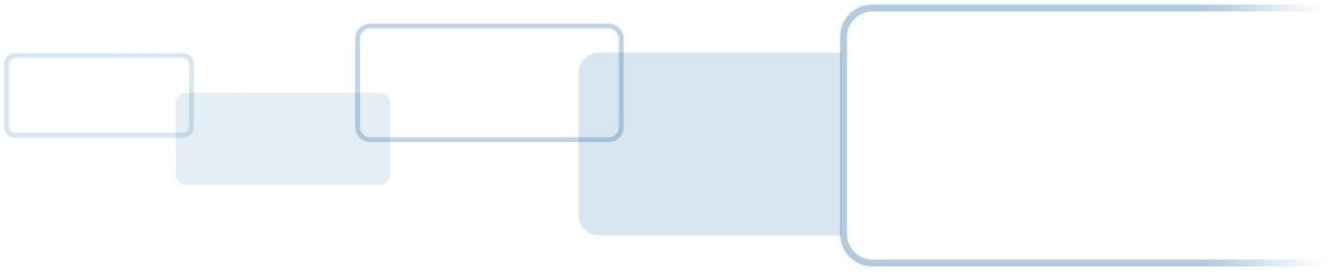
# HID Mobile Access
# Frequently Asked Questions

Support Documentation for Portal Administrators

PLT-02085, Rev. A.13
May 2015



# Contents

## Copyright



## Trademarks

HID GLOBAL, HID, the HID logo, HID Mobile Access, iCLASS SE, multiCLASS SE, and Seos are the trademarks or registered trademarks of HID Global Corporation, or its licensors, in the U.S. and other countries.

## Revision History

| Date | Description | Version |
|---|---|---|
| 10/1/14 | For HID Mobile Access v2.1 | A.11 |
| 5/4/15 | Updated for HID Mobile Access v2.1.3 | A.12 |
| 6/12/15 | Updated for HID Mobile Access v2.1.4 | A.13 |

## Contacts

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


| North America | Asia Pacific |
|---|---|
| 611 Center Ridge Drive<br>Austin, TX 78753<br>USA<br>Phone: 866-607-7339<br>Fax: 949 732 2120 | 19/F 625 King's Road<br>North Point, Island East<br>Hong Kong<br>Phone: 852 3160 9833<br>Fax: 852 3160 4809 |
| **Europe, Middle East and Africa** | **Brazil** |
| Haverhill Business Park Phoenix Road<br>Haverhill, Suffolk CB9 7AE<br>England<br>Phone: 44 (0) 1440 711 822<br>Fax: 44 (0) 1440 714 840 | Condomínio Business Center<br>Av. Ermano Marchetti, 1435<br>Galpão A2 CEP 05038001<br>Lapa - São Paulo/SP<br>Brazil<br>Phone: 55 11 5514-7100 |
| HID Global Technical Support: support.hidglobal.com | |

# 1 General Questions about HID Mobile Access

## 1.1 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 Secure Identity Services portal: A managed service that allows you to manage users and securely issue or revoke Mobile IDs to users' handsets.
- HID Mobile Access App for Android and iOS devices
- iCLASS SE® mobile-enabled Readers
- Mobile IDs with integrated Seos technology for management of trusted identities

## 1.2 What is Seos?

Seos is a technology invented by HID Global as a common standard that establishes privacy and trust in the communication of secure identity data on physical cards, smartphones, tablets and wearables.

The ecosystem of Seos-capable enterprise applications encompasses solutions for a broad and growing range of use cases, including PC login and authentication to IT systems, secure print job collection, automated vending, building access, opening door locks, elevator access, parking access, and time and attendance management. HID Global® continues to expand the open ecosystem of Seos-interoperable products and services.

Seos technology is chip-independent, enabling it to be easily ported across different hardware devices of different manufacturing origin. Importantly, Seos enables a smart device to become a trusted credential, replacing mechanical keys and access cards using communication technologies, such as NFC or Bluetooth Smart, to open doors in homes, hotels, offices, hospitals, universities, and industrial and commercial buildings. Seos technology has been adopted widely and Seos powers HID Mobile Access and the company's iCLASS SE® platform.

# 2 Questions about the HID Mobile Access Portal

## 2.1 How do I allow additional administrators to use the Mobile Access Portal?

If you would like to add additional Portal users, please send an email to SISRequest@HIDGlobal.com with the following details:

Email to: SISRequest@HIDGlobal.com

From: <<FirstName>> <<LastName>>, <<Company>>

| Email Address | Last Name | First Name | Mobile Device | Role* (Admin, Operator, Reviewer) |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |

*see *Section* ***Error! Reference source not found.*** for Role definitions.

## 2.2 How can I reset my HID password?

On the Mobile Access Portal (managedservices.hidglobal.com), enter your User ID and select the Forgot your password? link.
Note: Your User ID is the email address used to create your account.

You will be prompted to correctly answer the two security questions setup when you created your account. A new, temporary password will then be sent to this email address.

## 2.3 Why can't I see the HID Mobile Access web application after I log in to the portal?

Your login identity has not yet been granted access to this Service. Your application and account setup is 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 contact technical support: http://www.hidglobal.com/support.

## 2.4 What roles are available in the portal?

The HID Mobile Access portal is role-based. A description of the privileges for each Portal Administrator role for a particular company or institution are listed here:

| Portal Administrator Role | Functional Abilities |
|---|---|
| Administrator | • Configure reporting and notification settings<br>• Change the description and background image for the corporate badge<br>• Edit the invitation email sent to users<br>• Full edit, add and delete privileges to all users<br>• Issue and revoke Mobile IDs and delete mobile devices |
| Operator | • Full edit, add and delete privileges to all users<br>• Issue and revoke Mobile IDs and delete mobile devices |
| Reviewer | • Read only privileges to user data, devices and Mobile IDs |

## 2.5 Which browsers are supported by the HID Mobile Access Portal?

The following browsers have been fully tested with the HID Mobile Access Portal:

- Internet Explorer 9.x, Internet Explorer 10.x
- Chrome 37.0.2062.120 m
- Firefox 32.0.1
- Safari 5.1.7

# 3 Questions about the Mobile ID

## 3.1 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 unique to each device so that they cannot be copied. If a user switches devices, a new Mobile ID must be issued. To view the number of Mobile IDs you have available, hover the cursor over the corporate badge image on the main screen of the portal.

## 3.2 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.

Note: Look up the HID item number (part number) to speed up the process. The HID item number can be obtained in the portal by hovering over the corporate badge on the main screen

## 3.3 Is a Mobile ID more secure than a physical card credential?

Mobile ID is more secure than legacy access cards without processing capabilities. Mobile ID includes modern and well established security features to session key, non-reputation and non-reply attacks etc.

The nature of mobile usage also ensures higher security. If an employee loses their physical card it can be used by anyone. The loss of a mobile device is usually noticed and reported very quickly, but until then, the passcode protects the Mobile ID. Through the HID Secure Identity Services Portal, you can revoke the Mobile ID if the device still has coverage and disable the Mobile ID in the Access Control System.

## 3.4 How many Mobile IDs can be issued to a device?

- Up to five devices to each user profile
- Up to ten Mobile IDs per device

## 3.5 Can the Mobile ID be transferred to a new device?

For security purposes a Mobile ID cannot be transferred and/or used on another device. If a user use 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 replace the Mobile Ids numbers in the Access Control System.

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

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

## 3.7 What if I factory-reset my device, or uninstall the HID Mobile Access App?

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

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

# 4 Questions about the HID Mobile Access App

## 4.1 Where do users download the HID Mobile Access App?

The App can be downloaded from either the *iTunes App Store* or *Google Play Store* depending on the device. However, it makes sense for the end user to wait for the invitation email from the portal before downloading, as this contains links to the correct download area, including the registration code necessary for setting up the App.

.

## 4.2 Which mobile devices and operating systems are supported?

| Operating System | Verified Device Models |
|---|---|
| iOS 7+ with Bluetooth 4.0 | • iPhone: 4S, 5, 5C, 5S, 6S, 6S Plus<br>• iPAD: Air, Mini, 3rd & 4th gen |
| Android 4.3 with Bluetooth 4.0<br>Android 4.4 with Bluetooth 4.0 or NFC (Host Card Emulation) | • Google Nexus 5, Nexus 6<br>• Samsung Galaxy<br>  ○ Note 3, Note 4<br>  ○ S4, S4 Plus, S5, S6<br>• Sony Xperia Z2, Z3<br>• HTC One |

Note: Devices are added on a continual basis as demand warrants. There may be regional differences in device operability, as operating system versions are pushed at different times in each region.

## 4.3 Does HID Mobile Access work without network coverage?

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

## 4.4 Does HID Mobile Access work without 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.

## 4.5 What impact does HID Mobile Access have on battery life?

The mobile device and the reader communicate with each other using either BLE or NFC. Both communication 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 synching.

If the Mobile ID Protection option is disabled in the iOS app, then *Location Services* will be required on the device. This will have a minor impact on battery life.

## 4.6 Does the App collect private data?

We collect limited information like mobile device push ID, mobile device model and OS version, to offer

the service and provide technical support. Details of what data we collect are listed in the Privacy Policy users accept during the App installation process. Location data, such as GPS geocodes, is not collected.

## 4.7 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, as long as 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.

## 4.8 Why does the reader not recognize my App and Mobile ID?

To initially troubleshoot mobile device/reader connection, check that the following are in order:

- 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 into the Access Control System
- That 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
- If you are using NFC readers: You have a supported Android device, and NFC has been enabled on the device
- That the HID reader works with a traditional access credential.

If all of this is in order, 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.

## 4.9 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”.

## 4.10 What happens when there are multiple readers in range of the mobile device?

The device will communicate with the closest reader.

# 5 Security-Related Questions

## 5.1 Should the user keep the HID Mobile Access App and device software updated?

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 App should be updated when prompted.

## 5.2 What is the security level on the mobile device?

There are multiple layers of security on the mobile device on 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 to protect 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.

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

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, the device is eligible to 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.

## 5.4 What shall I do before reissuing the device to another user?

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

## 5.5 Are there any best-practice policies I should implement within the Enterprise?

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 loss of the mobile device 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. To jailbreak (or root) a device circumvents the built-in security and protection of the operating system, opening up the mobile device for high risk from malware and unsupported uses.
- Mandate the use of passcode or fingerprint scan as additional security mechanism against the loss of a mobile device (setting within the 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.