



Product Documentation

System Requirements

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

© 2025 Imprivata, Inc. All Rights Reserved.

This product is distributed under licenses restricting its use, copying, distribution and decompilation.

Imprivata's products may be covered in whole or in part by one or more U.S. pending or issued patents listed at <http://www.imprivata.com/patents>.

Trademark Information

OneSign, Imprivata, and the Imprivata logo are registered trademarks of Imprivata, Inc. ProveID and Imprivata OneSign APG are trademarks of Imprivata, Inc. in the United States and in other countries.

Legal Notices

Under international copyright laws, neither the documentation nor software may be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form, in whole or in part without the prior written consent of Imprivata, Inc., except as described in the license agreement.

The names of companies, products, people, and/or data mentioned herein are fictitious and are in no way intended to represent any real individual, company, product, or event, unless otherwise noted.

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

Document revision

Table of Contents

- Imprivata Mobile Access Management System Requirements 4**
 - MAM Administrator Console 4
 - Launchpad Mac or Windows PC 4
 - Network 5
 - MDMs 6
 - Required MDM Configurations 6
 - MDM Requirements for iOS devices 7
 - Proxy Support 7
 - USB Hubs and Carts 7
 - Proximity Card Readers 8
 - Imprivata Models 8
 - Devices 9
 - Apple Devices 9
 - Android Devices 9
 - Device Cases and Batteries 10
 - Supported Applications 10

Imprivata Mobile Access Management 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 Administrator 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

The MAM Launchpad software is supported on Mac and Windows computers that meet the following requirements.

Item	Mac	Windows
Form Factor	Headless desktop mini-PC <ul style="list-style-type: none">• Mac Mini M4 (using the front USB-C ports only)• 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 For more information, see Allow Accessory to Connect .	n/a
Unattended Use	Launchpad systems must be configured for unattended use. For more information, see Configure Unattended Launchpads .	
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. Do not install the Imprivata agent (for Imprivata Enterprise Access Management/OneSign) 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 Apple Devices app for Windows	n/a	<i>iOS environments only:</i> Install the current Apple Devices app or iTunes app or extract DLLS from iTunes for Apple's MobileDevice components.
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. For more information, see this article .	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 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 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 gs.apple.com appldnld.apple.com secure-appldnld.apple.com	HTTPS/443	Apple device activation & IPSW downloads
Launchpad	<i>Your Imprivata appliance</i>	HTTPS/443	Identity lookup during Checkout (if used)
Launchpad Locker app (iOS and Android)	ctlful.imprivata.com	HTTPS/443	Log submission
Device	US: groundcontrol-prod.s3.amazonaws.com UK: c16-assets-groundctl- com.s3.amazonaws.com	HTTPS/443	Checkout (if used)
Device	<i>Your Imprivata appliance</i>	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 US: 52.21.126.154, 52.20.201.34 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 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: <ul style="list-style-type: none">• Must include MAM's supervision identity. This allows your device to more reliably connect to MAM.• Should skip all setup screens.
Disable USB Restricted Mode	All devices must be set to Disable USB Restricted Mode . 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	<ul style="list-style-type: none">• 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.<ul style="list-style-type: none">◦ Apple permits a <u>maximum of one notification profile</u> on devices. This limitation is usually not enforced by MDM systems, leading to conflicts and unexpected behaviors.◦ 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 Hubs and Carts

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	<ul style="list-style-type: none"> • 20 port (Large) PowerSync Pro Gen 2 w/Lightning Cables • 10 port (Large) PowerSync Pro Gen 2 w/Lightning Cables • 20 port (Small) PowerSync Pro Gen 2 w/Lightning Cables • 10 port (Small) PowerSync Pro Gen 2 w/Lightning Cables • 20 port (Large) PowerSync Pro Gen 2 w/USB-C Cables • 10 port (Large) PowerSync Pro Gen 2 w/USB-C Cables • 20 port (Small) PowerSync Pro Gen 2 w/USB-C Cables • 10 port (Small) PowerSync Pro Gen 2 w/USB-C Cables
Datamation	<ul style="list-style-type: none"> • 24 Port (Phone) Unidock w/Lightning Connection • 24 Port (Phone) Unidock w/USB-C Connection • 16 Port (Phone) Unidock w/Lightning Connection • 16 Port (Phone) Unidock w/USB-C Connection • 8 Port (Phone) Unidock w/Lightning Connection • 8 Port (Phone) Unidock w/USB-C Connection • 8 Port (Tablet) w/Lightning Connection • 16 Port (Tablet) Unidock Tray w/Lightning Cables • 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](#).

Proximity Card Readers

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

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

Imprivata Models

Vendor	Model
rf IDEAS	<ul style="list-style-type: none"> • IMP-75 • IMP-80 • IMP-60 • IMP-82 • IMP-80-mini • HDW-IMP-82 MINI • HDW-IMP-80-MINI-BLE • 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	<p>Cisco:</p> <ul style="list-style-type: none">• Cisco CP 860 <p>Google:</p> <ul style="list-style-type: none">• Google Pixel 7• Google Pixel 7a• Google Pixel 8• Google Pixel 8 Pro <p>HMD:</p> <ul style="list-style-type: none">• HMD Fusion• HMD Pulse• HMD Skyline <p>Honeywell:</p> <ul style="list-style-type: none">• CT30 (non-healthcare)• CT37 <p>Samsung:</p> <ul style="list-style-type: none">• Samsung Galaxy S25 Ultra• Samsung S22, A14• Samsung A15 5G• Samsung xCover 6 Pro <p>Spectralink:</p> <ul style="list-style-type: none">• Versity 95, Versity 96, Versity 97XX <p>Zebra:</p> <ul style="list-style-type: none">• Zebra TC5 series - TC52, TC57• Zebra TC2 series - TC21, TC26• Zebra HC50, HC20• Zebra ET40 tablet
Mobile browsers	<p>MAM supports clearing browser cache as part of Check In action:</p> <ul style="list-style-type: none">• Google Chrome• Microsoft Edge

Item	Support
Device Settings and permissions	<p>The Imprivata Locker app for Android devices requires the following device settings and permissions:</p> <ul style="list-style-type: none"> • Draw over (overlay) other apps. Must be enabled manually on each device. • Accessibility Service. Must be enabled manually on each device. • Autofill Service, set to use the Locker app.
MDMs	<p>Android devices must be enrolled in an MDM system. Supported MDMs:</p> <ul style="list-style-type: none"> • Microsoft Intune • Samsung Knox Manage • SOTI MobiControl • Omnisia Workspace ONE (VMware Workspace ONE)

Device Cases and Batteries

- Basic protective cases are supported.
- Imprivata does not support using supplemental battery cases with data passthroughs. For more information, see [Device cases](#).

Supported Applications

For more information on supported applications, see the [Imprivata App support page](#).