imprivata®

# Product Documentation

## System Requirements

Imprivata Mobile Access Management

*Last Updated: April 23, 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

# System Requirements

This document describes the hardware and software requirements for Imprivata Mobile Access Management. Any limitations are noted in the support details and notes section for each component.

## MAM Administrator Console

- The MAM Admin Console supports any modern web browser on Mac and Windows.
- Imprivata tests with Safari, Google Chrome, Firefox, and Microsoft Edge.

## Launchpad Mac or Windows PC

Mac and Windows can be used to run the client-side MAM Launchpad software.

| Item | Mac | Windows |
|---|---|---|
| Form Factor | • Mac Mini M4 (using the front USB-C ports only)<br>• Mac Mini M2 | Headless desktop mini-PC |
| Operating System | macOS 15.4 or higher | Windows 10 or Windows 11 version within the last 2 years |
| RAM | 16 GB | 16 GB |
| Drive Capacity | 20 GB or greater SSD | 20 GB or greater SSD |
| Permission: Allow accessory to connect | Required for Mac Launchpads.<br>For more information, see "Allow Accessory to Connect" in the Imprivata help. | n/a |
| Unattended Use | Launchpad systems must be configured for unattended use.<br>For more information, see "Configure Unattended Launchpads" in the Imprivata help. | |
| Dedicated system | The PC should be dedicated for MAM, and not shared with other apps. | The PC should be dedicated for MAM, and not shared with other apps.<br>Do not install the Imprivata agent (for Imprivata Enterprise Access Management) on the Launchpad, because it will conflict with the proximity card reader. |
| VNC or other remote access | Some method of VNC or other remote access is required to all stations. | |
| iTunes app<br>Apple Devices app for Windows | n/a | *For iOS environments only:*<br>Install the current Apple Devices app or iTunes app or extract DLLS from iTunes for Apple's MobileDevice components.<br>Not required for Android environments. |
| GroundControl Launchpad.app installed in a directory local user has full file permissions to | The GroundControl Launchpad.app must be installed in a directory the local user has full file permissions over, or the local Mac user must be a macOS local admin. | n/a |
| Network connection | Imprivata requires that Launchpads use an Ethernet network connection to ensure stable 24 × 7 availability. | |

Imprivata does not test with or support virtual or thin-client systems.

**IMPORTANT:**
Test your model thoroughly before selecting a PC to be used as a Launchpad.

If your PC has trouble connecting to more than 8 or so iOS devices at once, disable XHCI in the PC's BIOS to determine if this solves the issue.

# Network

Imprivata Mobile Access Management uses HTTPS (port 443) for all communication between the Launchpad and the MAM Administrator Console. After initial registration, the Launchpad switches to Secure WebSockets (also port 443) for asynchronous bi-directional messaging.

Firewalls must support **Secure WebSockets**. A common firewall feature is to force close any sockets that remain open for a long period of time, but this will cause MAM to lose the client-server connection.

| Source | Destination | Protocol | Use |
|---|---|---|---|
| Launchpad | US: us.groundctl.com / 52.202.156.90, 54.197.149.48<br>UK: uk.groundctl.com / 18.168.161.122, 13.41.242.92 | HTTPS/443 and WSS/443 | Server communication |
| Launchpad | US: groundcontrol-prod.s3.amazonaws.com<br>UK: c16-assets-groundctl-com.s3.amazonaws.com | HTTPS/443 | Asset downloads |
| Launchpad | *.bugsplatsoftware.com | HTTPS/443 | Crash reporting |
| Launchpad (iOS only) | albert.apple.com<br>gs.apple.com<br>appldnld.apple.com<br>secure-appldnld.apple.com | HTTPS/443 | Apple device activation & IPSW downloads |
| Launchpad | *Your Imprivata appliance* | HTTPS/443 | Identity lookup during Checkout (if used) |
| Launchpad<br>Locker app (iOS and Android) | ctlful.imprivata.com | HTTPS/443 | Log submission |
| Device | US: groundcontrol-prod.s3.amazonaws.com<br>UK: c16-assets-groundctl-com.s3.amazonaws.com | HTTPS/443 | Checkout (if used) |
| Device | *Your Imprivata appliance* | HTTPS/443 | Identity lookup during Checkout (if used) |
| Device (iOS only) | *.push.apple.com | TCP Ports: 443, 80, 5223, 2197 | Apple push notifications |
| Device (Android only) | See Firebase Documentation | TCP ports: 443, 5228, 5229, 5230 | Firebase push notifications |
| MAM Server<br>US: 52.21.126.154, 52.20.201.34<br>UK: 18.169.178.163, 35.177.97.127 | Your MDM Server | HTTPS/443 | MDM API requests (if used) |

Apple products on enterprise networks typically require specific hosts and ports to be open. Here is Apple's documentation on the use of Apple products on enterprise networks.

Android products on enterprise networks require specific hosts and ports to be open for Firebase push notifications. For more information, see Google documentation.

# MDMs

The following MDM systems are supported for Check Out.

| Feature | Ivanti EMM | Ivanti Neuron | Jamf Pro | Samsung Knox Manage | Microsoft Intune | Soti MobiControl | Omnissa (VMware) Workspace ONE |
|---|---|---|---|---|---|---|---|
| **Check In / Check Out (iOS)** | | | | | | | |
| Personal Passcodes | ✓ | ✓ | ✓ | ○ | ✓ | ○ | ✓ |
| Set Labels/Tags/Org groups | ✓ | ○ | ○ | ○ | ✓ | ○ | ✓ |
| Assign to User | ✓ | ✓ | ✓ | ○ | ○ | ○ | ✓ |
| Enable Lost Mode | ○ | ○ | ✓ | ○ | ✓ | ○ | ✓ |
| **Check In / Check Out (Android)** | | | | | | | |
| Personal Passcodes | ○ | ○ | ○ | ✓ | ✓ | ✓ | ✓ |
| Set Labels/Tags/Org groups | ○ | ○ | ○ | ✓ | ✓ | ✓ | ✓ |
| Assign to User | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| Enable Lost Mode | ○ | ○ | ○ | ✓ | ✓ | ✓ | ✓ |
| **Provisioning (iOS)** | | | | | | | |
| DEP Provisioning | ✓ | ✓ | ✓ | ○ | ✓ | ○ | ✓ |
| Non-DEP Provisioning | ✓ | ✓ | ✓ | ○ | ✓ | ○ | ✓ |
| Assign DEP Profile | ○ | ○ | ○ | ○ | ✓ | ○ | ✓ |
| Delete / Retire | ✓ | ✓ | ✓ | ○ | ✓ | ○ | ✓ |

## Required MDM Configurations

- You must integrate MAM with your MDM's API.
  - The API integration is used by MAM to clear any device passcodes on check in.
  - The API integration can trigger Lost Mode for overdue devices.

## MDM Requirements for iOS devices

The following items are required in your MDM system for iOS devices.

| Item | Description |
|---|---|
| DEP profile | Your MDM DEP profile:<br>• Must include MAM's supervision identity. This allows your device to more reliably connect to MAM.<br>• Should skip all setup screens. |
| Disable USB Restricted Mode | All devices must be set to **Disable USB Restricted Mode**.<br>This feature has different names in different MDMs, but is used to keep your device's USB connection active even when it is passcode locked. |
| Allow Recovery for Unpaired Devices | The MDM should **Allow Recovery for Unpaired Devices**. |
| Notification profile to allow Imprivata Locker app to receive notifications | • All devices must receive a notification profile to allow our Imprivata Locker app to receive notifications. The app ID for the Locker app for iOS is **com.imprivata.b2b.locker**.<br>  ○ Apple permits a maximum of one notification profile on devices. This limitation is usually not enforced by MDM systems, leading to conflicts and unexpected behaviors.<br>  ○ To avoid unexpected notification behavior, Imprivata strongly recommends using one master notification profile for all iOS devices — both shared and dedicated — in your organization. |

# Proxy Support

Imprivata Mobile Access Management has limited support for proxies:

- Proxies must be configured in the Launchpad app during initial registration
- Only **unauthenticated** proxies are supported
- Authenticated proxies and PAC files are not supported
- System proxy settings are ignored

# USB Smart Hubs

Imprivata requires and only supports Smart Hubs from these manufacturers.

Imprivata supports Smart Hubs and cables from these manufacturers. Third party cables are not supported.

**NOTE:**
While these manufacturers do sell other variations of hardware, only the items listed below are tested and supported by Imprivata.

| Vendor | Model |
|---|---|
| Bretford | • 20 port (Large) PowerSync Pro Gen 2 w/Lightning Cables<br>• 10 port (Large) PowerSync Pro Gen 2 w/Lightning Cables<br>• 20 port (Small) PowerSync Pro Gen 2 w/Lightning Cables<br>• 10 port (Small) PowerSync Pro Gen 2 w/Lightning Cables<br>• 20 port (Large) PowerSync Pro Gen 2 w/USB-C Cables<br>• 10 port (Large) PowerSync Pro Gen 2 w/USB-C Cables<br>• 20 port (Small) PowerSync Pro Gen 2 w/USB-C Cables<br>• 10 port (Small) PowerSync Pro Gen 2 w/USB-C Cables |

| Vendor | Model |
| --- | --- |
| Datamation | • 24 Port (Phone) Unidock w/Lightning Connection<br>• 24 Port (Phone) Unidock w/USB-C Connection<br>• 16 Port (Phone) Unidock w/Lightning Connection<br>• 16 Port (Phone) Unidock w/USB-C Connection<br>• 8 Port (Phone) Unidock w/Lightning Connection<br>• 8 Port (Phone) Unidock w/USB-C Connection<br>• 8 Port (Tablet) w/Lightning Connection<br>• 16 Port (Tablet) Unidock Tray w/Lightning Cables<br>• 24 Port (Phone) Unidock Tray w/USB-C Cables |

For Smart Hub pricing and accessories, contact your account manager.

For best performance, MAM requires a 1 to 1 connection between the Launchpad and 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. For more information on Smart Hubs, see the "Implementation, Maintenance, and Best Practices Guide" in the Imprivata help.

# Proximity Card Readers

Imprivata Mobile Access Management supports USB-connected proximity card readers manufactured by rf IDEAS. Many brands resell rf IDEAS readers, including Imprivata.

Proximity card readers must be plugged directly into the Launchpad computer, not into the Smart Hub.

## Imprivata Models

| Vendor | Model |
| --- | --- |
| rf IDEAS | • IMP-75<br>• IMP-80<br>• IMP-60<br>• IMP-82<br>• IMP-80-mini<br>• HDW-IMP-82 MINI<br>• HDW-IMP-80-MINI-BLE<br>• HDW-IMP-80-BLE |

# Devices

Imprivata Mobile Access Management supports iOS and Android devices.

## Apple Devices

Apple device support is based on iOS version support. MAM supports iOS 18 and 17. Only factory-reset devices are supported. .

# Android Devices

Imprivata Mobile Access Management 6.0 and later supports Android devices.

| Item | Support |
|---|---|
| Android OS | Android 9 or later |
| Devices | **Cisco:**<br>• Cisco CP 860<br>**Google:**<br>• Google Pixel 7<br>• Google Pixel 7a<br>• Google Pixel 8<br>• Google Pixel 8 Pro<br>**HMD:**<br>• HMD Fusion<br>• HMD Pulse<br>• HMD Skyline<br>**Honeywell:**<br>• CT30 (non-healthcare)<br>• CT37<br>**Samsung:**<br>• Samsung Galaxy S25 Ultra<br>• Samsung S22, A14<br>• Samsung A15 5G<br>• Samsung xCover 6 Pro<br>**Spectralink:**<br>• Versity 95, Versity 96, Versity 97XX<br>**Zebra:**<br>• Zebra TC5 series - TC52, TC57<br>• Zebra TC2 series - TC21, TC26<br>• Zebra HC50, HC20<br>• Zebra ET40 tablet |
| Mobile browsers | MAM supports clearing browser cache as part of Check In action:<br>• Google Chrome<br>• Microsoft Edge |
| Device Settings and permissions | The Imprivata Locker app for Android devices requires the following device settings and permissions:<br>• Draw over (overlay) other apps. Must be enabled manually on each device.<br>• Accessibility Service. Must be enabled manually on each device.<br>• Autofill Service, set to use the Locker app. |
| MDMs | Android devices must be enrolled in an MDM system. Supported MDMs:<br>• Microsoft Intune<br>• Samsung Knox Manage<br>• SOTI MobiControl<br>• Omnissa (VMware) Workspace ONE |

# Device Cases and Batteries

- Basic protective cases are supported.
- Imprivata does not support using supplemental battery cases with data passthroughs.

# Supported Applications

For more information on supported applications, see the Imprivata App support page.