imprivata®

Product Documentation

Implementation, Maintenance, and Best Practices Guide

Imprivata Mobile Access Management

Last Updated: April 29, 2025

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

Table of Contents

Introduction

Purpose

Imprivata Mobile Access Management (formerly Imprivata Mobile Access Management) Check Out is Imprivata's tool for shared device accountability, management, and login acceleration. Based on years of experience, this topic is intended to help our customers successfully roll out and maintain Mobile Access Management (MAM) for daily use at hundreds of locations. Imprivata does this by setting expectations, identifying needed resources — both hardware and human — and documenting the best practices we have observed.

As you implement MAM, you may improve upon what is included in this guide. Imprivata encourages you to send us ideas and feedback to make this guide more useful for others in the healthcare community.

Before You Begin — Strategy

The key to a successful MAM implementation is preparation. This section will help you understand the questions and decisions you need to make before rolling out the solution.

Identify Decision Makers

As with any clinical or IT project, it is important to clarify who is going to be responsible for each aspect of supporting MAM. In particular, you need to clarify who will have the following roles. In your organization a single person or group may serve multiple roles.

- **Imprivata Mobile Access Management Administrators** – Configure and support of the overall MAM solution including the MAM console, Launchpad software, and Locker app on the mobile devices. Administrators will also support the device management piece of MAM operationally, utilizing the MAM dashboard to ensure mobile devices have a healthy MAM heartbeat.
- **Mobile Device Management (MDM) Administrators** – Manage mobile device systems that allow remote management of the devices and software settings, including monitoring compliance and enforcing policies. They own keeping the operating system, apps, and settings up to date.
- **Launchpad Workstation Support** – Maintain the Launchpad workstations including ensuring the operating systems, firmware, and settings stay up to date.
- **Smart Hub Support** – Maintain the physical and technical components of the Smart Hubs, including firmware updates, and ancillary hardware (USB cables) and supporting breaks and returns.
- **Mobile Device Owners** – Ensure there are enough mobile devices in each location. They will utilize the MAM console to identify overdue devices, devices placed in the wrong station, or missing devices and are responsible for following up on these devices.
- **Imprivata Enterprise Access Management** (**Imprivata OneSign**) **Administrators** – Ensure end users are in the right policy, providing information for the integration, and supporting the app profiles that enable Autofill.

- **Security Stakeholders** – Responsible for decisions related to the security posture of the devices and apps on the devices.
- **End User Stakeholders** – Responsible for understanding, validating, and supporting the end user workflows as well as the locations of the charging stations. If this is a clinical environment, they ensure clinical representation such as nursing and clinical informatics is included.
- **Network Administrators** – Ensure that Ethernet ports are open, the Wi-Fi connectivity is stable, and all firewalls are opened as necessary.
- **Training** – Responsible for training end users on how to utilize the MAM system to share mobile devices during implementation as well as incorporating it into new employee training.

Identify Shared Mobile Device Users

MAM integrates with Imprivata OneSign to allow seamless checkout of devices and autofill of apps. It is important to identify your users ahead of beginning your implementation to ensure they have what they need:

- Identify all named users that will need to share a mobile device.
- Ensure all named users are licensed for Enterprise Access Management (EAM).
- Validate departments are utilizing EAM tap solution today.
- Create an enrollment and training strategy for users or departments that are not currently utilizing EAM.

Communicate with Users

Communicate with users that MAM will be rolled out to support shared mobile devices and provide an overview of what they can expect. Continue to communicate with users during each phase.

Define Your Mobile Strategy

MAM is one component of your overall shared mobile device strategy. Below are mobile device strategy considerations that can impact the success of MAM and should be reviewed before adding MAM.

- Mobile device apps
  - What apps are required for end users to perform their job?
  - Vet only the required apps to ensure a simple solution for end users and supportability.

    The minimum number of apps required should be deployed to ensure a simple solution for end users, increase supportability, and reduce attack surfaces.
  - Identify whether an app requires automated logout capabilities. For more information, see the Imprivata App support page.
- Security
  - MAM enables devices to be shared with individual passcodes.
  - Establish passcode requirements that align with your security posture. The Health Insurance Portability and Accountability Act (HIPAA) requires encryption for any device that stores or

processes any of the 18 categories of personal health information (PHI).

- Understand app level timeouts and PINs. Review whether these are necessary, now that a device level passcode is enabled.

- Wi-Fi or Cellular Network
  - Introducing mobile devices requires constant connectivity. Ensure your Wi-Fi or cellular network strategy will support this 24 x 7 need.

Additional Resources

Imprivata has resources to assist customers with the implementation and support of this critical service. Your Imprivata account manager can provide more information on any of the following.

- Imprivata Mobile Access Management online documentation and knowledge base
- Imprivata Mobile Access Management Product Certification to ensure your team understands both basic and advanced features of your product
- Imprivata Advanced Management Services to provide dedicated, experienced, remote administration of your Imprivata Mobile Access Management system
- Imprivata Professional Services for remote and on-site assistance to set up and scale your implementation
- Customer Success Management to provide a close partnership covering all your Imprivata products

Change History

Version	Date	Description
4.0	September 2024	Update "Dashboard" section. Add "Audit Logs" section.
3.0	September 2024	Update "Maintenance" section.
2.0	July 2024	Add new sections for "Before You Begin — Strategy". Remove the "Audience" section. Update the "User Experience" section to "Settings" Add new section for "Deployment"
1.0	June 2024	Initial release of the guide

Components

NOTE:
Use the information in this guide in conjunction with the MAM system requirements.

The Imprivata Mobile Access Management (formerly GroundControl) solution integrates multiple first-party and related components:

- MAM Console
- your MDM system
- Imprivata Enterprise Access Management (Imprivata OneSign)
- MAM Launchpad on Mac or Windows computer
- Smart Hubs
- proximity card readers
- iOS and Android devices
- the Imprivata Locker app for iOS and Android
- Wi-Fi and network

MAM Console

Imprivata Mobile Access Management is a hybrid system with a cloud-based SaaS management console.

By default, MAM uses a traditional username and password for login. Imprivata recommends that you instead opt for SAML login, which reduces risk by keeping no passwords within the MAM cloud. Your organization is then able to enforce all authentication requirements. SAML is available for both shared and dedicated environments.

MAM requires each console administrator to be assigned a role. Review the role documentation to select the most appropriate role for each of your administrators.

MDMs

A well-configured mobile device management (MDM) system is critical for MAM to work as expected.

Imprivata Enterprise Access Management (Imprivata OneSign)

MAM's Check Out feature requires customers to integrate with Imprivata Enterprise Access Management as the web service to handle the translation of proximity card IDs to user IDs.

Equipment at Each Location

MAM requires equipment at each location where you will store devices. This includes a Launchpad Mac or Windows computer, a proximity badge reader, and a Smart Hub.

Launchpad on Mac or Windows Computer

The Mobile Access Management *Launchpad* software for Mac or Windows computers receives instructions from the MAM Server in the cloud, and reacts to device connections and proximity card taps.

- Each location with devices requires its own Mac or Windows computer. The computer must meet all system and networking requirements.
- Perform load testing on a Launchpad computer before deciding which Launchpad model you will use.

  Add all devices to the dock for load testing.
- Ensure your Launchpad computers are completely standard, using the same model, same Smart Hub, same USB cables, same mobile device models, and even the same cases. Differences in configuration will guarantee future headaches.
- Smart Hubs must always be connected directly to the Launchpad computer.
- For best performance, MAM requires a 1 to 1 connection between the Launchpad and the Smart Hub:
  - MAM does not support the daisy-chaining of hubs.
  - MAM does not support connecting more than one Smart Hub to a single Launchpad.
- The Launchpad computers require a stable 24 × 7 network connection via Ethernet.
- Hot Spot functionality should be turned off on Windows computers that host the Launchpad software because it can cause network connectivity issues.
- To scale for expansion, you should prepare your installation process. Imprivata supports automated Launchpad installation and registration, using systems such as UEM, SCCM, and Jamf Pro.

Set Up Launchpad Computers for Unattended Use

Whether you choose Mac or Windows computer, the systems must be set up for unattended use.

Imprivata requires that each Launchpad computer is a headless system, with no display, mouse or keyboard. Users should not be logging into these computers for any other purpose.

Launchpad and Smart Hub Monitoring

Launchpad computers and Smart Hubs are expected to be running 24 hours a day. The Launchpad Monitoring feature will help maintain that availability. Ensure the following:

- Turn on **Launchpad monitoring** and configure the alerts to provide a notification to supporting groups in your organization.

- Define a group of admins to receive the Launchpad alerts.
- Set the notifications to notify admins 15 minutes after a Launchpad disconnects, and 15 minutes after a Smart Hub disconnects.

- **Restart monitored Launchpads daily** - set to 4 AM daily or consider your organization's shift change schedule and specify a quiet time.

In the MAM console, go to **Admin > Launchpads > Launchpad Monitoring**.

Smart Hubs

The Smart Hub is a critical infrastructure component. Imprivata sells specific models that we have tested and which function reliably for demanding environments.

For more information on supported Bretford and Datamation Smart Hubs, see the system requirements.

BEST PRACTICE:
Smart Hubs have upgradable firmware.

Install the most current supported firmware, which will ensure you have support for current mobile devices.

MAM reports the Smart Hub firmware version in the Launchpad view of the MAM console.

Proximity Card Readers

Each Launchpad computer used for Check Out workflows requires a proximity card reader.

- Only certain proximity card readers are supported. See the system requirements.
- Plug the proximity card reader into an Imprivata Enterprise Access Management workstation for configuration and then unplug it. Repeat the process for all proximity card readers.
- Affix proximity card readers consistently using interlocking tape in locations that are easily accessible to end users, ensuring proper cable management to minimize the risk of tangled or obstructed cords.

Mobile Devices

iOS and Android devices must be running a supported operating system version. iPhones and iPads are supported as DEP and non-DEP devices.

Imprivata Locker App for iOS and Android

The Imprivata Locker app manages device sign in and out, and locks down the device between users. The Imprivata Locker app is required for Check Out customers and must be installed by your MDM solution.

Device Cases

- Imprivata recommends simple silicon cases.
- Imprivata does not support battery cases with data passthroughs.

Device Cleaning

For device cleaning recommendations, see your device manufacturer's recommendations and consult your organization's infection control best practices.

Wi-Fi and Network

For information on Wi-Fi and Network requirements, see the system requirements.

Configuration and Validation

Implement the following best practices to improve the interaction of end users and their devices.

> **NOTE:**
> Use the information in this guide in conjunction with the MAM system requirements.

Settings

The following best practices pertain to configuring settings in the MAM console for various features and functionality.

Check Out

Consider the following best practices when implementing device Check Out Workflows:

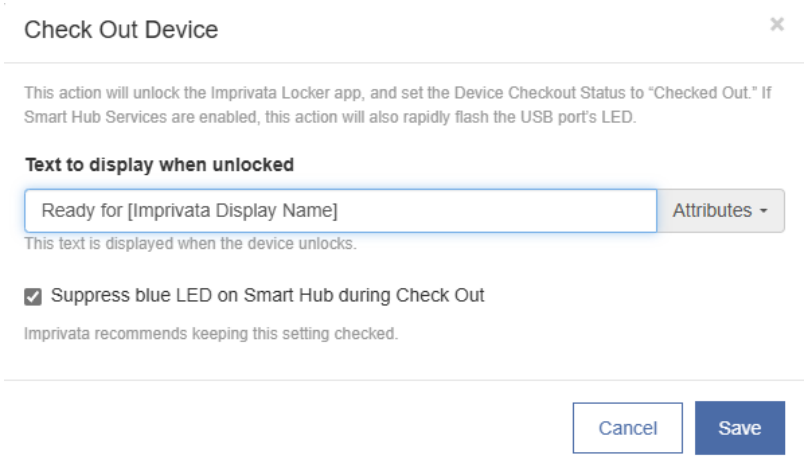
Device Passcodes

Imprivata recommends that you use devices passcodes to secure the devices, and that you set device passcodes to four (4) digits. For more information, see "Clearing Passcodes" in the Imprivata help.

Display the User's Name on the Device at Check Out

Imprivata recommends displaying the user's name on the device at check out, which is stored in the built-in Attribute **Imprivata Display Name**, when you are using Imprivata Enterprise Access Management (Imprivata OneSign).

- In your Check Out Workflow, in the Check Out action, set the text to display to "`Ready for [Imprivata Display Name]`", or something similar.



> **IMPORTANT:**
> Do not use the **[Device Checkout Status]** attribute for unlock text.

Lock Screen Display Text

Imprivata recommends setting the device lock screen embedded display text to include:

User: [Device User]

Property of <customer>
Please return to: [Device Home] before the battery runs out!

- For iOS devices, in the MAM admin console, go to **Workflows >** add an action to **Set Wallpaper**, and specify the information in the **Lock Screen Text & Color** section. For more information, see "Set Wallpaper" in the Imprivata help.

Lock Screen Display Image

Imprivata recommends using a marketing-approved color or image as the device's lock screen background, with a resolution appropriate for the specific device type.

NOTE:
Setting the lock screen display image requires specific Workflows for each device type.

Authentication Method — Network Username and Password

Imprivata recommends selecting the network username and password as an additional available authentication method. Using network username and password as an authentication method allows users to check devices out in the event of a Smart Hub or proximity card reader malfunction, as well as when they forget to bring their badge to work.

When enabled, the Imprivata Locker app lock screen adds a button to unlock the device with a network username and password.

In the MAM console, go to **Admin > Check Out > Available Authentication Methods**.

Suppress the Blue LED at Check Out

On some Smart Hubs, the standard blue LED may confuse users who try to remove the device before the device is unlocked.

Imprivata recommends that you use one of the following options to suppress the blue LED:

- As part of a Check Out Workflow. The Check Out Workflow, by default, suppresses the blue LED. Imprivata recommends that you keep this setting.
- For all Workflows, at the Launchpad level.

Device Checkout Limit

Imprivata recommends specifying the maximum number of devices allowed to be checked out by a user.

- Set the maximum number allowed to be checked out to the maximum number of devices a user may be required to use concurrently, plus one.

Example

A user requires an iPad for interpreter services, plus an iPhone for other workflows.

In this scenario, set the maximum number of devices to three (3).

Allowing the extra device ensures that devices are checked in, while still allowing a buffer of one device when a user needs to check out a new device mid-shift (this may be due to low battery or technical imperfection).

- Define a process to handle when a user has reached the maximum number of devices, and needs to check out a new device.

In the MAM console, go to **Admin > Check Out > Number of devices users are allowed to check out**.

Overdue Devices

Checked out devices can become overdue when they aren't returned to the Smart Hub within a certain length of time. You can configure MAM to identify devices that haven't been returned within the expected timeframe.

- Overdue devices are marked as such in the MAM admin console.
- MAM can trigger Lost Mode to lock down the device over the air, with a message of your choice, when using an MDM that supports it.

Imprivata recommends that you use the Overdue devices feature.

- Turn on the **Overdue Devices** setting.
  - Set the device **Lending Period** to the longest organizational shift hours **+ 1 hour**.

Example

For a 12-hour shift, set the device **Lending Period** to **13** hours.

This provides a 1-hour grace period for the user to return the device.

In the MAM admin console, go to **Admin> Check Out > Overdue Devices**. For more information, see "Overdue Devices" in the Imprivata help.

MAM automatically removes Lost Mode when the device is returned (checked in) to any Launchpad.

Emergency Unlock PINs

The Imprivata Locker app includes a feature that allows the user to unlock the device during emergencies when the network or other components may be unavailable. Imprivata recommends that you:

- Configure an Emergency Unlock PIN in your MDM via AppConfig.
- Have a documented process for dealing with downtime.
- Identify a process for rotating out the emergency unlock PINs in-use after a downtime event.

For more information, see "Configure an Emergency Unlock PIN" in the Imprivata help.

Configure Device Home

For every mobile device, designate a **Device Home**; this is the location the device is expected to connect to on a regular basis.

When a device is returned to a Launchpad other than its assigned Device Home, the device is considered in the wrong location and is counted as such on the Dashboard.

- Ensure the Device Home naming convention follows your organization naming standards.
- The most efficient way to set the Device Home on a large pool of devices is by uploading a CSV file of the devices.
- Set a device's Device Home once. It should not be changed via automated Workflows.
- In the MAM dashboard, use the **Device in Wrong Location** tile to identify the devices.

In the MAM console, go to **Admin > Dashboard > Device Health > Device in wrong location**.

Listing Checked Out Devices

By default, MAM will not show devices within the console as soon as they are unplugged.

Imprivata recommends listing checked out devices, in order to identify the users at any given moment.

MAM allows the display of checked out devices in three ways:

- In the MAM console, within the Launchpad detail.
- In the Launchpad display. Add "Device Checkout Status" and "Device User" to the Launchpad Display View.
- For iOS devices, on the device itself, an option enables a bookmark on each checked out device. iOS displays this bookmark as an app named "Checkouts" on the device home screen.

  These lists are always grouped by Launchpad. This feature helps each team manage its own pool of devices, without needing to see the entire population of devices at your organization. Each device has a Device Home Launchpad, and devices are expected to return to that Launchpad each day.

> **NOTE:**
> The ability to display checked out devices using a Safari bookmark is not compatible with the iOS Express Checkout workflow model.

App Integration - Sign In and Sign Out

Password AutoFill

MAM supports Enterprise Password AutoFill on iOS devices and Autofill Services on Android devices. The system leverages the power of Imprivata Enterprise Access Management (OneSign) to autofill passwords into most apps and web sites. In many cases, the system can also fill usernames.

> **NOTE:**
> Password AutoFill is not single sign-on (SSO). Users still need to sign into multiple apps, even though the sign in process is dramatically easier. The Password AutoFill feature does not make any improvements to app logout.

Signing Out of Apps

In some cases, your users will need to manually sign out of apps before checking in the device at the end of the day. If they do not sign out:

- Apps may continue to send push notifications to the device.
- Back-end systems may continue to show the user as “available” after they have left.
- The device’s next user may have access to data pertaining to the previous user.

Imprivata is working to improve the sign in and out user experience, and has introduced technologies such as Universal Link Callbacks. We encourage you to speak with your app vendors to learn about their plans to support ULCs for logout from shared devices.

Check In

The Check In Device Workflow action launched the Imprivata Locker app and locks the device.

To check in devices, your users connect the devices to the Smart Hub.

Check In Workflows for iOS Devices

In your Check In Workflows for iOS devices, Imprivata strongly recommends setting the option to **Launch a blank page before Check In**.

This action ensures the Imprivata Locker app is not foregrounded at the start of check in, increasing reliability.

Handling Check In / Check Out Workflow Failures

- **For Check In:** Configure an **On Failure** Workflow action for Check In and set the number of attempts to retry the Workflow to **3**.
  - Configure a Workflow action to run after the number of failures are exceeded.
- **For Check Out:** Configure an **On Failure** Workflow action for Check Out, but do not include the **Retry this workflow** setting.

  Instead, configure the setting **If still failing, run another workflow**, and select a **Check In** Workflow.

Device Battery Health

Imprivata strongly recommends that you train your end users to return the device to the Smart Hub when the device displays a low battery notification.

> **CAUTION:**
> If the user returns an iOS device with a dead battery to the Smart Hub, and thus the device cannot be unlocked, the device will need to be recovered in the MAM system.
>
> This could also result in the user not being able to check out another device if they are over their device checkout limit.

User Acceptance Testing

Because this is a new workflow for end users, user acceptance testing is a required part of implementation. Successful User Acceptance Testing (UAT) will include:

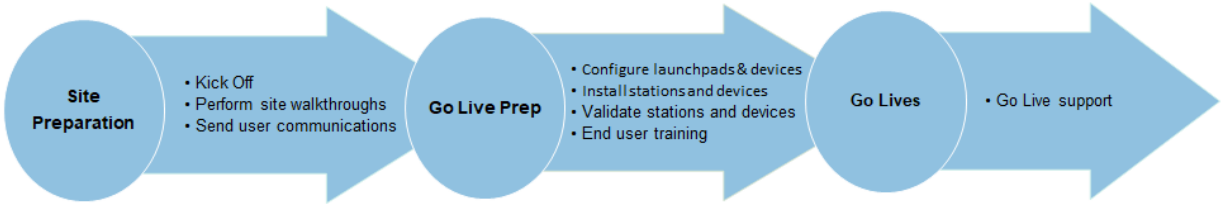
- User representation, including clinical informatics, if this is a clinical environment
- At least two Smart Hubs with full connectivity and configurations
- At least three (3) mobile devices in each Smart Hub
- Imprivata Enterprise Access Management (Imprivata OneSign) and app level user access for testers

Have end users follow a script to ensure all workflows are in working order and solicit feedback including:

- Initial Badge Check Out
- Initial Manual Check Out
- Creation of passcode
- Autofill of all apps in scope
- Check In
- Badge and Manual Check Out for previously checked out device
- All beep tones (Unenrolled badge, no mobile devices available, check out limit reached)

Deployment

Each time your organization deploys Imprivata Mobile Access Management Check Out to a new department, the methodology with tasks should be utilized to ensure success. Communicate with end users during each step along the way.



Perform Your Department Preparation Walkthroughs

The physical location of the MAM solution in each department is important. Ahead of each rollout, perform walkthroughs to identify the following:

- Departments that have or will be using shared devices
- Device Count - Define how many devices and Smart Hubs will be needed for each unit, taking into consideration:
  - Maximum number of end users during a shift
  - How many spare devices are needed
- Location of the Smart Hub
  - Ample space – when doing the walkthrough, bring along a cardboard cutout of the Smart Hub and Launchpad setup to ensure there is enough space.
  - In areas with multiple Smart Hubs, separate the Launchpads (as space allows) to prevent bottlenecks during device check in and check out.
  - Consider:
    - Where do end users start and end their shifts?
    - Is the location accessible for all end users to reach and see the devices?
    - Is the location accessible or visible to patients and visitors, and is this a concern?
- Correct and available number of Ethernet drops available and port is turned on.
- Correct and available number of electric ports.
- Validate Wi-Fi connectivity at the location.

Hardware Installation

Hardware should be installed and validated before go live.

Use the following task list to ensure that a department is ready to go live with MAM Check Out. Validating each device as described below will prevent technical issues at the time of go live.

- Smart Hub cables are properly connected to power and launchpad workstation.
- Launchpad workstation cables are properly connected to power and Ethernet.
- Proximity card reader cable is properly connected and affixed to the front of the Smart Hub within easy reach of end users.
- Devices can be easily seen by end users and within easy reach.
- Cable management is tidy and will not interfere with end user experience.
- Smart Hub lights are on next to each device either with a green flashing or green solid light.
- Check out each device via badge tap.
- Perform Autofill for at least one app on each device.
- On each device, in the Imprivata Locker app, click the information icon (next to the Imprivata logo) to display a diagnostics screen with connectivity and device health information. Ensure that the device is in a healthy state.

End User Training

Providing training to your end users is critical to the success of your Mobile Access Management implementation.

Conduct training for your end users, before a department goes live, that includes the following topics:

- Using the Smart Hubs to check devices in and out, with and without a proximity card.
- Understanding the LED status indicators and audible beeps for errors.
- Signing into apps using Autofill.
- Overdue Device settings
- Device check out limit
- The importance of battery health and returning a device before its battery is dead.

It is important to incorporate this training into new employee onboarding as well.

Imprivata's end user training video can be found here.

Imprivata recommends creating additional signage around the docking stations to remind end users of important information.

Go Live Support

Providing support to end users at the time of enabling the system will ensure proper workflows are being followed and the system is working appropriately.

At the time of go live, all Launchpads, Smart Hubs, proximity card readers, and mobile devices are expected to have been validated. Identify Imprivata services, internal go live support, and/or super users that will be support the following go live tasks:

- On the spot training as end users utilize check out, passcode creation, autofill, and check in for the first time.
- Spot checking of connectivity for smart hubs and devices throughout the go live period.

- Reinforcement of correct workflows including:
  - Waiting for a device to be ready before pulling the device during checkout.
  - Creating a passcode immediately following checkout.
  - Checking devices in appropriately and before the battery dies.
  - Spot checking for overdue devices, unpaired devices, and devices moving to the wrong Smart Hub.
  - Rectifying access issues.
  - Identifying configuration issues and following through until resolution.

Maintenance

Imprivata Mobile Access Management (formerly GroundControl) requires care and maintenance to ensure your environment stays healthy and supportable over time. Use the following best practices to create your organization's maintenance strategy.

> **NOTE:**
> Use the information in this guide in conjunction with the MAM system requirements.

Non-production Environment for Testing

- All Imprivata customers have access to a no-fee user acceptance test (UAT) environment for non-production testing of pre-release versions.
- Maintaining a UAT environment can ensure a stable production environment.
- To obtain access to our early release UAT environment, customers can open a ticket at support.imprivata.com. UAT environments are updated ahead of the next release 2-4 weeks before to a Prod release.
- Imprivata also gives access to Locker Apple TestFlight pre-releases for non-production testing, as well as early release Android APKs.
  - Customers may join the TestFlight pre-release by opening the following link from an iOS device, when Apple's TestFlight app is installed: https://testflight.apple.com/join/bU0feGam.
  - To obtain access to the early release Android APK, customers can email mobile@imprivata.com.

Launchpad Updates

Launchpad Workstations

Maintaining your Launchpad workstations will ensure all components function correctly. Ensure your organization has a strategy for maintaining all of the below:

Operating System Updates and Security Patches

- Create a strategy to keep the Launchpad computer operating system at a version supported by MAM. For more information, see the system requirements.

  Ensure that OS update testing includes MAM-specific testing, so that these 24 x 7 workstations are not negatively impacted during an upgrade.

Apple iOS MobileDevice Framework

- Ensure that the Apple MobileDevice Framework on the Launchpad computer is updated before updating to the next generation of iOS on the iOS devices.

- Ensure that the version of Apple MobileDevice Framework is the minimum supported version the iOS device will be upgraded to.

Apple iOS Mobile Device Drivers

- Device Drivers for iOS (Apple MobileDevice Framework) are released alongside each new release of iOS.

  It is imperative to keep this up to date or communication between MAM and the MobileDevice can fail.
- Windows Launchpad workstations can unknowingly overwrite Device Drivers for iOS. To prevent this from occurring, see "About Apple Mobile Device Driver on Windows" and "Devices Do Not Appear On Windows 11 Launchpad" in the Imprivata help.

Launchpad Application

- To ensure a healthy environment, the best practice is to stay within one version of the most recent release of the MAM Launchpad software.
- Uptime of the Launchpad is critical to the performance of MAM.

  For this reason, Imprivata does not recommend using the Automatic Upgrades setting for Launchpads. This allows you to test a Launchpad upgrade on a single machine before upgrading across your enterprise.

  For net new organizations, the Automatic Upgrades setting is defaulted to off.

  In the MAM admin console, go to **Admin > Launchpads > Automatic Upgrades** and ensure that the setting is **OFF**. For more information, see Launchpads.
- Mac Launchpads require specific settings to ensure that automatic Launchpad upgrade works correctly. For more information, see "Launchpad Update and Auto Launch on Mac" in the Imprivata help.

> **NOTE:**
> If you use an automated installation system, then generally you will use the same system to distribute updates to the Launchpad software and Apple Device app or iTunes components.
>
> Create a plan to update the Launchpad software.

Smart Hubs

Firmware Updates

- Ensure that the Smart Hubs have the most current supported firmware installed, which will ensure that you have support for current mobile devices.

  For more information, see "Update Smart Hub Firmware" in the Imprivata help.

Hardware

Create a strategy to routinely inspect and maintain the Smart Hub hardware, for example, during normal rounds. The inspection should include the following tasks:

- Examine and replace physically damaged cables.
- Ensure proper cable management — with cable ties for the Launchpad, Smart Hub, and proximity card reader — to reduce chances of tampering.
- For Bretford Smart Hubs, ensure that the cable security rails are secured.
- Clean Smart Hubs regularly by following vendor-supported cleaning solutions and chemicals.

For Smart Hub replacement:

- If purchased through Imprivata, or for general questions, contact Imprivata Customer Support.
- If purchased through a different vendor, contact the manufacturer.

Devices

Mobile Device OS Updates

Create a strategy for keeping the mobile device OS (iOS and Android) at a version supported by MAM. For more information on supported device OS versions, see the system requirements.

iOS Updates

- Use MAM automation to perform the iOS updates instead of your MDM's over-the-air, just in time iOS updates. MDM updates can interrupt Locker checkins.
- Do not perform an iOS update as part of a Check In Workflow.
- Use a scheduled automation and the iOS Update Workflow action to update connected iOS devices in target groups at specific times throughout an update window.
- Ensure that you run a Check In Workflow after the update is complete.
- For iOS 17 and higher, ensure iOS updates and provisioning are properly applied by reviewing these custom options.

Certificates

Track the certificates that are in use in your MAM organization. Take special note of the following:

- The expiry date of the certificates.
- Where the certificates are installed or being used.

Expiring and Exporting the Supervision Identity for DEP

The Supervision Identity for DEP, a cryptographic file in .crt format, has an expiry date tied to the date you export it from the MAM admin console.

Updating the SAML Certificate

For organizations using SAML to provision and authenticate users against their Identity Provider (IdP), Mobile Access Management takes the role of a Service Provider (SP). During configuration, you created a SAML certificate in the MAM admin console for use with your IdP.

Beginning 60 days before the SAML certificate expires, the MAM admin console displays an alert warning you of the expiration. The banner is only displayed when the active SAML certificate is expiring.

Utilizing the MAM Dashboard

Ensure your enterprise has a team responsible for reviewing the MAM Dashboard to identify Launchpads and devices that require investigation. For more information, see "Dashboard" in the Imprivata help.

Launchpad Health

Use the Launchpad Health section of the Dashboard to ensure all Launchpads are in a healthy status. This gives a real time snapshot of Launchpad health, including areas of improvement.

Ensure that all Launchpad tiles are turned on by reviewing the settings in **Admin -> Dashboard**.

Reviewing the Launchpad Health Dashboard is a daily activity that ensures the following:

Immediate Action is Necessary

- NO (zero) **Monitored Launchpad is disconnected**: Only monitor production Launchpads – these Launchpads should be connected 24 x 7. This tile displays the Launchpad computers that are not communicating with the Launchpad service.

  This tile is only displayed when Launchpad Monitoring is enabled; it is a best practice to enable it.
- NO (zero) **Monitored Launchpad has no Smart Hubs connected**: Only monitor production Launchpads – these Launchpads should be connected 24 x 7.

Daily Action is Necessary

- **Launchpad has failed devices:** Clear failed devices daily. Identify the devices that cannot be cleared, because they may require on-site support.
- **Launchpad has unpaired devices:** Clear unpaired devices daily. Identify the devices that cannot be cleared, because they may require on-site support.
- **Launchpad has checked out devices connected:** Remotely check in devices daily. Identify the devices that cannot be remotely checked in, because they may require on-site support.
- **Launchpad has devices in wrong location:** Review the Launchpads with devices in the wrong location. Use on-site support to ensure Launchpads have adequate and accurate devices.

Requires Future Action

- **Launchpad version is not current:** Launchpads with older software indicates the need for your organization to plan, test, and perform a Launchpad software version upgrade within the next 30 days.

Requires Review

- Zero (0) - **Monitored Launchpad has no connected devices:** Having Launchpads with no connected devices may indicate the need for more devices.
- **Launchpad has devices with no heartbeat**: A device with no heartbeat can indicate device or network issues in the environment.

It is important to monitor the number of devices with no heartbeat, identify trends, and ensure that Launchpads have an adequate number of devices with a heartbeat. For more information, see "Locker Heartbeat" in the Imprivata help.

Device Health

Reviewing the Device Health section of the Dashboard is a daily activity that ensures the following:

Daily Action is Necessary

- **Device last activity failed:** Review devices that are in a failed status. Take action on these devices to return them to a healthy state.
- **Device is unpaired:** Review devices that are in an unpaired status. Take action on these devices to return them to a healthy state.

  Review patterns as needed to identify necessary changes to the environment.

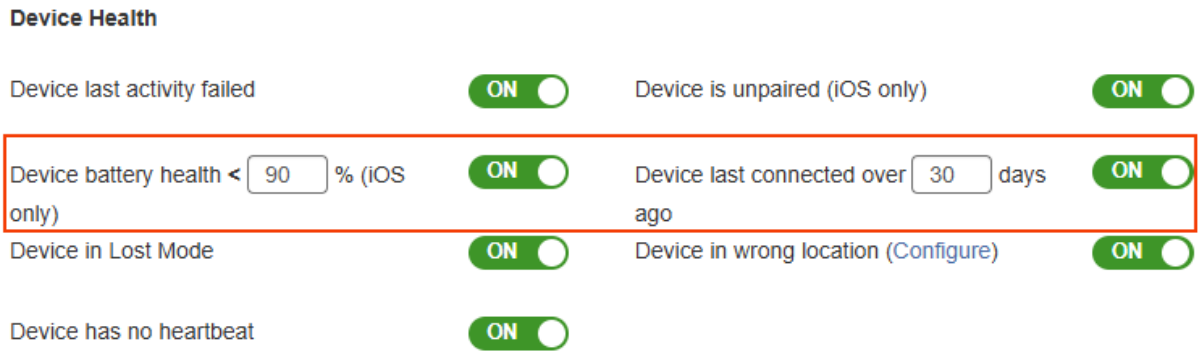
Requires Review

- **Device battery health < 75%:** These devices may be priority to replace as the devices age and their battery health degrades. 75% is the default setting and can be customized by the **Admin -> Dashboard** setting.
- **Device is overdue:** The organization should identify the team responsible for investigating overdue devices. If this number tracks too high, it will be important to take action.
- **Device In Lost Mode:** When Lost Mode is turned on, this number should match the **Device is overdue** metric.

  If you do not utilize Lost Mode, this setting can be turned off by the **Admin > Dashboard** setting.
- **Device last connected over 30 days ago:** Review this after resolving **Device is overdue** devices. Identify devices that may need to be retired, fall under break/fix, or may be identified as lost.
- **Device in wrong location:** The organization should identify the ownership around who ensures Launchpads have adequate devices.

  This tile can be utilized to review which devices can be returned to their home location.
- **Device has no heartbeat:** A device with no heartbeat can indicate device or network issues in the environment. It is important to monitor the number of devices with no heartbeat, identify trends,

and ensure that Launchpads have an adequate number of devices with a heartbeat.



Audit Logs

Periodically export and review the Audit Log. The following common audits can be valuable to review on a regular basis:

- **Smart Hub Connect/Disconnect data:** Identify trends or concerns for any historical disconnected Smart Hubs.
- **Modified Settings / Modified Workflows:** Ensure changes are being made via change control. Utilize when troubleshooting issues.
- **Emergency PIN:** Identify the misuse of the Emergency PIN.
- **Network Username / Password:** Utilize data to identify trends in the increase of Network username/password usage.