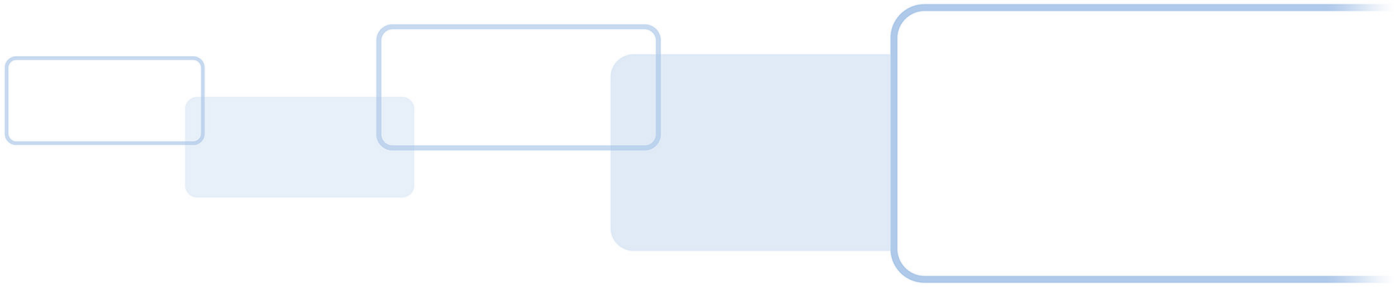
HID Mobile Access®

Solution Overview

PLT-02078, Rev. A.4
April 2020



Copyright

Trademarks

Revision history

Date	Description	Revision
April 2020	Updates implemented: ■ *Section 4.3 Terminating the Service*. Updated Note text. ■ Updated images with HID® Signo™ readers.	A.4
January 2020	Document re-structured and updated for new features and enhancements to the HID Mobile Access solution.	A.3
June 2016	Updated name of configuration card (Mobile Key Card).	A.2
March 2015	Updated Section 4.4.1 Supported Devices.	A.1
October 2014	Initial release.	A.0

Contacts

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

Americas and Corporate	Asia Pacific
611 Center Ridge Drive Austin, TX 78753 USA Phone: +1 866 607 7339 Fax: +1 949 732 2120	19/F 625 King's Road North Point, Island East Hong Kong Phone: +852 3160 9833 Fax: +852 3160 4809
Europe, Middle East and Africa (EMEA)	**Brazil**
Haverhill Business Park, Phoenix Road Haverhill, Suffolk, CB9 7AE United Kingdom Phone: +44 (0) 1440 711 822 Fax: +44 (0) 1440 714 840	Condomínio Business Center Av. Ermano Marchetti, 1435 Galpão A2 - CEP 05038-001 Lapa - São Paulo / SP Brazil Phone: +55 11 5514-7100

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

Contents

1 Introduction

1.1 Document purpose

This document is aimed at Enterprise Security Directors who have invested in HID Mobile Access® as well as a first point of reference for Project Managers responsible for deploying the Mobile Access solution in the enterprise.

It provides a high level overview of the solution, how the components interact with each other and how you can get the most out of your investment.

1.2 What is Mobile Access?

The HID Mobile Access solution has been designed for commercial deployment in enterprises, educational institutions, government offices or health care facilities and complements an existing access control solution. When the Mobile Access service is operational enterprise administrators manage the organizations users and issue/revoke Mobile IDs via a cloud-based portal, while company personnel access workplace locations using their mobile devices.

The Mobile Access solution, which leverages Seos® as its underlying credential technology, consists of a number components (these are outlined in more detail in *Section 2 Mobile Access solution components*):

- HID Origo™ Management Portal
- Mobile IDs
- Mobile Access compatible readers
- Mobile Access® App

As an alternative to using cards or fobs, the adoption of HID Mobile Access extends access functionality to mobile devices allowing end users to securely and conveniently enter workplace locations using their Android and/or iOS smart phones, tablets, or wearables.

When a user approaches a reader, the following modes of interaction can be performed with their mobile devices for access:

- **Tap:** The mobile device is brought very close to, or touching, the reader (a similar user experience to using a physical credential).
- **Twist and Go:** The mobile device holder initiates access by twisting the mobile device in a sharp 90° rotation in either direction (a similar motion to using a physical door handle).
- **App Specific:** This entrance opening mode is specific to an application, for example, widget opening from a wearable such as a smartwatch.

1.3 License agreements and policies

In addition to any purchase orders or contracts you may have signed with your supplier, HID Mobile Access requires Portal Administrators and End-users (the persons using HID Mobile Access on their mobile devices) to accept the following license agreements and privacy policies before they can start using the service.

Document title	Description	Target audience	Available from
HID Origo Management Portal Terms of Service	Informs Portal Administrators of their role and responsibilities in connection with the Mobile Access service	Portal Administrators	Accepted on registration of a user login
HID Origo Management Portal Privacy Notice	Covers data collected and processed about Portal Administrators via the portal as well as user data uploaded by Portal Administrators	Portal Administrators	HID Origo Management Portal (within the footer of each portal page)
HID Mobile Access Information Security and Privacy Overview	Provides information required to understand the security characteristics in HID Mobile Access	Security professionals	HID Origo Management Portal
HID Mobile Access License and User Agreement	Grants license to use the service and governs obligations of how to use it responsibly	Mobile Access end users	Accepted during end user App registration process
HID Mobile Access Application Privacy Notice	Covers data collected about users via the mobile device and stored on HID Global servers	Mobile Access end users	Accepted during end user App registration process

1.3.1 Recommended enterprise policies

In combination with HID Mobile Access, HID Global recommends implementing the following policies within your Enterprise environment:

- Install a reporting process for loss of a mobile device and the subsequent revocation of the Mobile IDs and disabling of the associated Mobile IDs within the Access Control System.
- Ban jailbroken or rooted mobile devices where the operating system has been compromised. Jailbroken or rooted mobile devices circumvent the built-in security and protection of the operating system, opening up the mobile device to high risk from malware and unsupported uses.
- Mandate the use of a passcode or fingerprint scan as additional security mechanism against the loss of a mobile device (set within the mobile device).
- 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.

1.4 Reference material

The following documents and instructional tutorials are available for more detailed information relating to Mobile Access:

Resource title	Description	Available from
HID Mobile Access Frequently Asked Questions (PLT-02085)	HID Mobile Access related questions and answers to support HID Origo Management Portal administrators.	HID Origo Management Portal
Readers and Credentials How to Order Guide (PLT-02630)	Provides information to Mobile Access implementers on Reader and Credential configuration (including Mobile Access) and the process that should be used to order them.	HID Global site via the **Document Library**
HID Reader Manager Solution User Guide (Android), (PLT-03858) *HID Reader Manager Solution User Guide (iOS)*, (PLT-03858)	Provides information relevant to HID Reader Manager portal administrators and Reader Technicians for procedures relating to the Reader Manager Portal and Reader Manager App.	HID Global site via the **Document Library** HID Reader Manager App
Getting Started with the HID Mobile Access App	Video tutorial that explains the HID Mobile Access App and the interaction between the mobile device and the reader.	HID Origo Management Portal Hosted on **YouTube**
How To Issue And Revoke Mobile IDs in the HID Origo Management Portal	Video tutorial aimed at Mobile Access portal administrators explaining how to send an invite to use HID Mobile Access, how to issue and revoke a Mobile IDs, and how to adjust settings in the Mobile Access App.	HID Origo Management Portal Hosted on **YouTube**
How to Set Up the HID Reader Manager App	Video tutorial aimed at Reader Manager portal administrators and Reader Technicians explaining how to download and register yourself as a technician on the HID Reader manager App.	Hosted on **YouTube**

1.5 Definitions, acronyms, and abbreviations

The following provides the definition of terms used throughout this document.

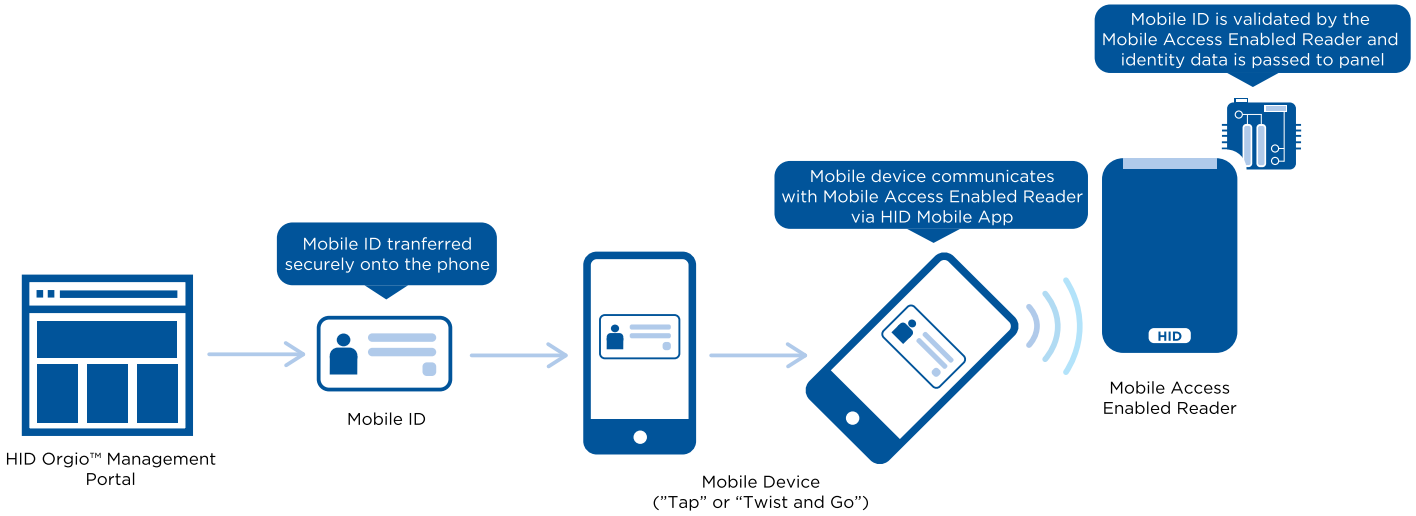
Term	Definition
BLE	Bluetooth Low Energy (formerly marketed as Bluetooth Smart) is a wireless personal area network technology. In contrast to Classic Bluetooth, Bluetooth Low Energy (BLE) is designed to provide significantly lower power consumption.
End user	Enterprise personnel using HID Mobile Access on their mobile devices.
Enterprise Policy Enforcement	A setting in the Mobile Identities Service on the HID Origo Management Portal which enforces the requirement that users within the organization have their mobile devices unlocked in order to open a door.
HID Mobile Access	The solution that enables employees to use a smartphone, tablet, or wearable for entrance access. Users gain access via intuitive “Tap” and “Twist and Go” gestures with mobile devices or an App Specific application. "App Specific" relates to an entrance opening mode specific to an opening application such as widget opening from a mobile device or wearable.
HID Origo Management Portal	A managed service that allows administrators to manage users and securely issue or revoke Mobile IDs to the user’s mobile device.
Mobile Credential/Mobile ID	Virtual credentials that are stored on a mobile device. Mobile IDs are issued and/or revoked via HID Origo Mobile Identities service on the HID Origo Management Portal. Mobile IDs are unique to each device and cannot be copied. If a user switches devices, a new Mobile ID must be issued.
Mobile-Enabled readers	Mobile-Enabled readers are fully activated and personalized to support an organization’s specific Mobile IDs.
Mobile Identities Service	A service available on the HID Origo Management Portal, used to manage Mobile Access users, devices, and Mobile IDs.
Mobile-Ready readers	BLE enabled readers that have been prepared to support HID Mobile Access but lack the personalized configuration (Mobile Keyset) to read an organization’s specific Mobile IDs.
Mobile Keyset (MOB or ICE)	Mobile Keyset is a reference number for a set of cryptographic keys loaded into a reader. Mobile IDs, Mobile Key cards, and Mobile Admin cards will securely authenticate only with readers programmed with a matching Keyset. An organization is assigned a Mobile Keyset upon registration into either the HID Elite™ (ICE) or HID Mobile Access (MOB) programs.
NFC	Near Field Communication (typically 13.56 MHz air interface) is a short range wireless connectivity standard to enable communication between devices when they are touched together, or brought within a few centimeters of each other.
Onboarding	Onboarding is a HID Global process where an account for an Organization is established in the HID Origo Management Portal. Automated Onboarding is an online process where an Organization can self register to setup up an account in the HID Origo Management Portal.
Organization ID	Organization ID is a reference number for a unique account within the HID Origo Management Portal . It is assigned at the conclusion of account registration. The correct Organization ID must be supplied when ordering Mobile IDs or User Licenses.

OSDP	Open Supervised Device Protocol (OSDP) is an access control communications standard developed by the Security Industry Association (SIA) to improve interoperability among access control and security products.
PACS	Physical Access Control System.
Portal administrator	HID Origo Management Portal Administrator with sufficient privileges to manage users and securely issue or revoke Mobile IDs to end user mobile devices.
Seos	A technology platform created by HID Global which provides a secure, portable, adaptable, device-agnostic way of managing secure identity information and applications.
Tap	The Tap gesture with mobile device for door opening. The operation is typically used when the mobile device is in close proximity to the reader.
Twist and Go	The Twist gesture with mobile device for door opening. The operation is typically used when the mobile device is at a longer distance from the reader.
User licenses	HID Mobile Access customers starting a subscription service for HID Origo Mobile Identities, order and pay for the service though User Licenses. User Licenses are valid for one year and can be renewed. Also the number of User Licenses can be increased within a service term by ordering Add-on licenses.

2 Mobile Access solution components

The Mobile Access® solution, which leverages Seos® as its underlying credential technology, consists of the following components:

- **HID Origo™ Management Portal:** An administration interface containing services that allow you to manage users and securely issue or revoke Mobile IDs to end user mobile devices. The portal is available as a hosted service.
- **Mobile IDs:** Virtual credentials, integrated Seos technology, that are stored on the mobile device and issued or revoked via the Mobile Identities Service on the HID Origo Management Portal.
- **HID Mobile Access® App:** The Mobile Access App used on end user Android and iOS devices.
- **Mobile-Enabled Readers:** iCLASS SE® or multiCLASS SE® readers configured to securely authenticate with an organization's Mobile ID's via Bluetooth Smart and/or NFC communication standards.

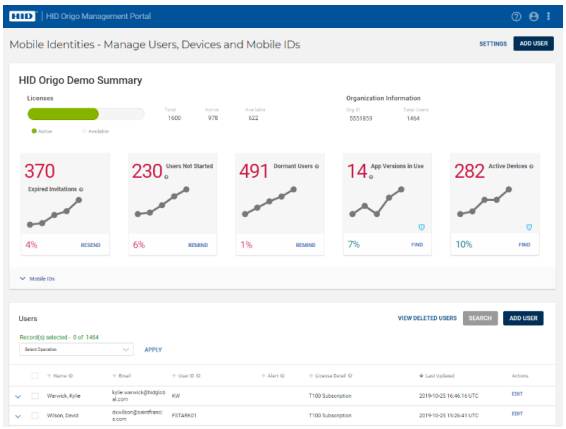


2.1 HID Origo Management Portal

The HID Origo Management Portal, or to be more specific, the Mobile Identities Service instance within the HID Origo Management Portal, allows enterprise administrators to manage users and issue and revoke Mobile IDs to user's mobile devices.

The HID Origo Management Portal is a hosted service available to registered users via:
https://portal.origo.hidglobal.com

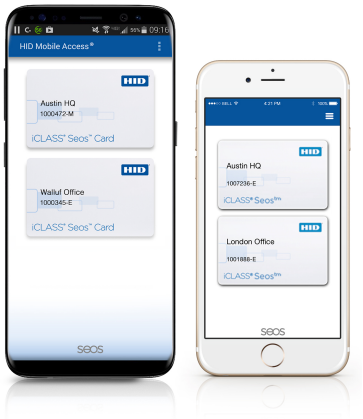
Each enterprise has its own instance of the portal, which is set up by HID Global during the Onboarding process. See *Section 3.2 Onboarding process*.



2.2 Mobile IDs

Mobile IDs are the virtual credentials that are stored on the mobile device and issued or revoked via the Mobile Identities Service instance on the HID Origo Management Portal. 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.

Once Onboarding has been completed, your purchased HID Origo Mobile Identities user licenses and your Mobile IDs will already be set up in the HID Origo Management Portal. See *Section 3.2 Onboarding process*.



2.3 HID Mobile Access App

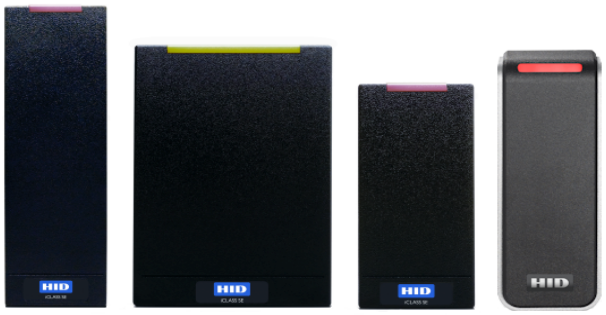
The HID Mobile Access App, on a user's mobile device, manages Mobile IDs and contains some limited user settings.

Users can download the HID Mobile Access App free of charge for Android mobile devices via Google Play and, for iOS devices, via the Apple App Store.

The Organization's portal administrator enrolls new users via the Mobile Identities Service instance in the HID Origo Management Portal. This generates an invitation email with the links to the respective app stores for HID Mobile Access App download as well as a registration code that end users use to register. See *Section 3.4 Mobile device setup*.

2.4 HID Mobile Access readers

HID Mobile Access compatible readers are readers that read Mobile IDs (virtual credentials on mobile devices) as well as 13.56 MHz and 125 kHz contactless credentials (with the exception of Indala Prox). When a virtual credential on a mobile device is presented to a HID Mobile Access compatible reader, the reader securely reads the access card number and then transmits the number to the access control panel. No special system modifications are required to read Mobile IDs. Existing Wiegand readers can easily be replaced and work with existing access control panel hardware.



For more information relating to HID Mobile Access compatible readers refer to *Section 3.1.1 Readers for HID Mobile Access*.

3 Solution deployment

3.1 Reader installation and configuration

This section provides an overview of infrastructure, deployment, and configuration considerations for site administrators and integrators deploying HID Mobile Access® readers. For detailed information relating to reader deployment and reader configuration refer to the following documents:

- *HID Mobile Access Reader Deployment Guide,* (PLT-02076)
- *HID Reader Manager Solution User Guide (Android)*, (PLT-03858)
- *HID Reader Manager Solution User Guide (iOS)*, (PLT-03683)

3.1.1 Readers for HID Mobile Access

HID Mobile Access requires Mobile Access compatible readers that are configured to securely authenticate with an organization's Mobile IDs via BLE and/or NFC communication standards.

Mobile-Enabled	Mobile-Enabled readers are fully activated and personalized to support an organization's specific Mobile IDs. These readers can only be ordered after the organization has completed registration for HID Mobile Access or HID Elite™ program. MOB or ICE Mobile Keyset will be required at time of order.
Mobile-Ready	Mobile-Ready readers are prepared to support HID Mobile Access but lack the personalized configuration (Mobile Keyset) to read an organization's specific Mobile IDs. These readers can be ordered at any time but will require field activation after the organization has completed registration for HID Mobile Access. To support a specific organization's Mobile IDs, these readers need to be personalized (Mobile Keyset loaded) using a Mobile Key Card or the HID® Reader Manager™ App.
Mobile-Capable	A Mobile-Capable reader is built from the base iCLASS SE® platform prior to market introduction of HID Mobile Access. The reader is not prepared with the necessary hardware and requires a compatible firmware version to work with Mobile IDs. It is possible to upgrade these readers in the field to support HID Mobile Access utilizing orderable iCLASS SE upgrade kits and configuration using the HID Reader Manager App. **Note:** For upgrade kit part numbers, refer to the *HID Readers and Credentials How to Order Guide* (PLT-02630).

If you have ordered Mobile Access compatible readers and the HID Mobile Access service subscription at the same time, your readers will be personalized at the factory to be Mobile-Enabled. In order to ensure that your existing credentials and environmental conditions are taken into account, it is recommended that your installer perform a site survey before placing his order with HID Global.

If you have purchased the HID Mobile Access service subscription at a later time, after Mobile-Ready readers have already been installed at your site, an installer can personalize those readers using the HID Reader Manager App (or Mobile Key Cards), to create Mobile-Enabled readers.

For ordering information relating to Mobile Access compatible readers, User License Subscriptions and/or Mobile ID Credentials, refer to the *HID Readers and Credentials How to Order Guide* (PLT-02630).

3.1.2 Reader installation

Site environmental considerations

Environmental conditions at the site influence the achievable read range distance. Metal takes power away from RF fields and thus decreases read range. This is true not only for BLE devices but contactless credentials as well. Plastic spacers (reader form factor dependent) can be used to space the reader away from metallic surfaces and reduce the impact the metal will have on read range. Your installer will be able to advise you accordingly.

Note: Reader spacers are orderable, and part numbers can be found in the *Readers and Credential How to Order Guide* (PLT-02630), located at: **https://www.hidglobal.com/documents**

Variances in antenna size, placement and the overall electrical design of the reader will impact the performance of the reader. Therefore, it is likely that a site with readers of multiple form factors will have different actual performances, even if all readers have the same configuration. To get the most consistent performance possible, BLE read range settings may need to be adjusted with the HID Reader Manager App for mobile-enabled readers.

Currently installed reader infrastructure

There is no need to replace all your installed readers at the same time. HID Mobile Access readers look exactly like standard iCLASS SE readers. If you would like your users to recognize the readers that have Mobile Access capability, we recommend either using the blue LED light (a configuration that can be ordered or configured with the HID Reader Manager App for a mobile-enabled reader) or marking readers with a small dot sticker (available in retail).

New reader installation

The installation of HID Mobile Access readers should be performed by an experienced installer, however installation should not be any more complicated than that of standard HID readers. Existing Wiegand readers can easily be replaced with new readers with no additional wiring required for the reader to support HID Mobile Access. Refer to your specific reader installation documentation.

It should be noted that a Mobile-Enabled iCLASS SE reader consumes slightly more power than a 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. Therefore it is recommended that existing access control panel hardware is checked.

3.1.3 Reader configuration

Depending on your environment and user requirements, HID Mobile Access readers may require configuration after reader installation.

Personalization of Mobile-Ready readers

If you are using a Mobile-Ready reader it must be personalized to support an organization's specific Mobile IDs using the HID Reader Manager App or a Mobile Key Card. This turns your Mobile-Ready reader into a Mobile-Enabled reader. See the Mobile-Ready information in *Section 3.1.1 Readers for HID Mobile Access*.

If you have ordered Mobile-Ready readers and HID Origo Mobile Identities user licenses at the same time, your readers can be personalized at the factory to be Mobile-Enabled, and therefore this configuration step will not be necessary.

Reader to mobile device communication standard

HID 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. Whether your mobile devices use BLE or NFC to communicate with the reader, depends on the installed readers and the mobile devices that are to be used for Mobile Access.

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 an App Specific application (for example, widget from a phone or wearable), use BLE.

The following provides the key differences between the two communication standards:

	NFC	**BLE**
Supported mobile network operators	All mobile operators	All mobile operators
Supported device operating systems[1]	All Android devices with NFC (iOS currently does not allow apps to use NFC)	Android 4.4 (or higher) iOS 7 (or higher)
Supported readers	iCLASS SE®/multiCLASS SE® readers (Rev E or newer, shipped after Q1 2013) or readers upgraded with a BLE upgrade kit	All iCLASS SE® or multiCLASS SE® that have a BLE module (i.e. 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)

1. Although iOS 6 and above supports NFC, Mobile Access does not yet support NFC in iOS.

Note: If issues are experienced when using Android devices, where both NFC and BLE are enabled, it is recommended to use BLE over NFC.

Reader read range

iCLASS SE® or multiCLASS SE® mobile-enabled readers are shipped with a short read distance in order to allow the mobile device Tap gesture to be used as default for door opening (the Tap gesture emulates door opening with a physical credential) or an App Specific application, such as a widget from a mobile device or wearable. However, if you have a case where a longer read range is required then the read range settings in the reader can be adjusted using the HID Reader Manager App. You can then use Twist and Go to open the door or barrier.

Note: As the range and performance of mobile devices may vary, it is recommended that you test the reader/mobile device connection at the time of installation with the devices most commonly used within your company.

For most doors (office environment) an opening range of 5.9 to 7.87 inches (15 to 20 cm) for Tap and 19.68 to 39.37 inches (0.5 to 1 meter) with Twist and Go is recommended. These values are typically less for areas where elevators are located or small areas where multiple readers may exist.

The settings listed below provide a starting point for some common locations:

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

In certain installations a higher or lower Transmit Power may be required, however this setting should only be adjusted if the Read Range settings do not result in the desired read range. It is recommended that the default Transmit Power setting (-4 dBm) is not exceeded unless absolutely necessary.

For detailed information on how to connect to readers with the HID Reader Manager App and adjust reader read ranges for Tap, Twist and Go, and App Specific (for example, widget) refer to the following:

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

3.2 Onboarding process

3.2.1 Onboarding

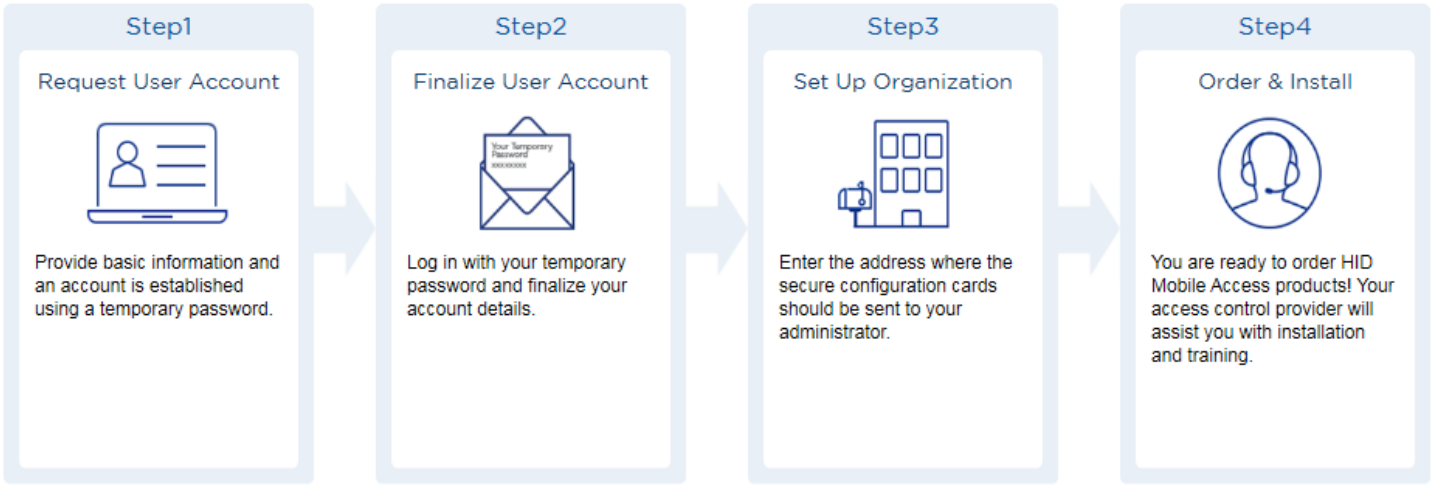
Onboarding is a HID Global process where an account for an Organization is established for HID Mobile Access in the HID Origo Management Portal. Once an account is created the Organization can order and purchase subscription user licenses or Mobile IDs through your Access Control Provider. During this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

3.2.2 Automated Onboarding

Automated Onboarding is an online self-registration process where an Organization can setup up an account for the HID Origo Management Portal. Automated Onboarding provides instant onboarding for new customers and it simplifies the ordering process.

To setup a HID Origo Management Portal account via the automated Onboarding process go to the following site and follow the online steps:

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



Once an account has been created and the organization has been setup in the system, Step 4 of the automated Onboarding process will allow you to order products, via your Access Control Provider, by providing the following information:

- Organizational ID
- Mobile Keyset
- Format and programming information
- HID Mobile Access part numbers. For more information refer to the *HID Readers and Credentials How to Order Guide*, (PLT-02630).

Note: Self-service Onboarding for HID Origo follows the above process. Once an order for subscription user licenses is placed the customer's account is automatically migrated to HID Origo and login is redirected to the HID Origo Management Portal.

3.3 HID Origo Management Portal

The HID Origo Management Portal, or more specifically the Mobile Identities Service instance within the HID Origo Management Portal, allows enterprise administrators to manage users and issue and revoke Mobile IDs to user's mobile devices.

The following outlines the features and functions of the Mobile Identities Service within the HID Origo Management Portal:

Note: Features and functions are regularly added to the Mobile Identities Service, therefore check the latest release notes, available from within the HID Origo Management Portal.

- Two-factor authentication on log-in.
- Enroll users individually or in batch by importing a .csv file.
- Invite users individually or in batch. This function generates an invitation email with details on where to download the HID Mobile Access App and a registration code.
- Edit invitation email (customize to the enterprise's requirements).
- View status of invitations.
- Issue a Mobile ID to a mobile device. This can be done automatically as part of the enrollment process, or as a second manual step thereafter.
- Revoke a Mobile ID from a mobile device.
- Delete obsolete Mobile IDs (MIDs), select and remove a range of MIDs.
- Multiple credentials per enterprise (for example, multiple credentials for different sites if sites have different MOB/ICE Keys).
- Configure up to five devices per user and up to 10 Mobile IDs per device (each Mobile ID must be unique).
- Batch-download of users and Mobile IDs. This generates a .csv file that can be uploaded into the Access Control System in order to assign access rights to Mobile IDs.
- Upload and assign a photo image to an individual enrolled user and subsequently edit/delete the user photo.
- Upload a corporate logo image and push this to mobile devices so that it is visible within the user's HID Mobile Access App on issuing new Mobile IDs.
- Enable/disable Enterprise Policy Enforcement for enrolled users.

To familiarize yourself with the portal functions, a good place to start is the *HID Mobile Access Frequently Asked Questions*, (PLT-02085) document. Also additional information and instructional videos are available from within the portal via the **Help** menu.

3.3.1 Portal access

The HID Origo Management Portal can be accessed via the internet on: **https://portal.origo.hidglobal.com**

The following browsers are supported:

- Internet Explorer
- Firefox
- Chrome
- Safari

The first administrator requesting a log-in will be setup as the Organization Administrator. The Organization Administrator can set up additional roles within the portal based on the following functional abilities:

Portal role	Functional abilities
Administrator	■ Configure reporting and notification settings ■ Change the description and background image for the corporate badge ■ Edit the invitation email sent to users ■ Full edit, add, and delete privileges to all users ■ Issue and revoke Mobile IDs and delete mobile devices
Operator	■ Full edit, add, and delete privileges to all users ■ Issue and revoke Mobile IDs and delete mobile devices
Reviewer	■ Read only privileges to user data, devices, and Mobile IDs

3.4 Mobile device setup

3.4.1 Compatible mobile devices

Although mobile devices are added on a continual basis, the list of compatible mobile devices that currently support the HID Mobile Access App can be found on:

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

3.4.2 Installation of the HID Mobile Access App

When enrolling a new user for Mobile Access, the Mobile Identities Service in the HID Origo Management Portal generates an invitation email (the email can be edited and customized so that it is specific for your company) to the user containing links to the relevant app stores to download the HID Mobile Access App. The generated invitation email also contains an invitation code.

Note: HID recommends sending invitation codes via the corporate email system and not to insecure email addresses, such as “free mail” accounts.

After downloading and installing the application, the user is prompted to register by clicking on the invitation code in the email or the user can manually enter the code in the Mobile Access App.

During the registration process, the device is registered via the Mobile Identities Service in the HID Origo Management Portal and Mobile IDs can then be pushed to the device. Depending on the options selected within the Mobile Identities Service, this either happens automatically, within a couple of minutes after registration, or the Portal Administrator has the option to manually push Mobile IDs to the device at a later time. During mobile device registration and Mobile ID delivery the mobile device must be connected to the internet, either via mobile data network or Wi-Fi.

For more detailed information on downloading and registering the Mobile Access App, refer to the *HID Mobile Access App User Guide* (PLT-02077).

3.4.3 Opening doors with the HID Mobile Access App

In order to open doors with the HID Mobile Access Application, Bluetooth and/or NFC must be enabled in the mobile device settings to communicate with the readers. The application will prompt the user, if this has not been done.

Opening doors using Tap

The mobile device functions like a physical credential. Tap the device to the reader. You will feel the device vibrate and the reader LED will change color/state.

HID recommends to use NFC for Tap openings with supported Android devices, due to it's high performance.

For iOS devices, Tap always utilizes BLE. Make sure Bluetooth is enabled on the mobile device (usually within the device Settings menu).

Note: The Tap range may require adjustment in order to prevent Apple Pay opening on the mobile device.

Opening doors using Twist and Go

On approaching the doors, within approximately six feet (two meters) of the reader (depending on the reader configuration), 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.

The reading distance is configurable, however these settings may be different, due to environmental factors (i.e. type of surface the reader is mounted on) and the hardware and software of the mobile device.

Setting a longer read distance is ideal for garages, and warehouses. It can also help meet some accessibility requirements for persons with mobility disabilities.

Opening doors using an App Specific Application

This entrance opening mode is specific to an application, such as opening doors with a widget, either from a mobile device or a wearable (smartwatch).

As an example, when the HID Mobile Access App is downloaded from the app store the HID Mobile Access widget can be accessed from the widget menu to open a door.

3.4.4 Mobile Access App settings

The Mobile Access App provides access to a number of additional configurable Mobile Access settings via the app **Settings** menu.

Note: The layout and availability of settings may differ between mobile device model and operating system.

- **Allow Mobile Access When:** Select this setting to access options to allow Mobile Access when:
  - The app is in the foreground
  - The device is unlocked
  - Always (when the app is in the foreground, background, and when the device is unlocked)
- **User feedback:** Options to enable/disable sound and vibration feedback.
- **Twist and Go:** The motion sensor can be disabled on the mobile device side, for readers set to long read distance.
- **Bluetooth sensitivity:** Option to adjust the sensitivity of the device's Bluetooth interface.
- **Notification:** Option to enable entrance access from the device Notification Panel and wearable.

For more detailed information on the above Mobile Access App settings, refer to the *HID Mobile Access App User Guide,* (PLT-02077).

3.4.5 User training

Customer feedback has shown that a short introduction and demo of the door opening experience for the first user groups enhances the user satisfaction with the solution.

Although the Mobile Access App contains animations within the **Help** menu for entrance access using, Tap, Twist and Go, and Smartwatch, it is recommended that the following is also provided:

- Make users aware of the NFC antenna in their mobile device when using Tap mode with NFC. Depending on mobile device model, the NFC antennas are placed in different areas of the mobile device.
- Provide information on which doors have been set up for Tap, which for Twist and Go and which doors have not yet been set up for Mobile Access.

For additional information refer to the documents and instructional videos listed in *Section 1.4 Reference material*.

4 General information

4.1 The role of the Access Control System

The role of the Access Control Systems does not change with HID Mobile Access®. The Mobile Identities Service in the HID Origo™ Management Portal allows issuing and revoking Mobile IDs, in a similar way to a card printer or card encoder today. Once a Mobile ID has been issued to a mobile device, the access rights for the Mobile ID must be set within the Access Control System in a second step. This also enhances the security of the solution.

4.2 Extending the Service

As soon as you have been through the Onboarding process for HID Mobile Access, you can use the Mobile Access part numbers to order new mobile-enabled readers and additional user licenses. Please ask your supplier to use these part numbers when placing their order with HID Global, refer to the *HID Readers and Credentials How to Order Guide,* (PLT-02630).

When ordering new user licenses your Organization ID and Mobile Keyset reference number will have to be supplied. This information is displayed in the Organization Summary section of the HID Origo Management Portal. The information is also sent to the email address of the Customer Administrator as entered at the time of Onboarding.

4.3 Terminating the Service

Termination of service is possible on an annual basis with a notice period of 30 days to the renewal date of the Mobile Identities Service subscription.

After termination, the enterprise no longer has access to the HID Origo Management Portal to manage Mobile IDs. Any Mobile IDs that have not been issued expire on termination.

Note: After termination, all Mobile IDs will be revoked from the users' mobile devices.

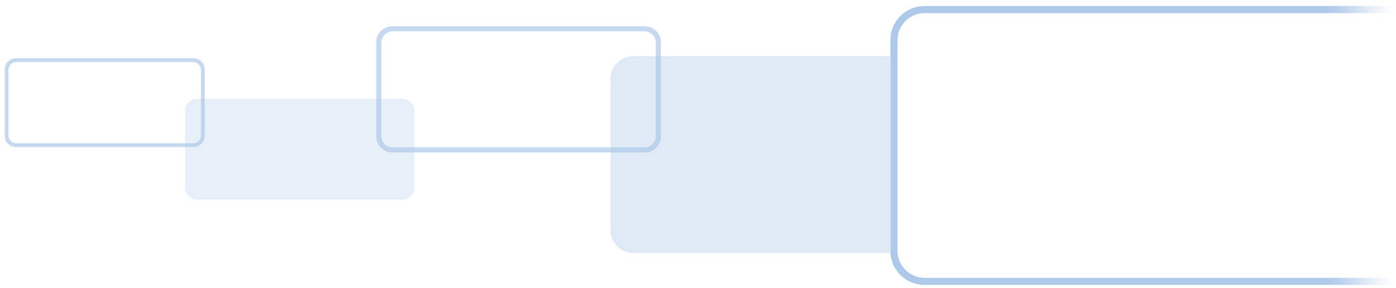
5 Conclusion and future opportunities

We hope you will enjoy implementing and using HID Mobile Access® within your organization.

HID Mobile Access service will continue to evolve, and as an existing customer you will automatically benefit from some of the additional features and functionalities. These include support for new mobile devices and mobile device operating systems, new portal features and functionalities, and security updates to the application.

We will keep you informed of any changes via the HID Origo™ Management Portal.

This page is intentionally left blank.



hidglobal.com