imprivata®

Product Documentation

Implementation Guide

Imprivata Mobile Device Access®

TOC

Imprivata MDA Implementation Guide

Success with Mobile Device Access

Imprivata MDA extends Imprivata authentication management and single sign–on to mobile devices and apps. The solution helps customers balance security with accessibility and convenience for end users. This is done by giving customers the ability to configure Imprivata MDA to achieve their goals.

While Imprivata knows our software, nobody knows your users better than you do. Every hospital system will find advice that works or does not work for that organization. As you implement Imprivata MDA, you may improve upon what is included in this guide.

As you think through your implementation of Imprivata MDA it is critical to the success of the deployment to think through the balance of security with accessibility to these shared devices and the impact on the daily work of end users and clinician staff. The most important recommendation that this guide can give is to consult with your clinical staff and understand how these shared devices are being used.

NOTE:
Imprivata has a team of professional services and clinicians who are experts in helping to ensure a successful deployment. Your account manager can help you take advantage of these services.

Audience

This document is intended for an IT team in a healthcare setting. The team should include at least the following:

- IT project manager
- Imprivata MDA Implementation Engineer
- Mobile device administrator to perform MDM configuration
- Imprivata Enterprise Access Management (formerly OneSign) administrator
- Clinical staff leadership, to ensure boots-on-the-ground success

Implementation Strategy

Based on Imprivata's experience with many hospitals of varied sizes, we strongly recommend a small, controlled Proof-of-Concept (POC), sometimes also called a Pilot, of a single unit or a handful of units before scaling to dozens or hundreds of sites. If possible, test your configuration with a group of real users in a real environment. Customers have often struggled after conflating an evaluation with a POC.

The difference between an *evaluation* and a *POC* is significant. These terms can be used differently across organizations.

- An evaluation is performed within an IT lab setting and is very controlled with the goal of understanding how a solution works technically.
- A POC (or pilot) takes the work done during an evaluation and is implemented and used in a real-world environment with end users, with the goal of understanding how the solution will impact the daily work of end users and its performance in production.

Often what works perfectly in a lab IT environment does not perform well in a real world, clinical environment. A well planned POC will help ensure success that scales across your organization.

Before You Begin

It is critical to the success of your Imprivata MDA implementation that the ecosystem of hardware and software is supported.

Review the following checklist before implementing Imprivata MDA. For more information on supported apps, workflows, and mobile operating systems, see https://www.imprivata.com/applications-supporting-mda.

- Identify and select the mobile devices compatible with Imprivata MDA
- Identify and confirm the mobile operating system that supports Imprivata MDA:
  - **Android 15** – Imprivata MDA 7.15.1 and later
  - **Android 14** – Imprivata MDA 7.13.4 and later
  - **Android 13** – Imprivata MDA 7.12 and later
  - **Android 12** – Imprivata MDA 7.8 and later
  - **Android 7 through 11** – All Imprivata MDA releases
- Identify and select compatible badges that support the 13.56 MHz MIFARE NFC Frequency.

> **NOTE:**
> Mobile devices leverage NFC Technology, which is 13.56 MHz MIFARE NFC Frequency.

- Imprivata MDA requires that you select a Mobile Device Management (MDM) software suite to deploy Imprivata MDA. For a list of supported MDMs, see the Supported Components.
- Identify the apps that you intend to use on your mobile devices and confirm they support an integration with Imprivata MDA.
- Confirm that your Imprivata Enterprise Access Management release is still supported by Imprivata. For more information on maintained Imprivata Enterprise Access Management releases, see the Imprivata Environment Reference.
- Perform the tasks to configure Imprivata MDA, including:
  - Import the Imprivata mobile app profiles. See "Enabling Imprivata MDA and Deploying Profiles" in the Imprivata MDA online help.
  - Configure the mobile policy in the Imprivata Admin Console..
  - Deploy the Imprivata MDA app to your devices and configure application-specific settings.

NOTE:
Any implementation is a living thing. New devices, new operating systems, and new apps are expected over time.

If during this pre-implementation evaluation, or after your implementation is live, you come across something not yet supported, Imprivata is willing to help you and be a partner for your success. Reach out to your account team to engage with our Product Management and Business Development teams to help.

About MDMs

A well-configured MDM system is required for the success of your implementation. Imprivata MDA is available in the Google Play Store and can be downloaded and distributed to your mobile devices using Mobile Device Management (MDM) software. Your implementation of Imprivata MDA must be configured for the MDM that you are using.

As of this writing, the following MDMs and their configurations have been qualified for integration with Imprivata MDA:

- Omnissa Workspace ONE UEM
  - Shared Mode Configuration with WMware Launcher
  - Dedicated Mode Configuration with WMware Launcher
- Microsoft Intune
  - Fully Managed Configuration with Microsoft Launcher
- SOTI MobiControl

About Badges

If you are an existing Imprivata Enterprise Access Management customer, the badges currently deployed may not support the necessary NFC frequency required by the mobile devices. Mobile devices leverage NFC Technology which is 13.56 MHz MIFARE NFC Frequency. If your current badges do not support this frequency, there are two options available:

- Replace existing badges with new badges that support dual frequency (both 125 kHz and 13.56 MHz).
- Use stickers (sometimes called “pucks”) which can be attached to a badge to allow for 13.56 MHz frequency to be read.

About Apps

Imprivata MDA helps users access their apps quickly and seamlessly, making it easy to get their work done. It is vital for your Imprivata MDA implementation to ensure that the apps you intend to deploy on your mobile devices support an integration with Imprivata MDA.

After a user has authenticated to the device with their Imprivata Enterprise Access Management credentials, Imprivata MDA leverages the user's EAM credentials (username/password) to access the provisioned apps.

There are three key use cases that Imprivata MDA supports with app vendors:

- **Login** – sign in the user into the app
- **Logout** – sign the user out of the app
- **Notifications (including voice)** – allow notifications to be displayed on the phone

For your implementation of Imprivata MDA, only deploy apps whose integrations have been certified with Imprivata and our app development partners. Some of the key apps which support an integration to Imprivata MDA include:

- Epic Rover
- TigerConnect
- Mobile Heartbeat
- Halo Health
- Zebra Workforce Connect

> **NOTE:**
> For the most current information on supported devices, applications, and workflows for Imprivata MDA, see https://www.imprivata.com/applications-supporting-mda.
>
> If you do not see an app listed, reach out to us! Our business development and product management teams are constantly working to add more apps to our ecosystem and are happy to work with vendors to guide them on how to integrate their app to Imprivata MDA.

Imprivata MDA Recommended Configuration

Imprivata MDA offers different activity timeouts to help ensure a mobile device is not sitting around unlocked, allowing unauthorized access to PHI and other data.

The following configuration is intended to address two key areas for Imprivata MDA customers and their end users:

- Balancing usability with security. The goal here is to optimize the use of inactivity timers to balance the security of a device with the end user experience.
- Allowing notifications to come through for all apps, including clinical notification apps that have not integrated Imprivata MDA support (e.g. alerts and voice calls). The goal is to allow notifications to be displayed while still maintaining required security policies for devices. For more information about Android alerts, see About Android Alerts.

This configuration of Imprivata MDA recommends the use of an important feature called Countdown to Lock. Countdown to Lock was designed to help our customers balance security with convenience. A key difference between the countdown to lock feature and the standard Imprivata MDAinactivity lock is that the Countdown to Lock feature allows your organization to use the native Android lock screen.

Countdown to Lock is a method of re-verification, ensuring that after a certain time period (ex. 4 hrs.) an end user will receive a notification asking for the user to renew their session prior to locking the device. Countdown to Lock is a setting that is customizable by a customer as to the time period (e.g. 2, 6, 12 hours) that a user would receive this notification.

IMPORTANT:
Countdown to Lock interacts with other inactivity and logout timers that can be set.

It is critical to think through the end user experience when deciding how to leverage these timers. Striking the right balance of security versus usability will help ensure that your mobile device investment is achieving its goals.

It is recommended to work with your clinical end users and observe and understand the impact of these timers on workflows. Taking the time to do this prior to your go-live will set your organization up for success.

About Inactivity Timers

Consider the following information regarding the various inactivity timers that affect Imprivata MDA.

Item	Description
Countdown to Lock timer	The timer for the Countdown to lock feature. Configured through the **CountdownToLockMinutes** AppConfig parameter in Imprivata MDA.
Imprivata MDA timer	The Imprivata MDA inactivity timer. This timer is independent of the Countdown to Lock timer. Configured through the Imprivata Admin Console**> Computers > Mobile Policy >Inactivity re-authentication** setting.
Android screen timeout	The native Android screen timeout Configured through your MDM.

Recommended Configuration for Imprivata MDA

The following inactivity timers should be configured for your implementation of Imprivata MDA:

- The Countdown to Lock timer
- The Android screen timeout.

  IMPORTANT:
  The Android screen timeout is required for the configuration.

- The Imprivata MDA inactivity timer

IMPORTANT:
The Android screen timeout threshold should be shorter than the Imprivata MDA inactivity timer, ensuring that the Android lock screen will allow the display of notifications.

For example, if your organization sets the device's inactivity timer to 10 minutes, set the Android screen timeout to 05:00 minutes, and the Imprivata MDA inactivity timer set to 10:00 minutes.

- The Imprivata MDA logout timer
- Any app-specific timers

IMPORTANT:
These timers are specific to an individual app and are not controlled by Imprivata MDA. However, they can still impact user experience. It is important to consider the use of these app specific timers when used with Imprivata MDA timers.

For example, the Epic Rover inactivity timeout is not controlled by Imprivata MDA, but still will affect the end user experience.

Example — Inactivity Timer Configuration

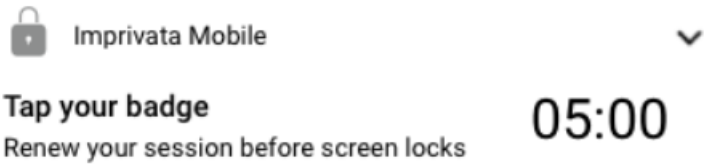
In this example, inactivity timers are configured as follows:

- **Countdown to lock timer:** 12 hours
- **Android screen timeout:** 1 minute
- **Imprivata MDA inactivity timer:** 5 minutes
- **Imprivata MDA logout timer:** 1 hour

Workflow

The following describes the workflow using the example inactivity timer settings above.

- It assumes a clinician is starting their shift for the day that will last 12 hours.
- The Imprivata MDA logout timer is set to 1 hour because the site has decided that a user who has not used the phone for 1 hour should be logged out. If you would prefer users to remain logged in for longer with no phone activity in order to continue receiving calls and notifications, this timer is fully configurable.

	**7:00AM** - At the start of a shift, a user selects a device and swipes up on the native Android lock screen. • The user signs into the device using Imprivata MDA by tapping their badge against the mobile device. • At this point, the Countdown to lock feature is invoked and remains silent until the Countdown to lock countdown time elapses. • During this time, if the user actively uses the phone, they are not presented with any lock screens until the 12-hour threshold.
	If the user is not using the phone during the shift (i.e. there is no activity) the following occurs: • At one (1) minute, the Android screen is displayed. At any point, the user can swipe up on the Android lock screen and gain access to the mobile device. Their user activity on the device and apps will remain. • When the device remains inactive for five (5) minutes, the Imprivata MDA lock screen is invoked. At this point, the user can regain access to the device by tapping their badge against the device. Their user activity on the device and apps will remain. • If the device remains inactive for an hour, then Imprivata MDA will log out the user from the device. The user activity on the device and apps will not remain.
	**6:55PM** - As the Countdown to lock time approaches the 12-hour threshold, and before the Countdown to lock timer expires, a reminder screen displays:  The user can interact with the reminder by tapping their badge to renew the session or to log out.
	After the countdown timer expires, the user is prompted to tap their badge to renew their session. No work will be lost if the same user authenticates.

The Countdown to Lock screen lock only occurs under the following conditions:

- When the user taps the Imprivata MDA app icon.
- When the countdown timer expires.
- When the user logs out of Imprivata MDA by using the **Log out** button accessed from the countdown notification.
- When a new user taps into the device.
- When the device reboots.

About Android Alerts

Imprivata MDA supports app notifications that adhere to Android standards for notifications. Some app developers will use a non-standard way or custom notifications. Imprivata MDA does not support

third party app notifications that use custom views or overlays to customize notification UI. Imprivata MDA does support notifications with standard title, text, subtext, notification actions as well as notification category set to Android SDK defined strings.

For more information on Android alerts, see the Android developer documentation for standard Android notifications and custom notifications.

Contacting Imprivata

20 CityPoint, 480 Totten Pond Road, 6th Floor

Waltham, MA 02451 USA

Phone: 781-674-2700

Toll-Free: 1-877-OneSign

Fax: 1 781 674 2760

Support: 1 800 935 5958 (North America)

Support: 001 408-987-6072 (Outside North America)

https://www.imprivata.com

support@imprivata.com

Copyright and Legal Information

Trademark Information

Legal Notices

Document revision