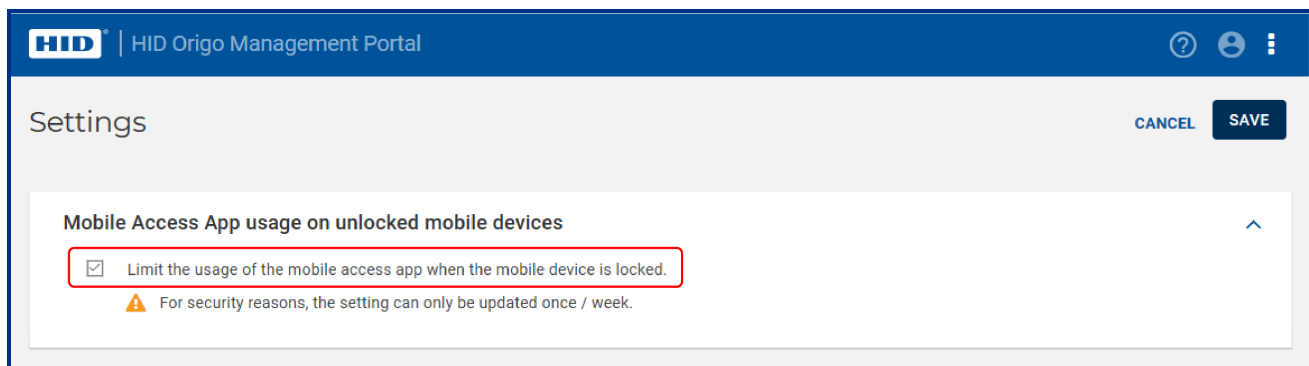
In most cases this will resolve the issue. However, if the symptoms persist, remove the user from the portal and direct the user to remove and reinstall the HID Mobile Access application. In this case a new invitation code will have to be issued to the user.

4.27 How do I enable Enterprise Policy Enforcement?

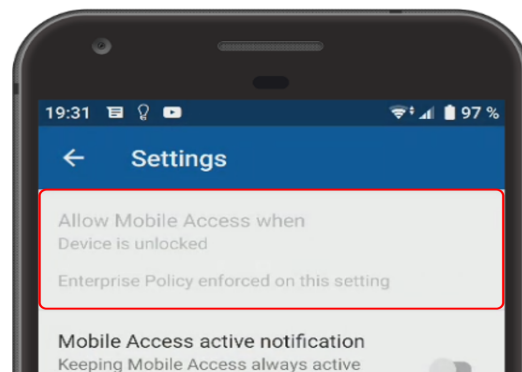
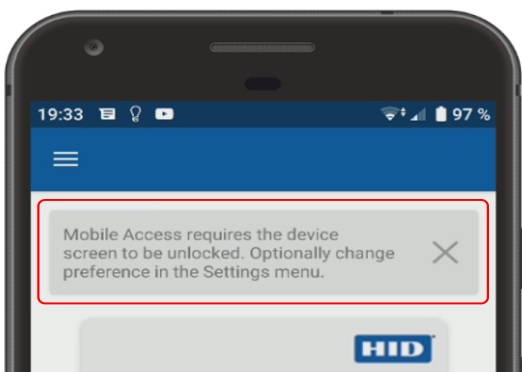
With Enterprise Policy Enforcement you can enforce the requirement that users within the organization have their mobile devices unlocked to open a door. In addition other mechanisms, such as ActiveSync, can then be used to enforce other security measures, for example, devices should be automatically locked with a password.

To enable Enterprise Policy Enforcement in HID Origo Mobile Identities:

1. Log into the HID Origo Management Portal and on the portal dashboard page select **Mobile Identities**.
2. If you are a HID administrator select an Organization and click **Go**. If you are a Mobile Identities administrator you will be automatically directed to the Mobile Identities page for your organization.
3. On the **Mobile Identities** page, select **Settings**.
4. On the **Settings** page, select the **Limit the usage of the mobile access app when the mobile device is locked** option.



In the Mobile Access app the user will be informed that an Enterprise Policy has been enabled and the app setting **Allow Mobile Access** when will be set to **Device is unlocked** and disabled.



The following are some common questions and answers relating to the Enterprise Policy Enforcement feature.

Question	Answer
Does it cost any extra to get access to the Enterprise Policy Enforcement feature?	No, Enterprise Policy Enforcement has been added as a feature in the standard subscription offering for HID Origo Mobile Identities.
Why can this setting only be changed once per week?	The setting triggers an update of all credentials in your system. This may cause a high load on the platform should customers frequently toggle the Enterprise Policy Enforcement feature on and off.
Will the Enterprise Policy also be enforced on Technology Partner apps?	The Enterprise Policy will be enforced on all apps based on the HID Origo SDK, including the HID Mobile Access app.
What happens if the user has two credentials, one from an organization where Enterprise Policy Enforcement has been activated, and one where it has not?	As soon as any of the credentials in the app are issued from an organization that has the Enterprise Policy Enforcement feature enabled, the setting Allow Mobile Access when will be set to Device is unlocked and disabled.
How long does it take before the policy has been enforced on all devices?	It may take up to 24 hours, but usually within one hour.
What if the user has not activated a password protection on the Mobile Device?	Then it will be regarded as an unlocked device, and the Mobile IDs will be activated even with screen unlit.
What happens if a user has a stricter setting for Allow Mobile Access when than Device is unlocked , for example, if the user has the setting App is in foreground ?	The user will keep the stricter setting.

4.28 How are MIDs replenished?

- As a new end customer, the portal is supplied with several credentials for each credential type. This is 2 x the number of user licenses.
- An automatic replenishment is triggered when the number of credentials falls below 1.25 x the number of user licenses.
- The number of auto-replenished credentials is 0.75 x the number of user licenses, but always at least 500 credentials.

4.29 How do I activate auto-replenishment?

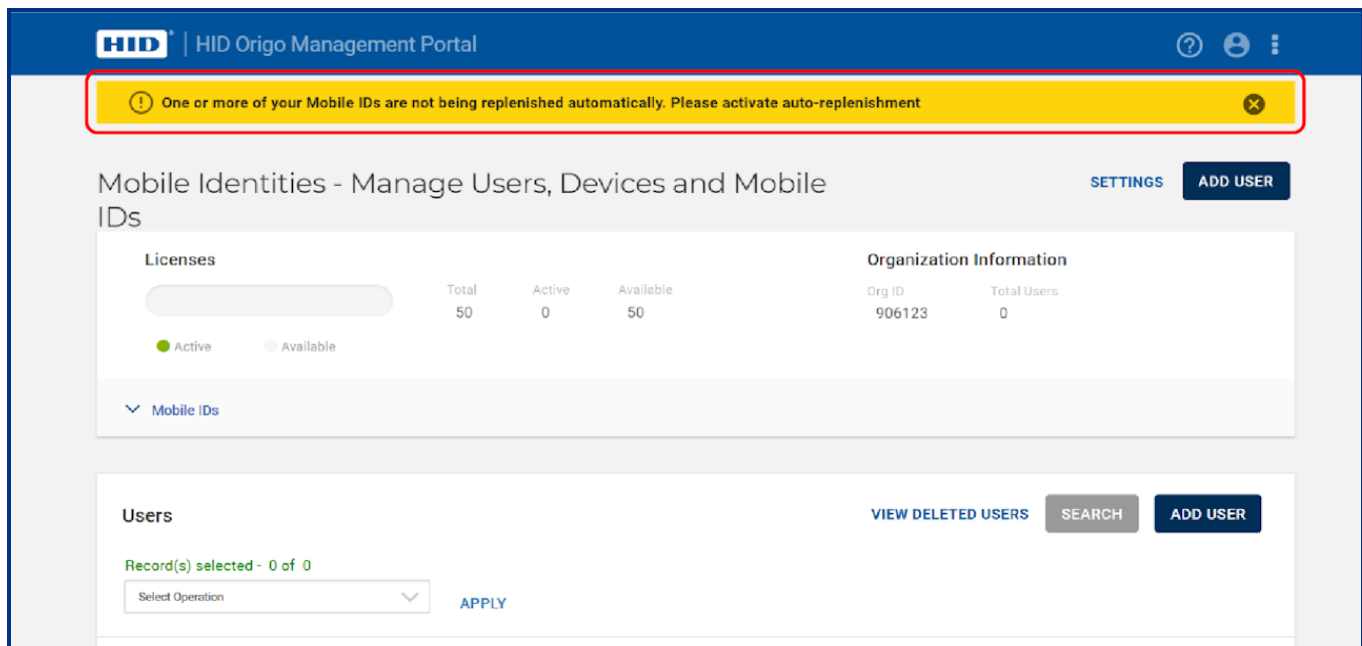
As a result of the discontinuation of the Mobile Access part of the HID Security Identity Services (SIS) Portal, HID Global is migrating Mobile Access customers, that have an existing account on the SIS Portal, to the HID Origo Cloud Platform and Management Portal.

The migration is completely automatic, and once completed, customers will be redirected to the new HID Origo Management Portal at their next login.

As part of the migration process:

- All users and digital credentials will be moved over to the new portal and become available for administration in HID Origo without any required actions.
- Credential holders will not be impacted by the transition to HID Origo and all issued credentials will continue to work as usual.
- Organizations using Open formats for their credentials will need to manually activate auto-replenishment after the migration has been completed.

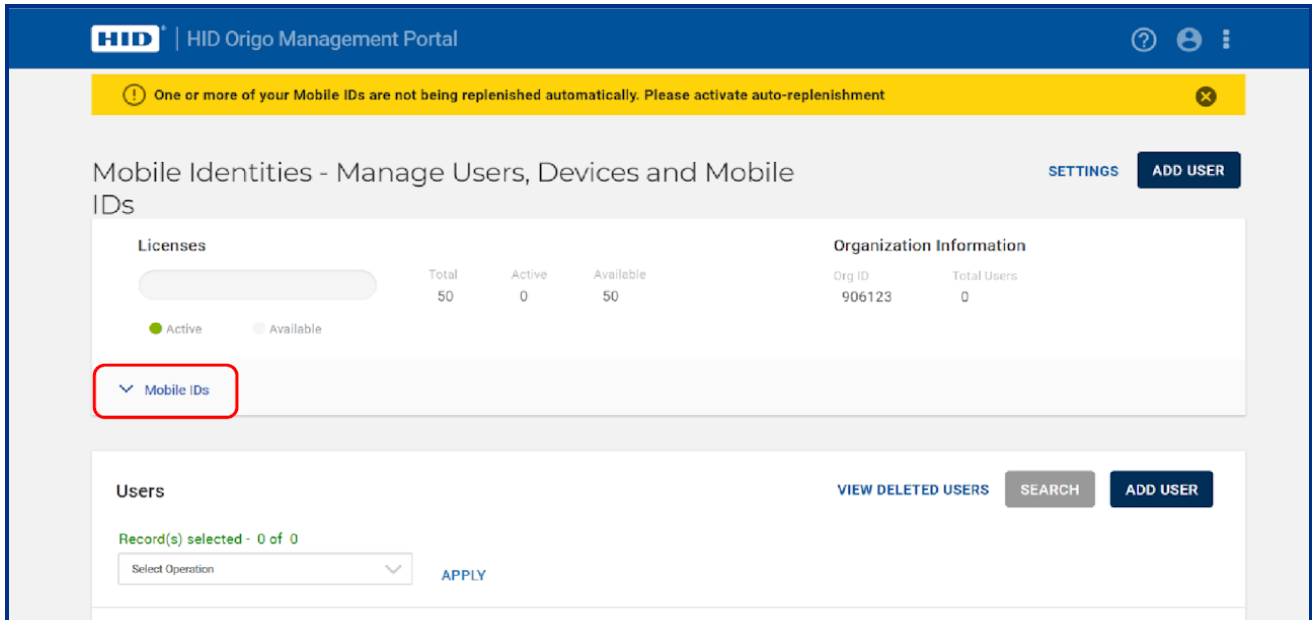
In the cases where auto-replenishment has been inactivated by HID Global, to avoid creating duplicated credential numbers, the Organization will see a notification bar displayed in the HID Origo Management Portal stating that auto-replenishment needs to be activated.



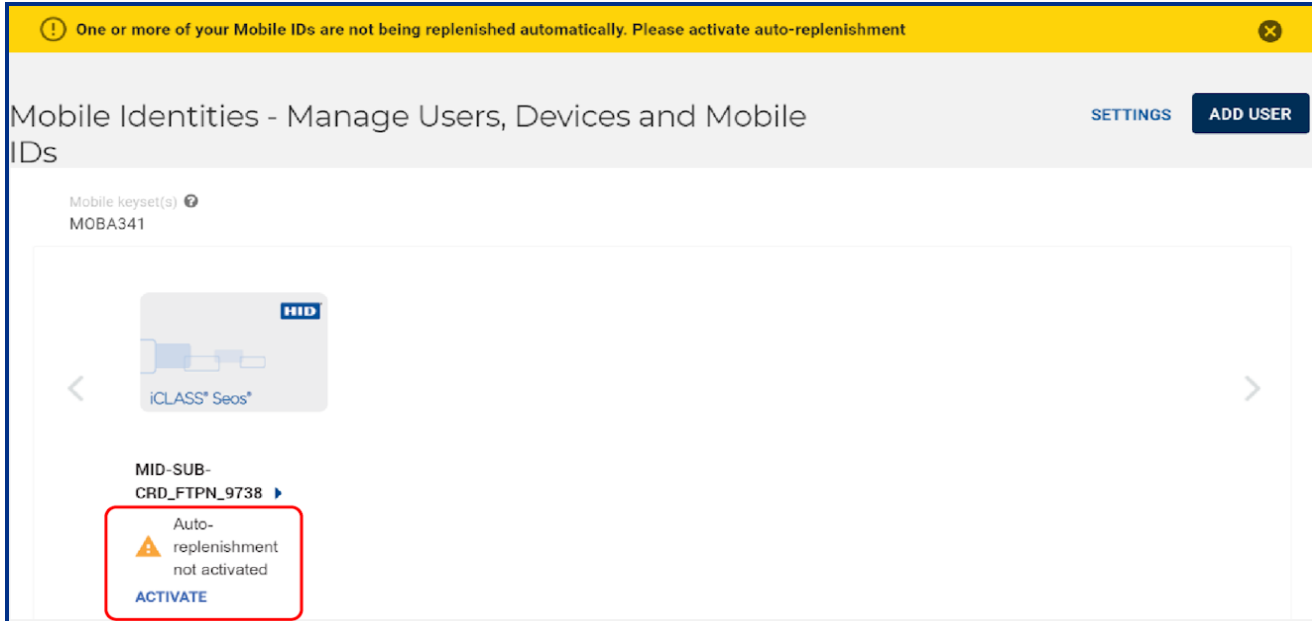
4.29.1 Activate auto-replenishment

To activate auto-replenishment for Mobile IDs:

1. On the **Mobile Identities – Manage Users, Devices and Mobile IDs** page, click **Mobile IDs**.



2. Under the displayed Mobile ID and the message, **Auto-replenishment not activated**, click **ACTIVATE**.



3. In the activation dialog, enter the highest credential value from where the replenishment should start. This credential start value should be higher than the last number used for Mobile IDs and physical credentials to avoid overlapping numbers.

Note: If a notification message is displayed (as shown below), then on the **Mobile ID Detail** page, under **Mobile ID Specifications**, selected number ranges and duplicates can be removed without affecting the license count.

- Click **ACTIVATE** to start the auto-replenishment.

A credential start number is required to activate auto replenishment. To avoid the risk of overlapping numbers, the credential start number should be higher than the last number used in mobile and physical credentials.

Current Inventory	
Quantity	20 Available
Next credential value	1
Highest mobile credential value	
Latest series added	1 - 20 on Apr 21, 2020 14:54:25 UTC
Replenish status	Not Needed

Start credential value from

CANCEL ACTIVATE

4.30 What subscription contract renewal notifications are communicated?

Subscription contract renewal notifications are delivered to the following:

- **Channel Partner (Contact Manager):** notifications start 90 days before the renewal date:
 - Automatic renewal: monthly notifications
 - Manual renewal: monthly notifications
- **End Customer and HID Renewal Team:** notifications start 60 days before the renewal date:
 - Automatic renewal: monthly notifications
 - Manual renewal: weekly notifications

4.31 What happens if my subscription contract is on manual renewal and I don't place a renewal order before my subscription expires?

Your service will at first be limited so that you can no longer add users or issue new mobile IDs, although your already issued mobile IDs will continue to be active. This will last for a maximum of 30 days, after which your service will become **Suspended**, which means that all your mobile IDs will be temporarily disabled and can no longer be used to open doors.

Within 60 days, your service will be **Terminated**, which means that all mobile IDs are permanently revoked and all information about your account, including information about users and their devices, is deleted.

Note: There may be slight deviations from the above quoted timelines while pending activation of the next service state.

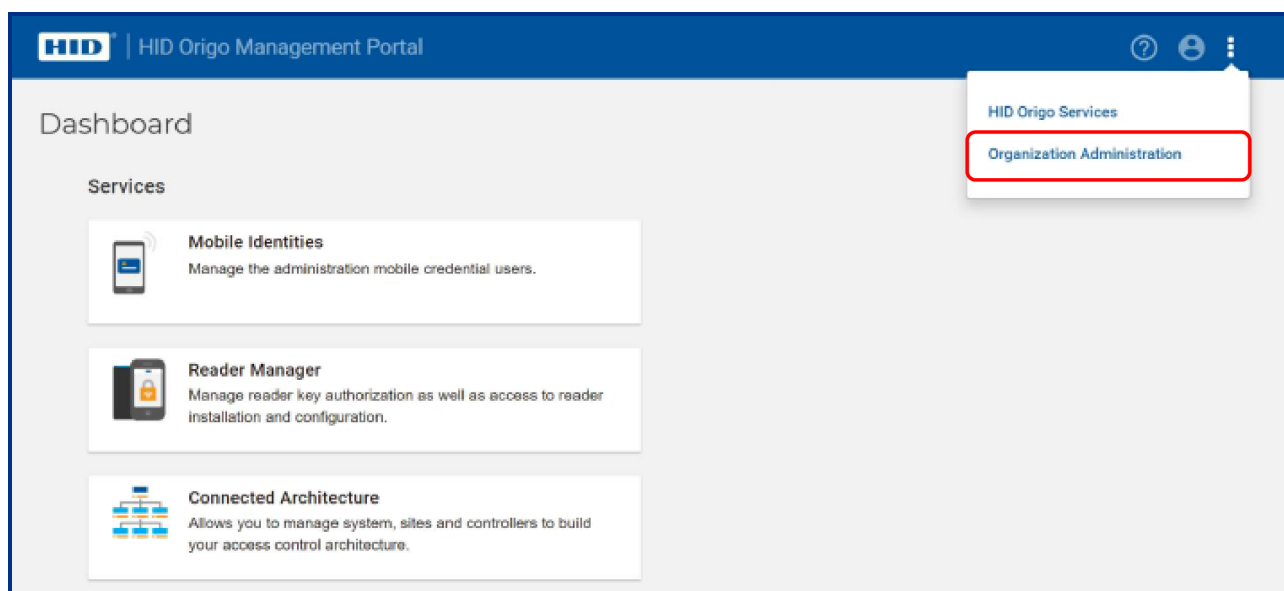
4.32 How do I activate Delegated Authorization functionality?

To address managed service scenarios, Delegated Authorization functionality in the HID® Origo™ Management Portal allows organizations to establish trust relationships with other organizations.

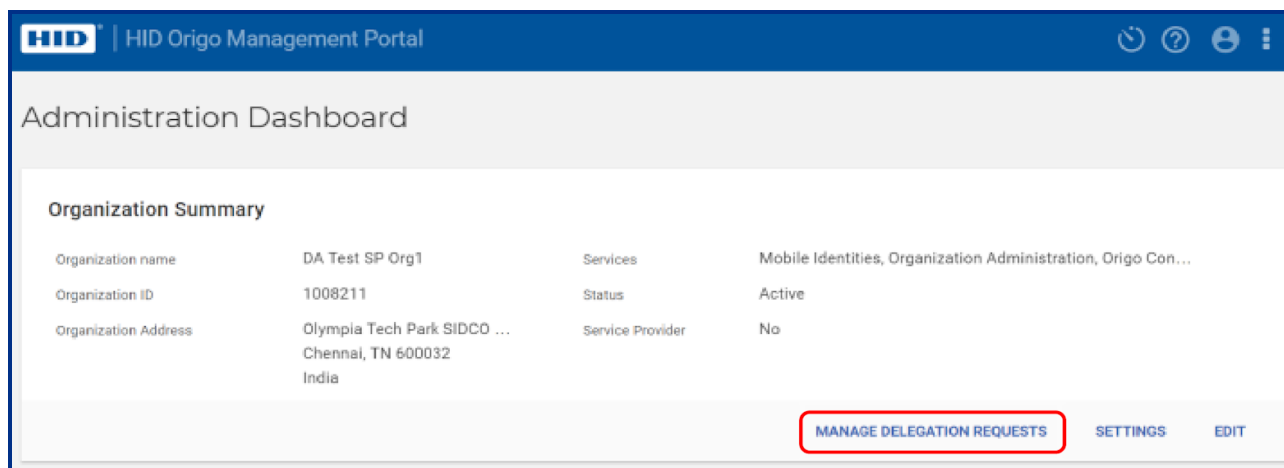
When an organization has been enabled as a Service Provider, other organizations (trusting organizations) can establish a trust relationship with Service Provider organization (trusted organization) through the creation and approval of Delegation Requests. Once a Delegation Request has been approved the Service Provider can perform administration actions on behalf of the trusting organization.

4.32.1 Approve a Delegation Request

1. Log into the HID Origo Management Portal as a **Trusted** organization admin (Service Provider organization admin).
2. On the **Dashboard**, click the options icon [⋮] and select **Organization Administration**.

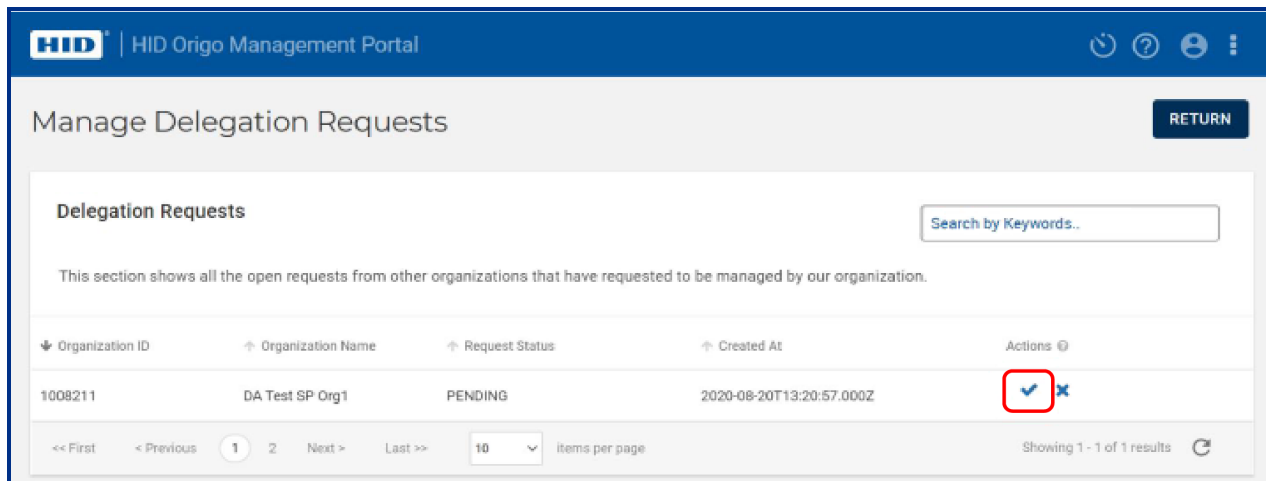


3. On the **Administration Dashboard**, click **MANAGE DELEGATION REQUESTS**.

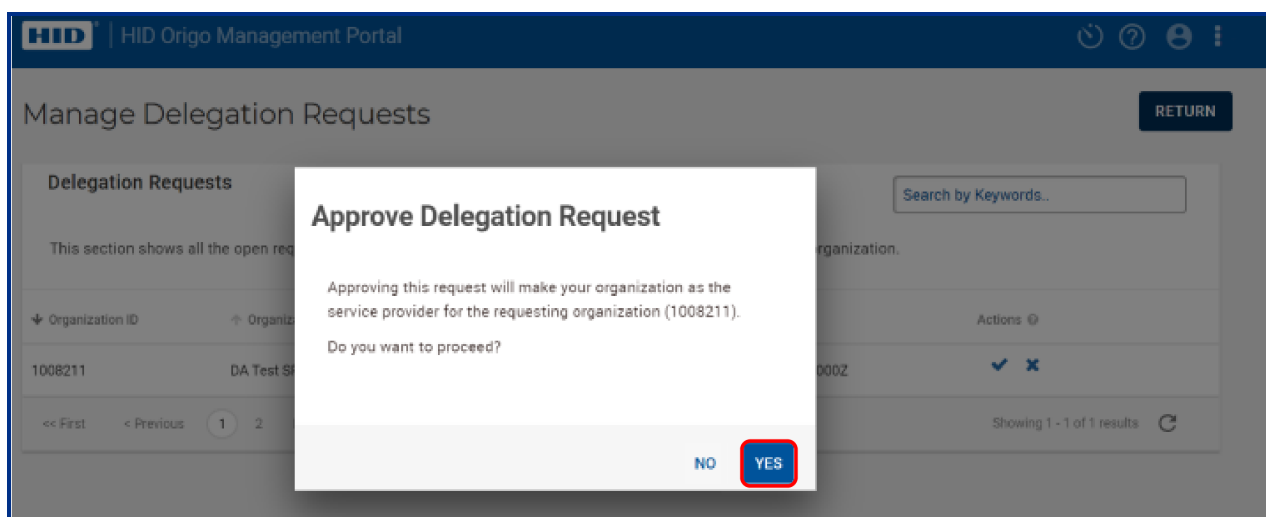


- 4. In the **Delegated Requests** table, click the approve icon [✓] associated with an organization.

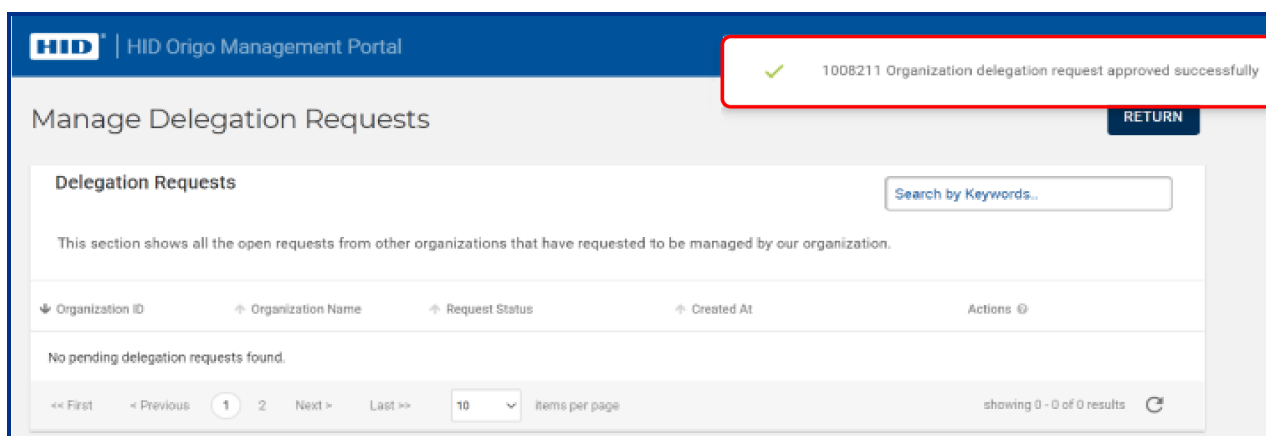
Note: To reject the request click on the reject icon [✗].



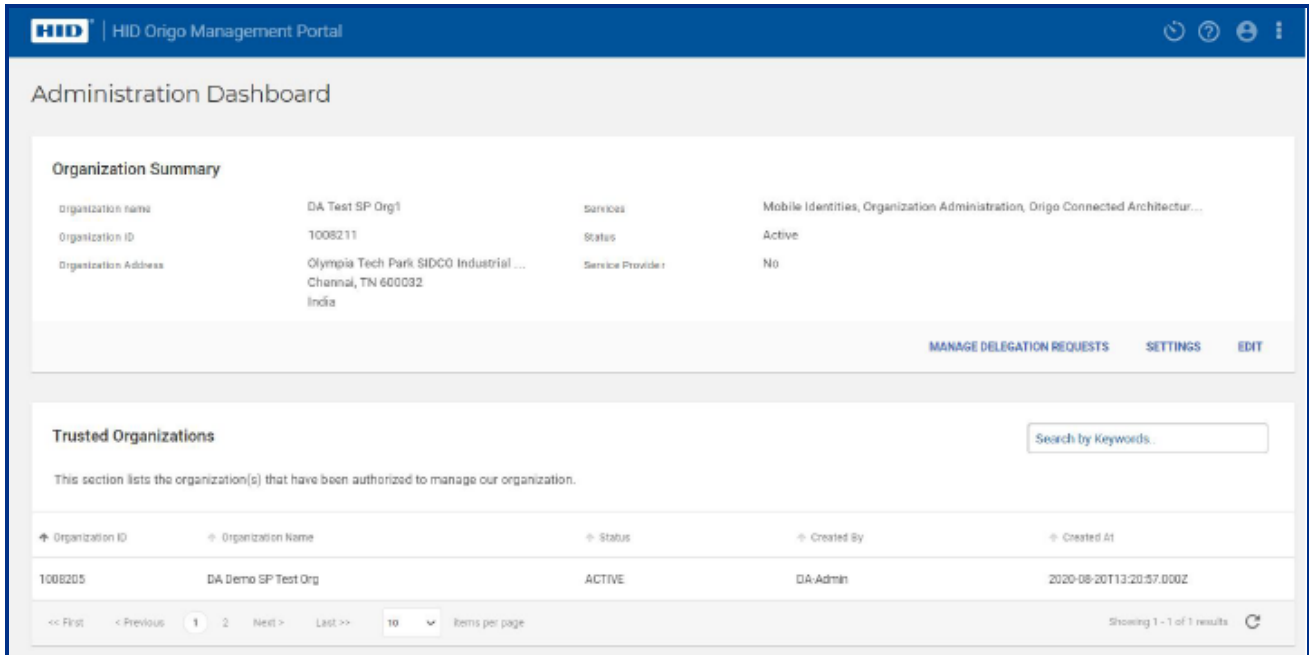
- 5. In the **Approve Delegation Request** dialog, click **Yes**.



- 6. A notification message is displayed to state that the Delegation Request was successfully approved.

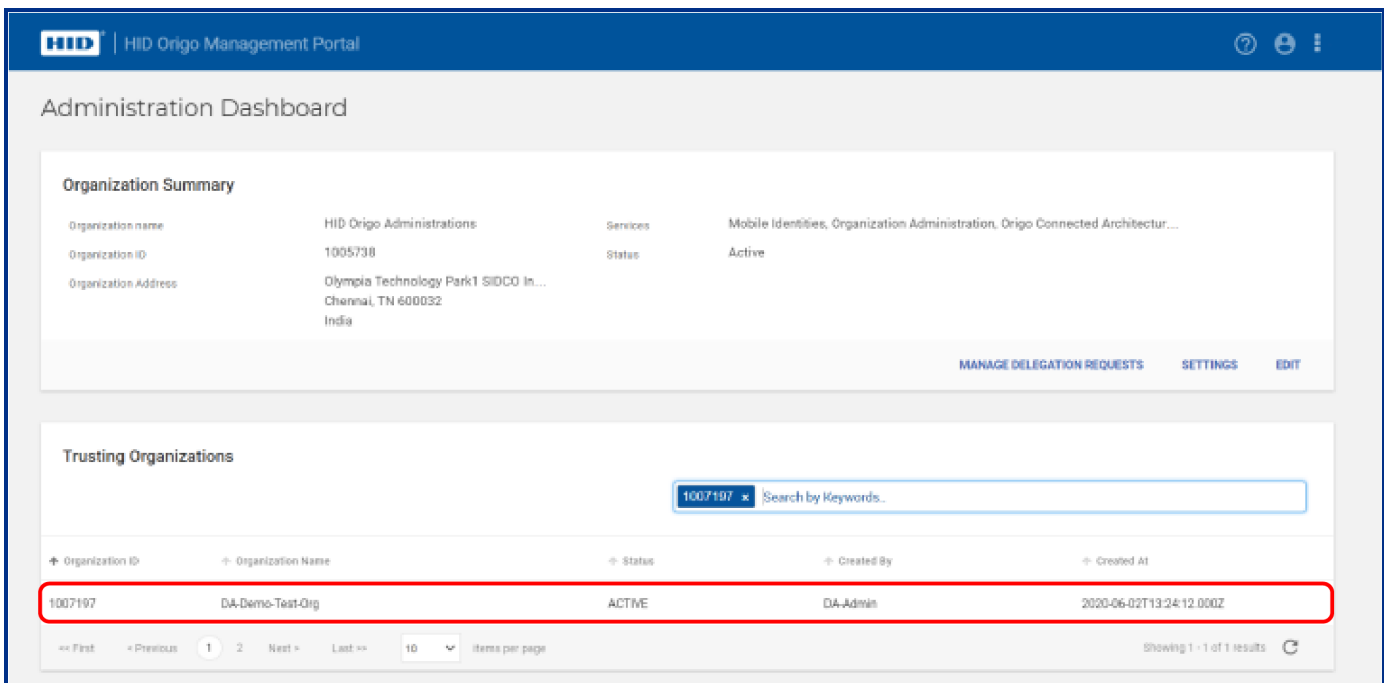


- To view the list of trusted organizations, on the **Dashboard**, click the options icon [H] and select **Organization Administration**.
- On the **Administration Dashboard**, the trusted organizations that have been authorized to manage the organization are listed in the **Trusted Organizations** section.



4.32.2 Perform Organization administration actions

Once the organization trust relationship is established, the trusted organization admin is able to perform all of the admin actions for the trusting organization by clicking the organization entry listed in the **Trusting Organizations** section.



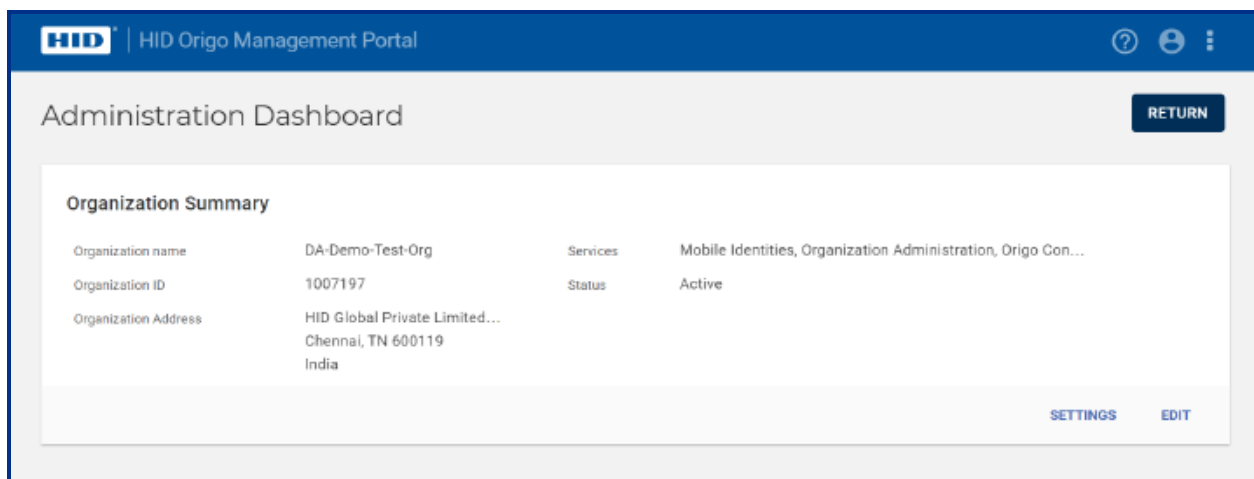
On the trusting organization **Administration Dashboard**, the trusted organization admin can perform admin actions for the trusting organization, for example:

- Edit trusting organization details.
- Settings: Enable Single Sign-On.
- Edit Shipping Address.

Note: Before editing the shipping address, make sure that the Mobile Keypad is present.

- Add/Edit/Delete Admin User.
- Add/Edit/Delete System Account.

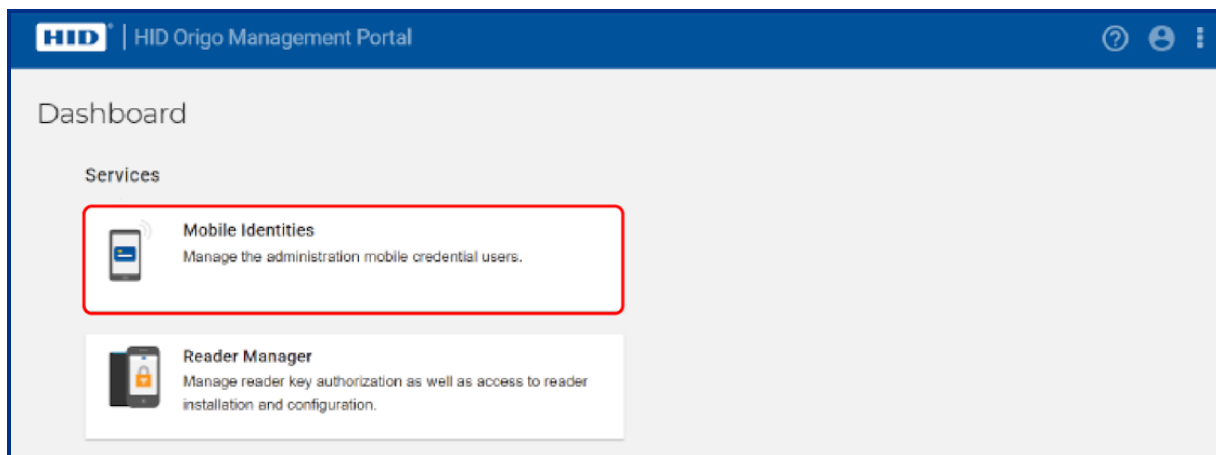
Note: To add a System Account, an organization should contain at least one org admin user, then only the System Account section will be visible.



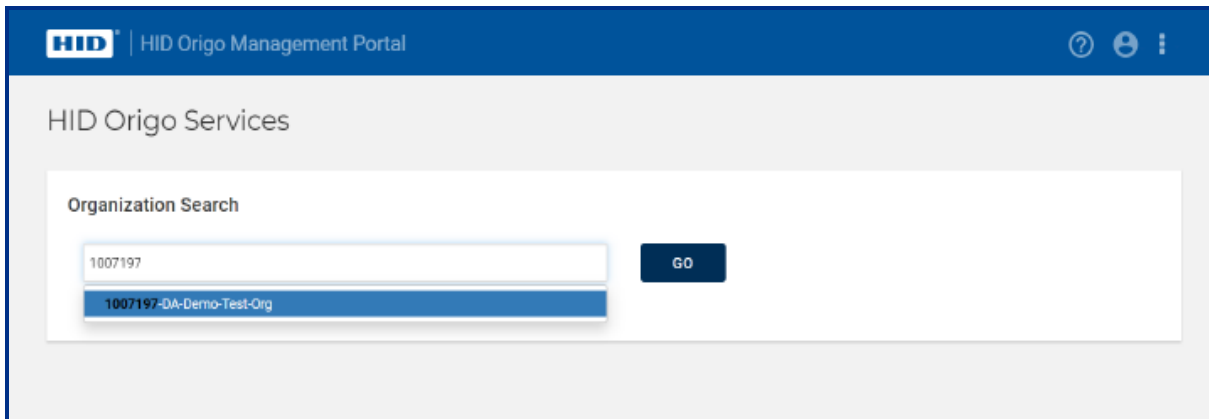
4.32.3 Perform Mobile Identities actions

Once the organization trust relationship established, the trusted organization admin is able to perform Mobile Identities actions.

1. Log into HID Origo Management Portal as a trusted organization admin and select **Mobile Identities**.

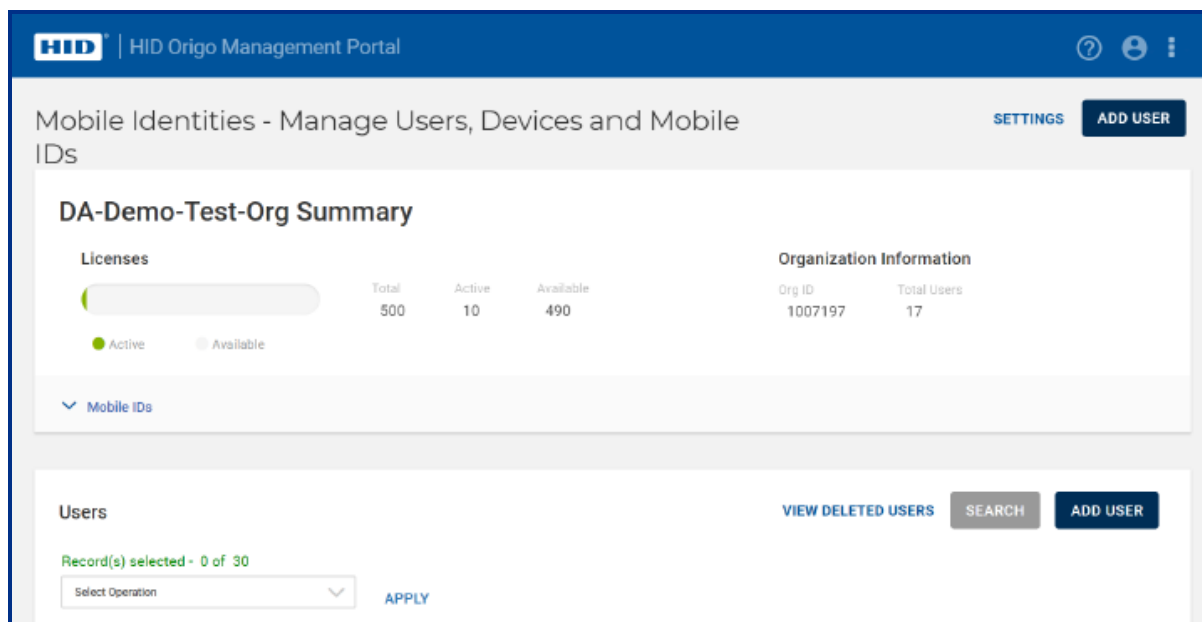


2. In **Organization Search** section, search for the trusting organization and click **GO**.



3. On the **Mobile Identities - Manage Users, Devices and Mobile IDs** screen, the trusted organization admin can perform Mobile Identities related actions such as:

- Add Mobile User, both Auto Assign User and Plain User Enrollment:
 - Send Invitation
 - Issue Mobile ID
 - Revoke Mobile ID
 - Delete Device
- Edit User
- Delete User
- View Deleted Users
- Search User
- Edit Mobile ID
- Configure settings



4.32.4 Delegated Authorization limitations

The following section provides details on Delegated Authorization limitations:

- If the Service Provider contains at least one Trusting Organization, then the organization cannot be disabled as Service Provider.
- The ability to cancel the trust relationship between the Service Provider and Trusting Organization is currently not available. IT Support must be contacted for manual intervention.
- If an organization contains both the Trusting and Trusted roles, then that organization can perform Trusted Organization responsibilities. However, there is a limitation in building complex multiple layer Service Provider relationships. Once a Service Provider has started to manage other organizations, they cannot submit a request to be managed by another Service Provider.
- If a HID Admin logs into the HID Origo Management Portal, then they can view the Trusted and Trusting Organization table only in read mode. In addition, they will not be able to view the **Manage Delegation Requests** screen.
- When a Trusting Organization is created via the DA API and the Trusted Organization admin navigates to Trusting Organization's administration dashboard, the System Account section will not be visible. Once the admin user is created for the Trusting Organization, the System Account section will be visible.
- If the Trusted Organization Admin navigates to the Trusting Organization via the Trusting Organization table, the **Manage Delegation Requests** option and Trusted Organization table will not be visible. In addition the **Service Provider** field in the **Organization Summary** section for the Trusting Organization will not be visible.
- When editing an organization's shipping address make sure that the Mobile Keypad is available.
- On the **Manage Delegation Requests** screen, once a request to be managed is submitted, it cannot be withdrawn. Although a **Delete** option is visible, it is currently disabled. For a work around for this, the Service Provider organization can reject the request.

Note: The availability of the **Delete** option is planned to be enabled in a future release.

4.33 What role does a Service Provider have for Delegated Authorization?

When you delegate authorization to a Service Provider for your organization, the Service Provider will have the same role within your organization as is assigned for the Service Provider in the Service Provider's organization.

4.34 Certificate-based Authentication

Certificate-based authentication is supported by using [JSON Web Token \(JWT\)](#).

4.34.1 Prerequisites

The System Account identifier and a token URL are used as input to the signed token. The following instructions provide guidance on how to configure a System Account for PKI authentication and to capture the properties to be included in the token.

1. Log into the HID Origo Management Portal and on the **Dashboard**, click the options icon [⋮]. Select **Organization Administration** from the drop-down menu.
2. In the **System Accounts** section click **ADD SYSTEM ACCOUNT** or edit [✎] an existing account.
3. In the **System Information** section select the roles to be assigned to this system account user and upload the **PKI certificate** (public key).
4. Click **SAVE** to return to the return to the **Organization Administration** screen.

HID | HID Origo Management Portal

Add System Account CANCEL **SAVE**

System Information

Please create a system account below to access the HID Origo Mobile Identities portal via SDK.

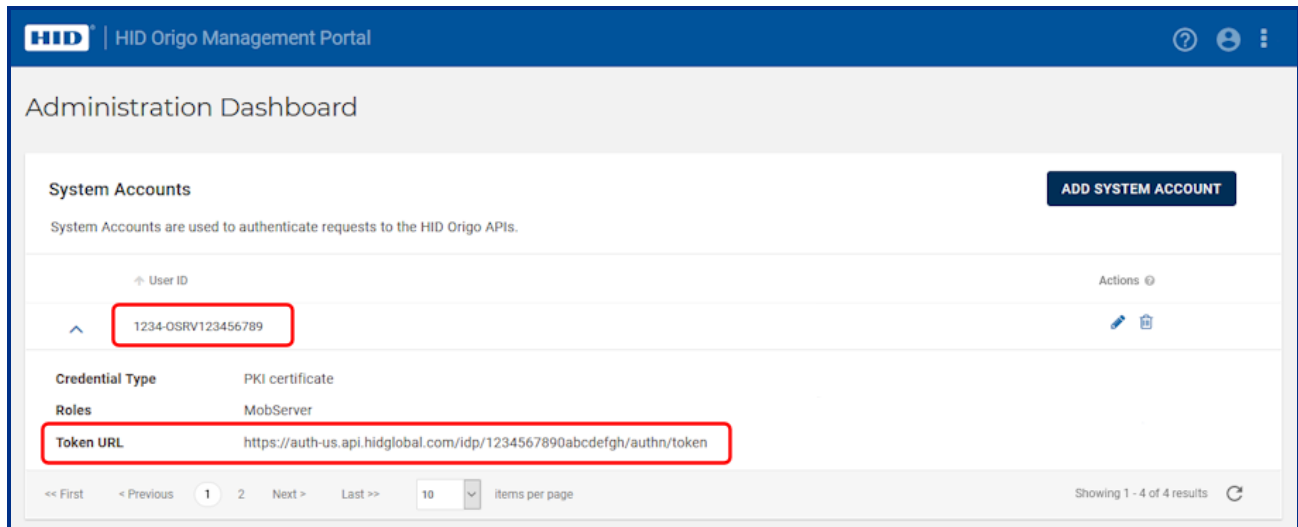
Client ID 1234-OSRV123456789

Service	Active
Mobile Identities	<input checked="" type="checkbox"/>
Connected Architecture	<input type="checkbox"/>
Connected Architecture: Certificate Manager	<input type="checkbox"/>

Credential type PKI credential (Recommended for better security) Password

PKI certificate

5. In the **System Accounts** section, obtain the Client ID and Token URL.



4.34.2 Base64 encoding

HID Origo expects that any file(s) uploaded only contain a single X.509 certificate encoded in Base64 format.

Section **05**

HID Mobile Identities Subscriptions

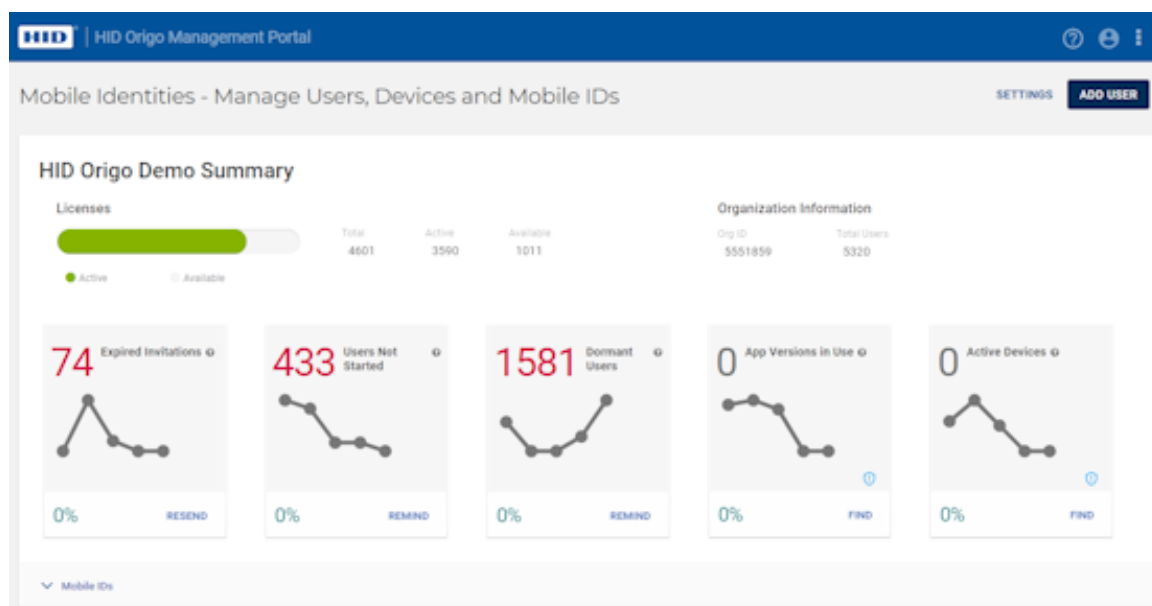
5.1 What Mobile Access Subscription contracts are available?

HID Origo Mobile identities is a Software as a Service (SaaS) model where you purchase subscription user licenses. This means that you are only charged for the user that uses mobile access, regardless of whether you get only one or many credentials. Currently there are two types of contract for purchasing subscription user licenses:

- Pre-paid subscription user licenses
- Activation based subscription user licenses

5.1.1 Pre-paid subscription user licenses

You purchase a set of subscription user licenses which is then consumed as you activate users. You will see the inventory and the usage displayed in the portal.



Your subscription contract will automatically be renewed at the end of the term. For pre-paid subscription user licenses there are two period terms, each with two tiers:

- One year contracts:
 - **MID-SUB-T050** (Essentials)
 - **MID-SUB-T100** (Enterprise)
- Three year contracts:
 - **MID-SUB-T053** (Essentials)
 - **MID-SUB-T103** (Enterprise)

5.1.2 Activation based subscription user licenses

If you purchase activation-based subscription user licenses, you will be charged in-arrears for the number of active users in a month. There are two types of activation-based subscriptions:

- **MID-ACT-T100:** App enabled activation-based subscription using the HID App (charged monthly).
- **MID-ACT-T200:** Wallet enabled activation-based subscription (charged monthly).

There is also, **FEE-AAPL-01**, a fee that gets added if you are using Apple wallet (yearly fee, charged monthly).

5.2 How do I change my Subscription model?

5.2.1 Activation based subscription to a pre-paid subscription model

Simply place an order for a pre-paid subscription. The new subscription model will take effect after the end of the term (end of month).

5.2.2 Pre-paid to an activation based subscription model

When the contract for the activation based subscription is placed, the portal displays the following notification:

You have conflicting contract(s) your oldest contract will take precedence, please review your active subscriptions in the administration dashboard

Your new contract will be available as soon as the existing contract expires or is terminated.

5.2.3 Upgrade an existing pre-paid subscription

If you wish to upgrade a pre-paid subscription from a MID-SUB-T050 to a MID-SUB-T100, then place an order for MID-SUB-T100-UPG, and you will be transitioned to the higher tier.

If you wish to upgrade a pre-paid subscription from a MID-SUB-T053 to a MID-SUB-T103, then place an order for MID-SUB-T103-UPG, and you will be transitioned to the higher

5.2.4 Multiple channel partners

If you have multiple channel partners and wish to upgrade, you can place an order with multiple or one channel partner for a MID-SUB-T10x-UPG. If the order is placed for only one channel partner, the portal displays the following notification:

You have conflicting contract(s) your oldest contract will take precedence, please review your active subscriptions in the administration dashboard

You need to reach out to your channel partner to terminate the existing contract or upgrade this contract as well.

5.3 What subscription contract renewal notifications are communicated?

Subscription contract renewal notifications are delivered to the following:

- **Channel Partner (Contact Manager):** notifications start 90 days before the renewal date:
 - Automatic renewal: monthly notifications
 - Manual renewal: monthly notifications
- **End Customer and HID Renewal Team:** notifications start 60 days before the renewal date:
 - Automatic renewal: monthly notifications
 - Manual renewal: weekly notifications

5.4 What happens if my subscription contract is on manual renewal and I don't place a renewal order before my subscription expires?

Your service will at first be limited so that you can no longer add users or issue new mobile IDs, although your already issued mobile IDs will continue to be active. This will last for a maximum of 30 days, after which your service will become **Suspended**, which means that all your mobile IDs will be temporarily disabled and can no longer be used to open doors.

Within 60 days, your service will be **Terminated**, which means that all mobile IDs are permanently revoked and all information about your account, including information about users and their devices, is deleted.

Note: There may be slight deviations from the above quoted timelines while pending activation of the next service state.

Section 06

HID Mobile IDs



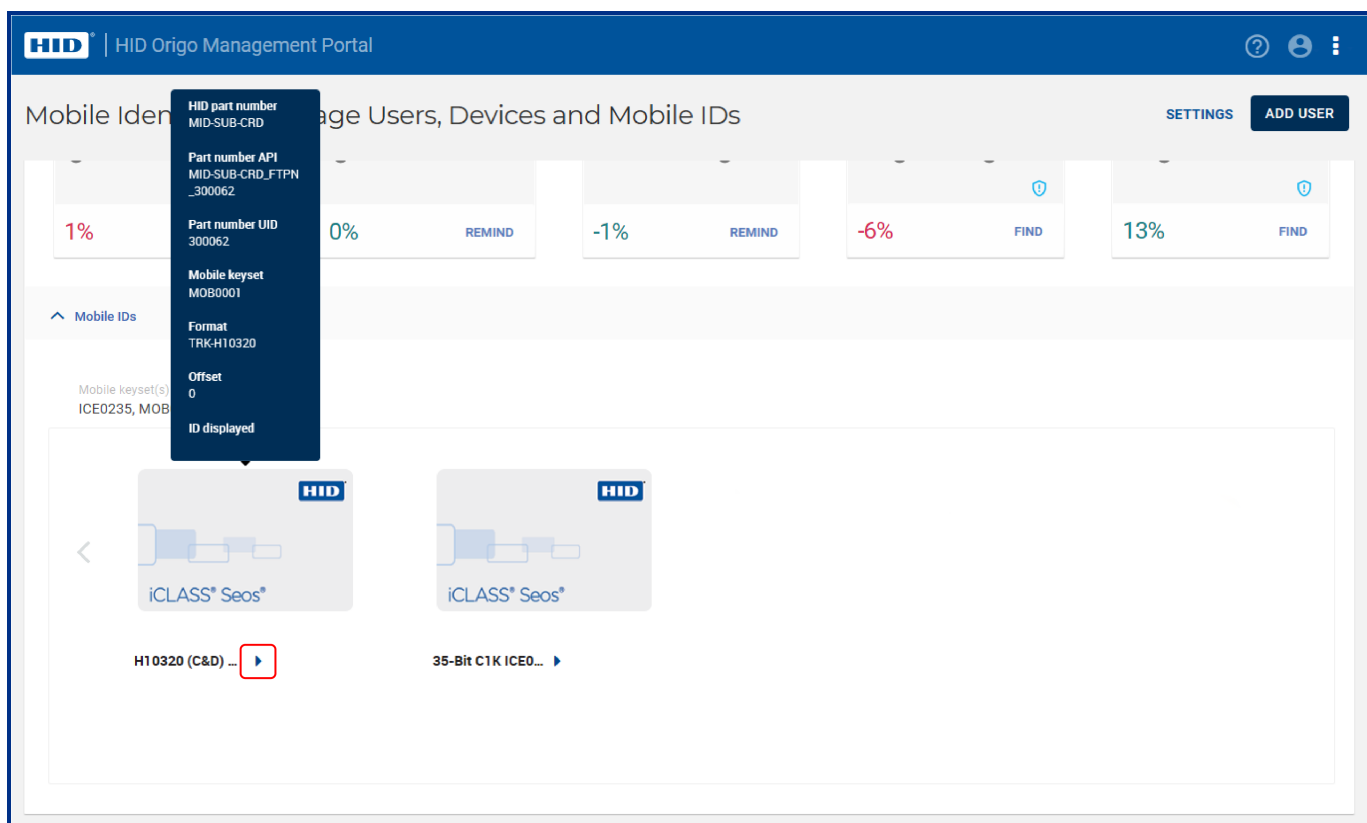
6.1 What are Mobile IDs?

Mobile IDs are the virtual credentials that are stored on the mobile device and issued or revoked via the HID Mobile Access® portal. Mobile IDs are not included in device backups. If a user switches devices or uninstalls the application, a new Mobile ID must be issued.

6.2 How can I buy additional Mobile IDs?

To purchase additional Mobile IDs, contact your access control integrator or the vendor where you purchased HID Mobile Access.

Look up the HID part number to speed up the process. The HID part number can be obtained in the portal by hovering over the corporate badge on the main screen or by clicking the [▶] icon below the badge to access the Mobile ID Specification information.



HID | HID Origo Management Portal

 ?

Mobile ID Detail

CANCEL
EXPORT INVENTORY
SAVE

Mobile ID Specifications

Mobile ID friendly name	H10320 (C&D) MOB0001
Description <i>(Optional)</i>	H10320 (ABA CLK & DATA) MOB0001 FORMAT TRK-H10320
HID part number	MID-SUB-CRD
Mobile keyset	MOB0001
Format	TRK-H10320

Current Inventory

Quantity	6075 available
Next credential value ⓘ	202
Highest credential value ⓘ	5162
Latest series added ⓘ	2704 - 5203 on Oct 09, 2019 05:36:03 UTC
Replenish status ⓘ	Not Needed

Reference Value ⓘ

Display ID on credential ⓘ	<input checked="" type="checkbox"/>
Marking offset ⓘ	0
Prefix <i>(Optional)</i>	CN
Suffix <i>(Optional)</i>	

REMOVE RANGE
REMOVE DUPLICATES

6.3 Is a Mobile ID more secure than a physical card credential?

A Mobile ID is more secure if the device is used with a passcode.

If a staff member loses a physical credential, it can be used by anyone. If a staff member loses a mobile device, the passcode protects the Mobile ID. As with a physical credential, you can revoke a Mobile ID in the Access Control System. Additionally, through the Portal, you can delete the Mobile ID on the mobile device itself as long as the mobile device still has coverage.

6.4 How many Mobile IDs can be issued to a device?

The following number of Mobile IDs can be issued to a device:

- Up to five devices to each user profile. You do not have to wait for a current device to be deleted if the five device limit has not been reached.
- Up to ten Mobile IDs per device.
- One Mobile ID with a specific MOB Key reference, i.e. you cannot provide two Mobile ID(s) for the same site to a device.

Note: Mobile IDs are unique to each device, therefore they cannot be copied, transferred, re-issued, or re-used. If a user switches devices a new Mobile ID must be issued.

6.5 Can the Mobile ID be transferred to a new device?

For security purposes Mobile IDs are unique to each device and therefore cannot be copied, transferred, re-issued or re-used on another device. If a user buys a new device you must send a new invitation email to download the HID Mobile Access app and issue another Mobile ID.

Note: You must also update the Mobile IDs in the Access Control System.

6.6 Can one user's Mobile ID be accessed from multiple devices?

For security purposes each Mobile ID is unique to a device. It is possible to assign up to five devices per user with new Mobile IDs, if the organization allows it.

6.7 What if I factory-reset my device, or uninstall the Mobile Access App

This process deletes the Mobile ID from the device. For security purposes a Mobile ID cannot be reused. You must have the user download the HID Mobile Access app, send a new invitation email, and issue another Mobile ID.

Note: You must also replace the Mobile IDs in the Access Control System.

6.8 Can Mobile IDs be utilized beyond access control in the future?

Many services such as secure print release or a purchase at a vending machine are possible, if the machine includes an embedded Seos® mobile-enabled reader. Today, most machines support NFC but not BLE.

6.9 If a Mobile ID has been disabled, does this free up a Mobile ID that I can then use for another phone?

No, it does not free up a Mobile ID. A Mobile ID cannot be transferred and/or used on another device.

Section 07

HID Mobile Access App



7.1 Which mobile devices and operating systems are supported?

Mobile Access compatible devices are added on a continual basis as demand warrants. There may be regional differences in device interoperability, as operating system versions are released at different times in each region.

For the list of mobile devices that are compatible with the latest version of the HID Reader Manager App, visit:

<https://www.hidglobal.com/mobile-access-compatible-devices>

HID Mobile Access App version information and device operating system compatibility can be found on the App Store (HID Mobile Access App for iOS) or Play Store (HID Mobile Access App for Android).

7.2 Where can users download the HID Mobile Access App?

The HID Mobile Access® App can be downloaded from either the App Store (iOS) or Play Store (Android), depending on the device's operating system.

However, it is recommended that the end user waits for the invitation email from the Mobile Access portal before downloading, as this contains links to the correct download area, including the registration code necessary for setting up the app.

7.3 How do I open a door using HID Mobile Access?

HID continuously works to secure support for new releases of Android and iOS operating systems. Make sure to use a mobile device supporting HID Mobile Access, listed at:

<https://www.hidglobal.com/mobile-access-compatible-devices>

The door opening experience is slightly different, depending on the reader type or if using BLE or the NFC option.

7.3.1 Using HID Mobile Access with BLE on iPhone or Android with BLE

1. On the mobile device make sure Location Services is set to **On** and for **Mobile Access** (device Settings menu) make sure:
 - **Location** is set to **Always**
 - **Bluetooth Sharing** is enabled
 - **Background App Refresh** is enabled
2. Launch the HID Mobile Access App.
3. Hold the device close to the reader. You will feel the device vibrate and the reader LED will change color/state (default is green).

Some doors or garage barriers may have been configured for Twist and Go. On approaching the doors, within approx. 6 feet (2 meters) of the reader, twist the device briefly 90° to the right and left as if turning a door knob. If successful, the device will vibrate and the reader LED will change color/state (default is green).

Doors can also be opened with a widget, either from a mobile device or a wearable device (iOS or Android). When the HID Mobile Access App is downloaded from app store the HID Mobile Access widget can be accessed from the widget menu. Tap the widget to open the door from around 6 feet (2 meters) of the reader.

7.3.2 Using HID Mobile Access with NFC on an Android device

1. On the mobile device make sure Location Services is set to **On** and NFC is set to **On**. For **Mobile Access** (device Settings menu) make sure **Allow all the time** is enabled for **Location Access**.
2. Launch the HID Mobile Access App.
3. Tap the device to the reader or lock, to open the door. You will feel the device vibrate and the reader LED will change color/state.

Note: NFC uses a short read range and therefore you may need to experiment to find where in your mobile device the NFC chip is located – this is the best place to tap. HID recommends to use NFC for Tap openings with supported Android devices, due to its high performance.

7.4 Does HID Mobile Access work without network coverage?

Once the HID Mobile Access App is installed and the Mobile ID has been issued, network coverage (for example, WI-Fi or cellular) is not necessary. Mobile Access can also be used in areas such as garages or rooms underground.

7.5 Does HID Mobile Access work without a battery?

If the battery is fully drained or the mobile device is switched off, HID Mobile Access will no longer be available. Therefore, we recommend charging the mobile device regularly or to keep an access card or fob as a backup.

7.6 What impact does HID Mobile Access have on battery life?

The mobile device and reader communicate with each other using either the BLE or NFC communication standard. Both standards have been designed with extremely low battery consumption in mind. There should not be any noticeable impact on battery life, especially compared to other popular applications that are constantly syncing.

7.7 Should the user regularly update their mobile device to the latest operating system?

HID Global recommends that you verify that the latest device OS is supported with the site administrator before upgrading the mobile device. A software update should not affect the installed HID Mobile Access App or Mobile ID, if the device is not reset to factory defaults. After updating the mobile device software it is important to check that the Mobile ID is still valid and visible in the HID Mobile Access App.

7.8 Should the user regularly update their mobile device to the latest HID Mobile Access App?

HID Global recommends that you always update to the latest available Mobile Access App to ensure optimal performance and security.

7.9 What is the average data usage by the HID Mobile app?

The following tables provide data consumption figures for Mobile Access App settings on iOS and Android mobile devices. The figures are based on issuing one mobile credential plus ten unlock attempts in a day.

7.9.1 iOS mobile devices

Mobile Access setting	Data consumption
App is in foreground	372 KB
Device is unlocked	421 KB
Always	450 KB

7.9.2 Android mobile devices

Mobile Access setting	Data consumption
App is in foreground	183 KB
Device is unlocked	177 KB
Always	181 KB

7.10 Does the app collect private data?

To offer the service and provide technical support we collect some information, such as:

- Email address
- Mobile device model and OS version
- Mobile device push identifier
- Application identifier
- Reader interaction and error logs

Details of what data we collect are listed in the Privacy Policy users accept during the app installation process or can be found in the [HID® Mobile Access® Application Privacy Notice](#).

Section 08

HID Mobile-enabled readers



8.1 Why doesn't the reader recognize my mobile device?

To initially troubleshoot mobile device/reader connection, confirm the following:

- The Mobile Access® Portal includes the user with the correct device.
- The HID Mobile Access App is installed correctly, and a valid Mobile ID is visible in the device screen.
- The Mobile ID has been entered as a credential in the Access Control System.
- The HID reader is a mobile-enabled reader that supports BLE and/or NFC.
- If you are using Bluetooth readers:
 - You have a supported iOS/Android device with Bluetooth 4.0, and Bluetooth has been enabled on the device.
 - Location Services is enabled on the device.
 - Data connection (internet connection) is enabled on the device.
- If you are using NFC readers:
 - You have a supported Android device, and NFC has been enabled on the device.
 - Location Services is enabled on the device.
 - Data connection (internet connection) is enabled on the device.
- The HID reader works with a traditional access credential.

If you still experience issues, consult your access control vendor for support. Please note the color of the reader LED and reader part number, as this may provide further insight into the issue.

8.2 Why do I get vibration or sound from the device before the reader LED shows green?

This means that the device has successfully communicated with the HID reader and started the transaction. We refer to this feature as "active feedback".

8.3 What happens when Twist and Go is used and there are multiple readers in range of the mobile device?

The device will communicate with the reader with the strongest signal.

8.4 Why is the door opening experience slower with mobile than with a physical card?

The transaction time to validate a Mobile ID compared to a regular card is still slightly longer. However, the users can start the transaction further away from the reader and therefore the overall user experience is not perceived to be slower. Over time the transaction time will be optimized even further.

8.5 How does the user know when to Tap vs. Twist and Go?

Currently, users will not be able to visually recognize which mode the reader has been set to. However, a "Twist and Go not supported" message is displayed when the reader is not enabled for Twist and Go. It is recommended that you proactively communicate or provide information to the users on access door configurations. Suggested options include:

- Configure a blue LED by default on readers where is enabled.
- Place a sticker on the reader.

8.6 Can you have both Tap and Twist and Go enabled at the same time?

Yes.

8.7 Is the power consumption and wiring different to standard readers?

A mobile-enabled iCLASS SE reader consumes slightly more power than non-mobile iCLASS SE reader.

Specifically with a mobile-enabled iCLASS SE reader, there is an added 17mA nominal current and 37mA peak current, compared to nominal and peak currents of non-mobile iCLASS SE readers.

Note: There are no wiring changes required to the reader to support HID Mobile Access.

8.8 Can I control the reading range?

Mobile Access compatible readers are shipped with a short reading distance to allow Tap as default. However, if you have a case where a longer read range is required then your installer can adjust the read range settings in the reader using the HID® Reader Manager™ App. You can then use Twist and Go to open the door or barrier.

Note: Device models can behave differently, therefore you should test the reader/mobile device connection, at the time of installation, with the devices most commonly used within your company.

If you are using NFC as the communications standard between mobile device and reader, the long read range option with Twist and Go and wearables/widget is not available.

8.9 What are possible starting dBm values for BLE reader locations?

The reader opening range values for Tap, Enhanced Tap, Twist and Go, and App Specific can be adjusted using the HID® Reader Manager™ App. For most doors (office environment) you want a n operating distance of 0 to 4 inches (0 to 10 cm) for Tap/Enhanced Tap and 1 to 10 ft (0.3 to 3 m) with Twist and Go. Usually, you will want less for small areas where multiple readers may exist. This will deviate between different mobile devices, and you will need to test and fine tune the settings for the site.

The tables below provide a starting point for various common locations:

SE readers

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

HID Signo readers

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

1. iOS Background and iOS Foreground.

The default setting for App Specific (for example, widget opening from a wearable such as a smartwatch) is -74 dBm and a minimum of -40 dBm (disabled).

8.10 What is Enhanced Tap door opening mode?

Enhanced Tap is a door opening mode that can be configured for HID Signo readers. Similar to standard Tap, Enhanced Tap is typically used for most office environment doors where the mobile device is used in close proximity to the reader (approximately, 0 to 4 inches, 0 to 10 cms).

As opposed to standard Tap, where your mobile device attempts to connect to the reader, the Enhanced Tap opening mode operates with the reader attempting to connect to the mobile device. This allows the Enhanced Tap operation mode to achieve faster opening times.

For detailed information on how to configure HID Signo readers with the HID Reader Manager App to enable the Enhanced Tap opening mode, and adjust reader read ranges, refer to the following:

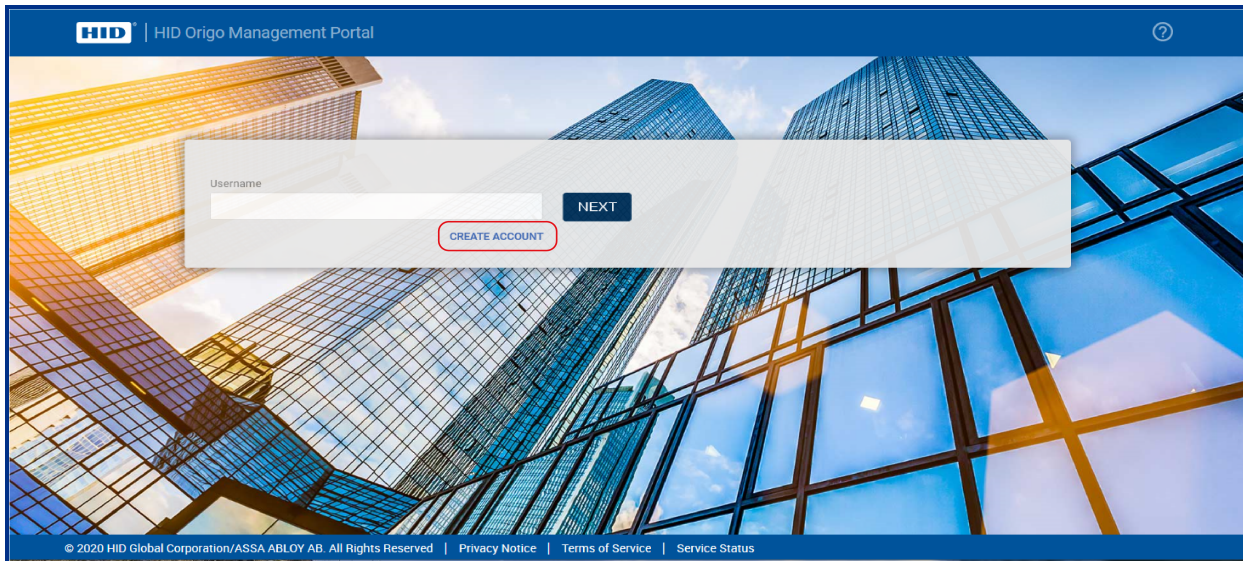
- *HID Reader Manager App User Guide (Android)*, (PLT-03858)
- *HID Reader Manager App User Guide (iOS)*, (PLT-03683)

Section 09

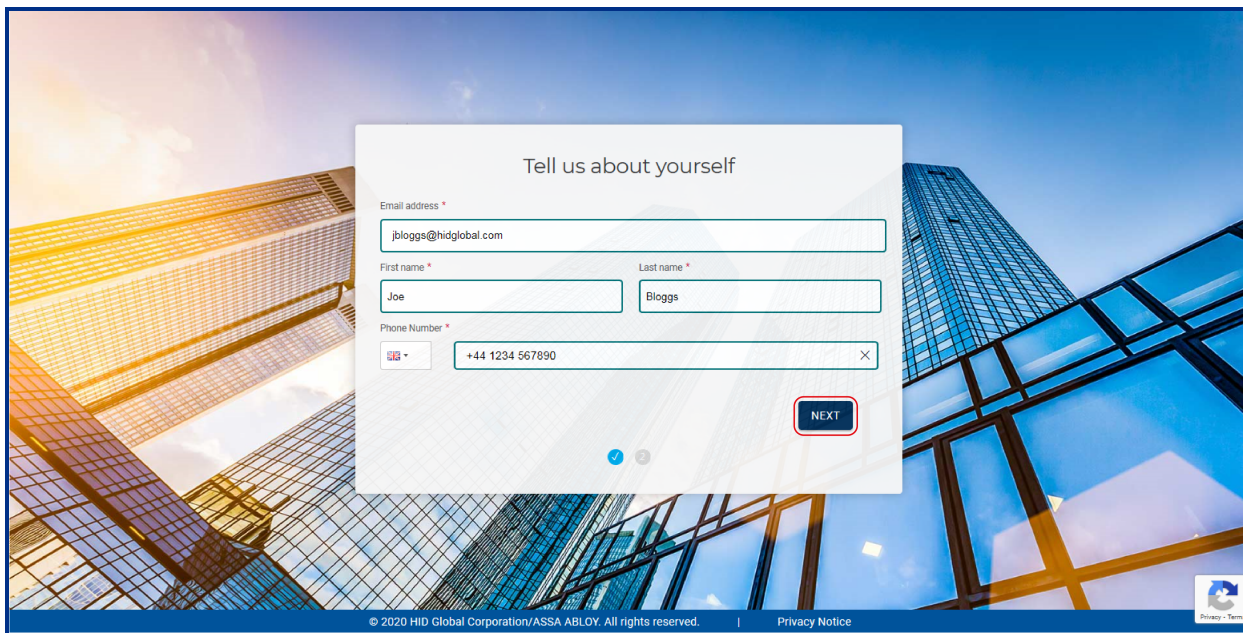
Automated onboarding

9.1 How do I submit a self onboarding request?

1. On the HID Origo Management Portal home page, click **CREATE ACCOUNT**.



2. In the **Tell us about yourself** dialog all fields must be completed. Enter your **Email address**, **First name** and **Last name**. Select your phone region from the drop-down menu and enter your **Phone Number**.
3. When complete, click **Next**.

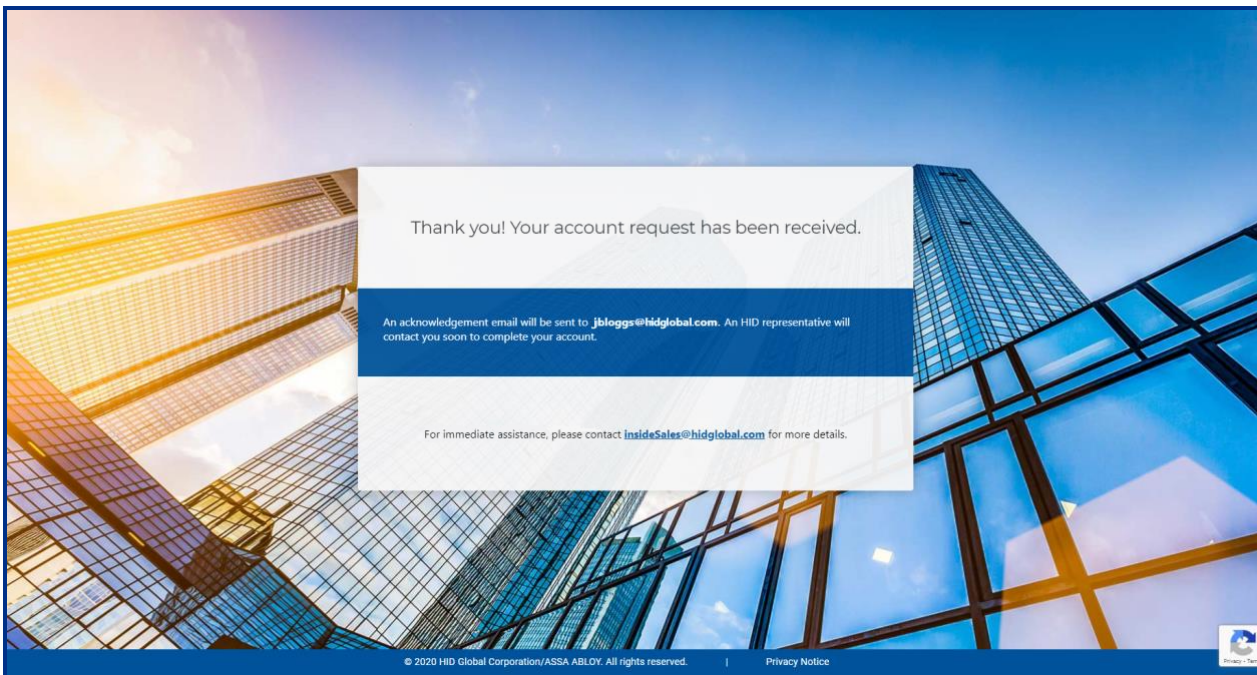


4. In the **About your organization** dialog enter your **Organization name** and **Address** details.

Note: Required fields are indicated.

5. When complete, click **SUBMIT**.

A notification message is displayed to confirm that your request has been received and that an acknowledgment email will be sent to the provided email address.



9.2 What is automated onboarding?

Automated onboarding is an online self-registration process where customers can setup up an account for the HID Mobile Access® Portal.

Automated onboarding provides instant onboarding for new customers. It also simplifies the ordering process via the introduction of new static part numbers. Ordering information and part numbers for Mobile Access can be found in the *Readers and Credentials How to Order Guide* (PLT-02630), available from: <https://www.hidglobal.com/documents>.

9.3 How long does the automated onboarding process take?

The automated onboarding process is extremely efficient and can happen in a matter of a few minutes.

9.4 Can I change the Organization name after onboarding?

Yes. Once the Organization is in the **Pending Account Setup** state or later, the Organization name can be changed.

Note: The **Pending Account Setup** state denotes that Organization, along with the users, have been fully created and only the user email verification is pending.

9.5 Can I start using the Mobile Access service right after the onboarding process?

While you can start exploring the portal features and add users, to use the actual physical access functionality, you will need to place an order for Mobile IDs and readers (if you do not already have mobile enabled readers).

9.6 Why am I asked for HID Elite Program in Step 1 of the onboarding process?

If you are already a member of the iCLASS Elite® (ICE) program, then the request for account creation needs to follow a different path specifically designed for our Elite customers.

9.7 Does automated onboarding include ordering Readers and Mobile IDs

No. The process is designed only for onboarding end users into the HID Origo Management Portal.

9.8 What is needed to place the order?

The information provided in the last step of the automated onboarding process is important to place the commercial order for Mobile IDs, readers, and admin cards. Any HID partner can place the order with the following information:

- Organization ID
- Organization name
- Mobile Keypad
- Format information (if required)
- HID Part Numbers

9.9 What is an organization ID?

An organization ID is a unique identifier that identifies a specific customer portal account.

9.10 What is a Mobile Keypad?

A Mobile Keypad is a reference number for a set of cryptographic keys loaded into a reader. Mobile IDs, Mobile Key Cards, and admin cards will securely authenticate only with readers programmed with matching keypads.

9.11 How can I find my organization ID and Mobile Keypad?

This information is shown at step four of the automated onboarding process. In the Mobile Access portal, the information is displayed in the **Organization Summary** section. The information is also sent to the email address of the Customer Administrator as entered at the time of onboarding.

Section 10

Legacy support

10.1 Are legacy parts being discontinued?

No. You can continue to order Mobile IDs and Reader Admin Cards using the custom part numbers that were previously provided to you.

10.2 If I use the automated onboarding process, am I obliged to place an order? Will my organization ID and Mobile Keyset be reserved forever even though I am not ordering?

HID currently has no such restriction, however we reserve the right to change this policy at any time.

10.3 If I am a HID Partner, how can I ensure that Mobile Admin cards are sent to me as opposed to the end user?

You will need to ensure that your address is entered as the secure shipping address for that particular customer account. You have to be authorized by the end user admin to ensure a safe and secure delivery.

Note: Mobile Admin Cards must be purchased and are not sent out automatically. Ordering information and part numbers for Mobile Access can be found in the *Readers and Credentials How to Order Guide* (PLT-02630), available from: <https://www.hidglobal.com/documents>.

10.4 Are there any issues about shipping the Mobile Admin cards internationally?

No as long as the provided secure shipping address is in a country with no explicit international shipping or trade limitations.

Note: Mobile Admin Cards must be purchased and are not sent out automatically. Ordering information and part numbers for Mobile Access can be found in the *Readers and Credentials How to Order Guide* (PLT-02630), available from: <https://www.hidglobal.com/documents>.

10.5 What formats are allowed when booking an order for a MOBILE-ID?

All current formats will continue to be supported, with the exception of Indala.

10.6 Can I use new part numbers to order for a legacy customer?

Yes. Just use it together with the Organization ID and Mobile Keyset information of the legacy customer (this information can be found in the portal).

Section 11

Security

11.1 What happens if I lose my device?

The mobile operating system protects data on the device if you have enabled the device passcode. It is important that lost devices are reported to you, as the Portal Administrator, so that you can revoke the Mobile ID and remove access rights for the Mobile ID in the Access Control System. We recommend setting up an internal process for reporting lost devices.

11.2 What is the security level on the mobile device?

There are multiple layers of security on the mobile device, both Android and iOS, which continuously update and evolve. The app runs in a dedicated Sandbox with sole access and ownership of its data. The encrypted Mobile ID is stored in a keychain vault within the Sandbox. The vault that protects the Mobile ID is tied with the unique key chain ID for that particular device.

In addition to the security of the mobile OS, Seos® signs and encrypts all Mobile IDs using AES and uniquely binds the Mobile IDs to the specific device. The HID Mobile Access App offers an optional setting to ensure the passcode is entered before activating the Mobile ID.

11.3 How is security maintained?

As part of the service, HID Global will continuously evolve the security standards and adapt them to the latest capabilities offered in the operating systems. Therefore the HID Mobile Access® App should be updated when prompted. For more information on mobile device software update, see [Should the user regularly update their mobile device to the latest operating system?](#)

11.4 When someone downloads the HID Mobile Access App, can they automatically use it?

No, the user needs a valid registration code to register the app. This code can only be issued from the portal, preferably to a secure corporate email address. Only after the registration code has been successfully authenticated can the device be issued a Mobile ID. The HID Mobile Access App will not work in your facility until the Mobile ID has been entered in the Access Control System.

Note: HID Global recommends not using insecure email addresses, such as “free mail” account to send registration codes.

11.5 What should I do before re-issuing a device to another user?

We recommend wiping the mobile device (to scrub its stored data) before re-issue to another user or retiring/recycling the device.

11.6 How do you protect the privacy of the information I provide?

All customer sensitive data is handled according to HID® Global Privacy Notice:

<https://www.hidglobal.com/about/privacy>

To access Mobile Access specific product privacy notices, select the **Product Privacy Notices** option on the **HID Global Privacy Notice** page.

11.7 What if I want to associate an existing Mobile Keypad to a newly created Org?

It is possible to associate an existing Mobile Keypad to a newly created organization with correct end user approvals. For an account created by the automated onboarding process, a system generated Mobile Keypad will be issued which can then be changed via an explicit request to HID Customer Service.

11.8 Can the end user restrict which partners can order Readers and Mobile IDs with their Mobile Keypad or ICE?

HID Elite™ customers can restrict by authorizing certain partners to use the ICE reference when ordering. Non-elite customers with Mobile Keypad references cannot exercise this restriction on the partners.

11.9 What happens if there is no Mobile Keypad for a given end user?

This is mandatory information which every account must have. If for some reason you are missing this information, please contact [HID Customer Service](#).

11.10 Does HID Global perform penetration testing of your Mobile Access solution?

Yes, HID Global continuously perform penetration tests of our Mobile Access solution and we are able to share summaries of those tests under an NDA.

11.11 Is there a defined Information Security role within HID Global?

Yes, HID Global has a CISO (Chief Information Security Officer) that reports into the VP of IT.

11.12 Is education / training given to provide HID Global staff with an awareness of information security?

Yes, security awareness training is mandatory for all ASSA ABLOY staff. The training covers a number of topics, including but not limited to: Social Engineering, Email and Messaging, Browsing, Social Networks, Mobile Device Security, Passwords, Data Security, Wi-Fi Security, Working Remotely, Physical Security, Personally Identifiable Information, Cloud, Privacy.

11.13 Where does HID Global store and process End Customer data?

End Customer data is hosted and processed in HID Global facilities, a secure ViaWest data center and Virtual Private Cloud instances hosted on Amazon Web Services. The HID Global and ViaWest data centers are fully secured and only authorized HID personnel have access. All services are hosted in the United States.

11.14 How does HID Global monitor your network for unauthorized devices?

HID Global continuously monitors the network for unauthorized devices and are implementing controls, such as device hostscan for the Cisco VPN, to ensure only authorized devices are granted access to the network.

11.15 Is HID Mobile Access GDPR compliant?

Yes, HID is GDPR (General Data Protection Regulation) compliant, including EU-U.S. Privacy Shield Framework and Swiss-U.S. Privacy Shield Framework(s).

Revision history

Date	Description	Revision
August 2023	Sections 5.2.3 Upgrade an existing pre-paid subscription and Section 5.2.4 Multiple channel partners. Added information for upgrading from a MID-SUB-T053 to a MID-SUB-T103 subscription.	C.0
August 2023	Section 4.14 How can I find out which users are inactive? Added a note regarding the use of quick and advanced searches.	B.9
April 2023	<ul style="list-style-type: none"> Section 4.7 Can I try Mobile Access free of charge? Updated the Portal screenshots for the Trial Subscription feature. Section 5: New section added related to HID Mobile Identities Subscriptions. 	B.8
March 2023	Section 4.7 Can I try Mobile Access free of charge? Updated the number of licenses included in a Trial Subscription (from 20 to 100).	B.7
March 2022	Section 6.10 Does the app collect private data? Updated section to remove information related to "GPS position and Location data".	B.6
February 2022	<ul style="list-style-type: none"> Section 3.6: How do I onboard for the Mobile Access service. Updated section content and onboarding url. Section 4.4: How can I reset my HID password. Added a note regarding email notifications sent for modified account password and/or modified authentication factor. Section 4.8: How do I redeem an invitation code using a QR Code. New section added. Section 4.19: How do I configure an invitation link. Added sub-sections for removing the invitation code from the invitation email and configuring the invitation email distribution. Section 7.10: What is Enhanced Tap door opening mode. New section added. 	B.5
October 2021	<ul style="list-style-type: none"> Section 4.27: How are MIDs replenished? New section added. Section 6.10. Update to section text. 	B.4
July 2021	<ul style="list-style-type: none"> Section 1.1. Updates to section text. Section 3.5. Added HID Signo readers to the "Supported readers" entry in the table. Section 3.8. Added links to product support terms and HID Origo Service Status. Section 4.1. Expanded definition of "jail-broken" mobile devices. Section 4.3. Expanded definition of roles and role functions for the HID Origo Portal. Section 4.6. New question and answer section added. Section 4.7. Updates to section text and "Mobile Identities" screenshot. Section 4.10. Updated the "Mobile Identities" screenshot. Section 4.12. Added Readers and Credentials How to Order Guide reference. Section 4.24. Updated section text to define "Obsolete" MIDs. Section 4.28 and 4.29. New question and answer section added. Section 4, 5, and 9. Removed sections related to the legacy SIS portal. Section 9.3 and 9.4. Added Readers and Credentials How to Order Guide reference. 	B.3
April 2021	<ul style="list-style-type: none"> Removed the following: <ul style="list-style-type: none"> Section 4.12: I am using all my purchased user licenses, how do I free up user licenses? Section 8.12: Which new simplified part numbers are introduced as part of the improved ordering process? Section 8.13: What is the validity period of the temporary Mobile ID? Section 4.30 Certificate-based Authentication. New section added. 	B.2

Date	Description	Revision
March 2021	<ul style="list-style-type: none"> Section 2.8 Does HID Global comply with ISO27001? Updated compliance information. Section 4.14 How do I enable the Site field and Phone Number field in the Portal? New section added. 	B.1
November 2020	Section 4.8 How do I configure the time zone setting in the Portal. New section added.	B.0
October 2020	<ul style="list-style-type: none"> Section 4.26 How do I activate auto-replenishment. New section added. Section 4.27 How do I activate Delegated Authorization functionality. New section added. Section 4.28 What role does a Service Provider have for Delegated Authorization. New section added. Section 6.6 What impact does HID Mobile Access have on battery life. Answer text updated. Section 8.1 How do I submit a self onboarding request. New section added. 	A.9
July 2020	<ul style="list-style-type: none"> Section 4.6 Can I try Mobile Access free of charge? New question added. Section 5.1 What are Mobile IDs? Updated description. Updates to a number of sections with additional screenshots added. 	A.8
April 2020	Section 3.15 How do I configure a custom mail server? New section added.	A.7
October 2019	<ul style="list-style-type: none"> Section 3.21 Deleting credentials issued to the same device/phone from different Mobile Access Portals? New section added. Section 3.22 How do I enable Enterprise Policy Enforcement? New section added. 	A.6
September 2019	Section 3.17 How do I manage obsolete or duplicate Mobile IDs? New question and answer section added.	A.5
August 2019	Section 3.11 How do I assign a photo image to an individual enrolled user? New question and answer added.	A.4
May 2019	<ul style="list-style-type: none"> Section 4.12 How do I configure an invitation link? New question and answer added. Section 4.14 Why can't I delete users? New question and answer added. Section 6.11 Why do I get a HCE Error Code 101 when I try to open a door with HID Mobile Access on my Android device? New question and answer added. 	A.3
April 2019	<ul style="list-style-type: none"> Minor updates throughout document. Combined questions in previous Section 8: Security and Section 11: Privacy and security into Section 10: Security. 	A.2
February 2018	<ul style="list-style-type: none"> Updated all sections with additional FAQs. Updated the included Mobile Access Portal screenshots. 	A.1
October 2014	Initial release.	A.0



hidglobal.com

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

© 2023 HID Global Corporation/ASSA ABLOY AB.

All rights reserved.

PLT-02085, Rev. C.0

Part of ASSA ABLOY