



# MobileIron Core and Connector 11.1.0.0 Release and Upgrade Notes

March 4, 2021

For complete product documentation see:  
[MobileIron Core Documentation Home Page](#)

Copyright © 2009 - 2021 MobileIron, Inc. All Rights Reserved.

Any reproduction or redistribution of part or all of these materials is strictly prohibited. Information in this publication is subject to change without notice. MobileIron, Inc. does not warrant the use of this publication. For some phone images, a third-party database and image library, Copyright © 2007-2009 Aeleeeta's Art and Design Studio, is used. This database and image library cannot be distributed separate from the MobileIron product.

“MobileIron,” the MobileIron logos and other trade names, trademarks or service marks of MobileIron, Inc. appearing in this documentation are the property of MobileIron, Inc. This documentation contains additional trade names, trademarks and service marks of others, which are the property of their respective owners. We do not intend our use or display of other companies' trade names, trademarks or service marks to imply a relationship with, or endorsement or sponsorship of us by, these other companies.



# Contents

---

<b>About MobileIron Core</b> .....	<b>5</b>
<b>Before you upgrade</b> .....	<b>5</b>
Understand the impact of TLS protocol changes .....	5
<b>New features and enhancements summary</b> .....	<b>7</b>
General features and enhancements .....	7
Android and Android Enterprise features and enhancements .....	9
iOS and macOS features and enhancements .....	10
MobileIron Threat Defense features .....	11
<b>Support and Compatibility for MobileIron Core 11.1.0.0</b> .....	<b>12</b>
<b>Support policy</b> .....	<b>12</b>
<b>MobileIron end of sale and support policy</b> .....	<b>12</b>
<b>MobileIron Core support and compatibility</b> .....	<b>13</b>
SAML / Identity Provider .....	13
LDAP .....	14
Hardware appliances .....	14
Atlas .....	14
Reporting database .....	15
Monitor .....	15
Sentry .....	15
Access .....	15
Android .....	16
iOS .....	16
macOS .....	17
tvOS .....	17
Windows .....	18
<b>Supported browsers and browser resolutions</b> .....	<b>19</b>
Supported browser resolutions .....	19



---

<b>Language support</b> .....	<b>20</b>
Language support for MobileIron Core messages .....	20
Language support on Android and Android Enterprise devices .....	21
Language support on iOS and macOS devices .....	21
Language support on Windows devices .....	21
<b>Resolved issues</b> .....	<b>22</b>
<b>Known issues</b> .....	<b>24</b>
<b>MobileIron Core upgrade information</b> .....	<b>26</b>
Support community .....	26
MobileIron Core upgrade readiness checklists .....	26
Pre-Upgrade checklist .....	26
Upgrade considerations .....	28
Post-Upgrade checklist .....	29
Check disk space availability .....	30
The CLI command: show system disk .....	30
The System Manager .....	30
MobileIron Core upgrade paths .....	31
MobileIron Core upgrade URL .....	31
Backing up MobileIron Core .....	31
MobileIron Core end of sale and support policy .....	31
<b>Enterprise Connector upgrade information</b> .....	<b>32</b>
Enterprise Connector upgrade overview .....	32
MobileIron Enterprise Connector upgrade paths .....	32
Enterprise Connector upgrade URL .....	33
Enterprise Connector upgrade notes .....	33
<b>Documentation errata</b> .....	<b>34</b>
Correction to Apple device enrollment profile settings .....	34
<b>Documentation resources</b> .....	<b>35</b>



# About MobileIron Core

MobileIron Core is a mobile management software engine that enables IT to set policies for mobile devices, applications, and content. This product enables Mobile Device Management, Mobile Application Management, and Mobile Content Management capabilities.

## Before you upgrade

Before you upgrade, you must consider the possible impact of certain security enhancements on your environment:

## Understand the impact of TLS protocol changes

For heightened security, when you upgrade to MobileIron Core 10.3.0.0 through the most recently released version as supported by MobileIron, MobileIron Core's configurations for incoming and outgoing SSL connections are automatically updated to use **only** protocol TLSv1.2. TLSv1.2 cannot be disabled.

*This change occurs regardless of the protocol settings before the upgrade.*

This change means that MobileIron Core now uses only TLSv1.2 for incoming and outgoing connections with all external servers. Examples of external servers to which Core makes outgoing connections are:

- Standalone Sentry
- Integrated Sentry
- Connector
- SCEP servers
- LDAP servers
- MobileIron Gateway
- Apple Push Notification Service (APNS)
- Content Delivery Network servers
- MobileIron support server (support.mobileiron.com)
- Outbound proxy for Gateway transactions and system updates
- SMTPS servers
- Public app stores (Apple, Google, Windows)
- Apple Volume Purchase Program (VPP) servers



- Apple Device Enrollment Program (DEP) servers
- Android for Work servers

**Therefore, if an external server is not configured to use TLSv1.2, change the external server to use TLSv1.2.**

To determine TLS protocol usage with external servers:

- **For outgoing connections from Core to external servers**, use the MobileIron utility explained in the following article to determine the TLS protocol usage with those servers:  
<https://help.mobileiron.com/s/article-detail-page?Id=kA134000000Qx3UCAS>
- **For incoming connections to Core from external servers**, determine each server's TLS protocol usage (no MobileIron utility is available).

For more information:

- [Threat Advisory: Notice of Deprecation of TLS 1.0 and 1.1 on MobileIron Systems](#)
- "Advanced: Incoming SSL Configuration" and "Advanced: Outgoing SSL Configuration" in the *MobileIron Core System Manager Guide*.



# New features and enhancements summary

This section provides summaries of new features and enhancements available in this release of MobileIron Core. References to documentation describing these features are also provided, when available.

- [General features and enhancements](#)
- [Android and Android Enterprise features and enhancements](#)
- [iOS and macOS features and enhancements](#)
- [iOS and macOS features and enhancements](#)
- [MobileIron Threat Defense features](#)

For new features and enhancements provided in previous releases, see the release notes for those releases, available in [MobileIron Core Product Documentation](#). MobileIron Support credentials are required to access the site.

## General features and enhancements

This release includes the following new features and enhancements that are common to all platforms.

- **Weaker SSH algorithms removed from Core in favor of stronger ones:** The following SSH algorithms have been removed from the options on the **System Manager > Security > Advanced > SSH Configuration** page:
  - diffie-hellman-group-exchange-sha1
  - diffie-hellman-group14-sha1
  - hmac-sha1

Admins are encouraged to use the stronger algorithms, such as **diffie-hellman-group-exchange-sha256** and **hmac-sha2-512** instead. For more information, see **Advanced: SSH Configuration** in the Security Settings chapter of the *MobileIron Core System Manager Guide*.

- **Confirmation email sent automatically for new client registrations:** When a device user accepts the Terms of Service (ToS) agreement in a registration invitation, the admin automatically receives an audit email confirming the registration, from Core version 11.1.0.0 through the most recently released version as supported by MobileIron. The email consists of a message and identifying client information:  
"The following user has accepted device registration terms and has attempted to enroll a new device:"  
User name, display name, email address, date and time, IP address, platform, employee owned.



For more information, see "Configuring an end user Terms of Service agreement" in the Self-service user portal chapter of the *MobileIron Core Device Management Guide* for your operating system.

- **New option to hide QR code and registration URL:** A new configuration checkbox has been added to the Settings > System Settings > Users & Devices > Device Registration page that allows you to choose whether or not to show users a QR code and registration URL. This option is enabled by default. When enabled, the QR code and registration URL display to users. For more information, see "Disabling the QR code and registration URL" in the *MobileIron Core Device Management Guide* for your operating system.
- **New option to hide self-service portal (SSP) Activity page:** A new configuration checkbox has been added to the Settings > System Settings > General > Self-Service Portal page that allows you to choose whether or not to show users their activity in the SSP. This option is enabled by default. When enabled, the SSP Activity page displays to users. For more information, see "Disabling device history logs in the self-service user portal" in the *MobileIron Core Device Management Guide* for your operating system.
- **AppConnect passcode history updates:** The Passcode history option in the AppConnect Global policy is changed as follows:
  - The value options are updated to 12. This means that you can restrict device users from reusing any password up to the past 12 passwords.
  - The passcode reuse is case insensitive. This means that the passcode case is not considered for reuse. Device users cannot change the case for past passcodes and reuse them. Password and passWord are considered the same.

These feature updates require Mobile@Work 12.11.10 for iOS.

- **Increased capacity for broadcast notification messages to all device users:** When an administrator sends a message out to all device users via label, and the label contains more than 200 device users, Core now sends the messages out in batches, and so is not limited to only sending 200 at a time. Administrators can send, monitor, and confirm this process from the **Devices & Users > Labels** tab.  
Because of the potential for accidental or deliberate spamming of users with this feature, Core provides two levels of confirmation before sending the message. For more information, see "Notifying all device users using labels" in the Managing Labels chapter of *Getting Started with MobileIron Core*.
- **"Unlock User" option available to MobileIron administrators:** MobileIron administrators now have the ability to unlock users who have locked themselves out of the user portal. Typically, if a user does not log in correctly within a configured number of tries, the user must wait the configured time before they can log in again. This option allows the administrator to reset the account immediately, through the **Devices & Users > Users > Actions** menu. This feature is available on Core 11.1.0.0 through the most recently released version as supported by MobileIron. For more information, see "Unlocking locked-out local users in the admin portal" in the User Management chapter of *Getting Started with MobileIron Core*.





- **New endpoint for mutual certification authentication:** New mutual authentication device endpoints are available for use by iOS and Android clients. The existing (old) OAuth endpoint is not protected by 2FA or mutual certificate authentication and is vulnerable to password spraying and DOS attacks. The administrator can disable the original OAuth endpoint and utilize the new endpoint. This feature is applicable on Mobile@Work for Android version 11.1.0.0 and Mobile@Work for iOS version 12.11.10 through the latest versions as supported by MobileIron. For more information, see "New endpoint for mutual certification authentication" in the *MobileIron Core Device Management Guide for Android and Android Enterprise Devices* or the *MobileIron Core Device Management Guide for iOS and macOS Devices*.

## Android and Android Enterprise features and enhancements

This release includes the following new features and enhancements that are specific to the Android and Android Enterprise platforms.

- **New Lockdown Policy field added: "Allow install from unknown sources on the device"** allows installation of apps from untrusted sources in the personal profile. Unless this field is selected, the work profile never allows installation of apps from unknown sources. Applicable for Android 11+ devices. For more information, see "Lockdown policy fields for Android Enterprise devices in Work Managed Device mode and Managed Device with Work Profile mode" and "Lockdown policy fields for Android Enterprise devices in Work Profile for Company Owned Device mode" in the *Getting Started with MobileIron Core*.
- **Support for Samsung Knox Dual Encryption (DualDAR):** Support for Dual Encryption (DualDAR) has been added to further secure and protect sensitive data on devices. Samsung Knox includes a FIPS 140-2 certified encryption module within the inner layer of the encryption. DualDAR is applicable to Knox 3.0 on Android 8.0 devices through the latest version as supported by MobileIron. DualDAR is applicable to Android Enterprise:
  - Work Profile mode
  - Managed Device with Work Profile mode

For more information, see "Samsung Knox Dual Encryption (DualDAR) support" in the *MobileIron Core Device Management Guide for Android and Android Enterprise Devices*.

- **New Lockdown Policy field added: "Enable Cross profile whitelisting of Apps"** allows users to share information from specific apps from within the work profile to the personal side of the device. This allows data from the Work Profile container to share data to the exact same app that is located on the personal side. Applicable for Android 11+ devices. For more information, see "Lockdown policy fields for Android Enterprise devices in Work Profile for Company Owned Device mode" in *Getting Started with MobileIron Core*.



- **Ability to set apps to the foreground in devices:** A new field setting, **Auto Launch Application on Install**, allows administrators to set Android Enterprise apps to the foreground upon registration or installation. A typical use case would be for a security/VPN app that needs to be configured by the device user before the device can be protected. Applicable to:
  - Any Android Enterprise app in the App Catalog
  - Android devices version 6.0 through the latest version as supported by MobileIron
  - Device Owner, Managed Device with Work Profile, Work Profile on Company Owned Device modes
 For more information, see "Adding in-house apps" and "Public and private Android Enterprise app deployment" in the *MobileIron Core Apps@Work Guide*.

- **Added support for app restrictions with in-house applications for Android non-GMS devices:** For devices registered to Core in modes other than Google Mobile Services (GMS) mode, administrators can apply Android Open Source Project (AOSP) in-house app restrictions to these devices. Using the "Enable AOSP app restrictions" field, the administrator can now set the in-house restrictions to display in the App view page of the App Catalog.

Applicable to the following Android Enterprise modes:

- Work Managed Device mode
- Work Profile mode
- Managed Device with Work Profile mode
- Work Profile on Company Owned Device mode

For more information, see "App restrictions with in-house applications for Android" and "Adding in-house apps" in the *MobileIron Core Apps@Work Guide*.

## iOS and macOS features and enhancements

This release includes the following new features and enhancements that are specific to the iOS and macOS platforms.

- **Two new fields have been added to Apple Per-App VPN configurations - Associated Domains and Excluded Domains:** In the Per-app VPN and in the MobileIron Tunnel configurations, administrators can specify associated and excluded domains to be considered for association or exclusion from the per-app VPN and tunnel server connections. Applicable to iOS 14.3 and macOS 11.0 through the latest version as supported by MobileIron. For more information, see "Managing VPN Settings" in the *MobileIron Core Device Management Guide for iOS and macOS Devices*.
- **Support for IdP-based device registrations:** As part of the DEP profile, the MDM server provides Custom enrollment URL along with a standard URL to get the MDM profile to the Apple server. This URL



can be used by administrators to enforce their own authentication model or provide any other information. An example use case would be where administrators cannot use their organization's Identity provider "as is" for DEP authentication without heavy changes on the infrastructure. For more information, see "Customized registration using SAML IdP" and "Creating Apple Device Enrollment profiles" in the *MobileIron Core Device Management Guide for iOS and macOS Devices*.

- **New option to parse or not parse .mobilconfig file:** In the Configuration Profile Setting dialog box, there is a new field "Send File Verbatim" that you can select if you wish to deploy a signed .mobileconfig file, for example, Apple debug configurations via MobileIron MDM. Because Core does not expect a signed file, it would not be able to parse it and inject a substitution variable because it would change the signature of the signed file. Files uploaded with this option selected are sent "as is" to the device without parsing, validating, or signing of the file by MobileIron. For more information, see "Configuration profile settings (iOS, tvOS, and macOS)" in the *MobileIron Core Device Management Guide for iOS and macOS Devices*.
- **Supported certificate type values for iOS IKEv2 VPN configurations:** iOS VPN configurations using Internet Key Exchange version 2 (IKEv2) need to include a selected value from the following list of certificate types:
  - RSA
  - ECDSA256
  - ECDSA384
  - ECDSA512

For more information, see "IKEv2 (iOS Only)" in the "Managing VPN Settings" chapter of the *MobileIron Core Device Management Guide for iOS and macOS Devices*.

## MobileIron Threat Defense features

MobileIron Threat Defense protects managed devices from mobile threats and vulnerabilities affecting device, network, and applications. For information on MobileIron Threat Defense-related features, as applicable for the current release, see the *MobileIron Threat Defense Solution Guide for Core*, available on the [MobileIron Threat Defense for Core](#) Documentation Home Page at [MobileIron Community](#).

NOTE: Each version of the MobileIron Threat Defense Solution guide contains all MobileIron Threat Defense features that are currently fully tested and available for use on both server and client environments. Because of the gap between server and client releases, MobileIron releases new versions of the MobileIron Threat Defense guide as the features become fully available.



# Support and Compatibility for MobileIron Core 11.1.0.0

This section includes the components MobileIron supports with this release of MobileIron Core.

NOTE: This information is current at the time of this release. For MobileIron product versions released after this release, see that product version's [release notes](#) for the most current support and compatibility information.

## Support policy

MobileIron defines supported and compatible as follows:

TABLE 1. DEFINITIONS FOR SUPPORTED AND COMPATIBLE

<b>Supported product versions</b>	The functionality of the product and version with currently supported releases was systematically tested as part of the current release and, therefore, will be supported.
<b>Compatible product versions</b>	The functionality of the product and version with currently supported releases has not been systematically tested as part of the current release, and therefore not supported. Based on previous testing (if applicable), the product and version is expected to function with currently supported releases.

## MobileIron end of sale and support policy

For details on the MobileIron end of sale and support policy, go to <https://community.mobileiron.com/docs/DOC-1089>.



# MobileIron Core support and compatibility

This version of MobileIron Core is supported and compatible with the following product versions:

- SAML / Identity Provider
- LDAP
- Hardware appliances
- Atlas
- Reporting database
- Monitor
- Sentry
- Access
- Android
- iOS
- macOS
- tvOS
- Windows

## SAML / Identity Provider

TABLE 2. SAML / IDENTITY PROVIDER SUPPORTED AND COMPATIBLE PRODUCTS AND COMPONENTS

Product / Component	Supported	Compatible
SAML / Identity Provider	<ul style="list-style-type: none"><li>• OpenSAML 3.3.0</li><li>• ADFS 3.0</li><li>• Okta - Developer Account 3.6.0</li><li>• Ping Identity – Trial version 1.3.0</li><li>• OneLogin – Developer Account</li></ul>	<ul style="list-style-type: none"><li>• Shibboleth</li></ul>



## LDAP

TABLE 3. LDAP SUPPORTED AND COMPATIBLE PRODUCTS AND COMPONENTS

Product / Component	Supported	Compatible
LDAP	<b>Windows Active Directory</b> <ul style="list-style-type: none"><li>• Server OS: Windows Server 2003, Version: 5.2</li><li>• Server OS: Windows Server 2008, Version: 6.1</li><li>• Server OS: Windows Server 2012R2, Version: 6.3</li></ul> <b>IBM Domino Server</b> <ul style="list-style-type: none"><li>• Server OS: Windows Server 2008, Version: 8.5.2</li></ul>	Not applicable

## Hardware appliances

TABLE 4. HARDWARE APPLIANCES SUPPORTED AND COMPATIBLE PRODUCTS AND COMPONENTS

Product / Component	Supported	Compatible
Hardware appliances	<ul style="list-style-type: none"><li>• M2200 (Core and Enterprise Connector)</li><li>• M2250 (Core)</li><li>• M2600 (Core)</li></ul>	Not applicable

## Atlas

TABLE 5. ATLAS SUPPORTED AND COMPATIBLE PRODUCTS AND COMPONENTS

	Supported	Compatible
Atlas	End of life. See <a href="https://community.mobileiron.com/docs/DOC-1666">https://community.mobileiron.com/docs/DOC-1666</a>	Not applicable



## Reporting database

TABLE 6. REPORTING DATABASE SUPPORTED AND COMPATIBLE PRODUCTS AND COMPONENTS

Product / Component	Supported	Compatible
Reporting Database	2.0.0.2	1.8.0.0, 1.8.0.2, 1.9.0.0, 1.9.1.0, 2.0.0.0, 2.0.0.1

## Monitor

TABLE 7. MONITOR SUPPORTED AND COMPATIBLE PRODUCTS AND COMPONENTS

Product / Component	Supported	Compatible
Monitor	2.0.0.2	1.1.0, 1.1.1, 1.2.0, 1.2.1, 2.0.0, 2.0.0.1

## Sentry

TABLE 8. SENTRY SUPPORTED AND COMPATIBLE PRODUCTS AND COMPONENTS

Product / Component	Supported	Compatible
Standalone Sentry	9.12.0	9.8.1, 9.9.0
Integrated Sentry	6.4.0	6.2.0–6.3.0

## Access

TABLE 9. ACCESS SUPPORTED AND COMPATIBLE PRODUCTS AND COMPONENTS

Product / Component	Supported	Compatible
MobileIron Access	R45	Not applicable, because only the latest version is available to all customers.



## Android

TABLE 10. ANDROID SUPPORTED AND COMPATIBLE PRODUCTS AND COMPONENTS

Product / Component	Supported	Compatible
Android	8.0, 8.1, 9.0, 10.0, 11.0	5.0–7.1
Mobile@Work	11.0.0.0, 11.1.0.0	9.3.0.0–10.8.0.0
Tunnel (Android native, Android Enterprise, and Samsung Knox Workspace)	4.5.0, 4.6.0	4.3.0, 4.3.2, 4.4.0
Secure Apps Manager	9.1.0.0	8.3.0.0–9.0.0.0
Email+ (Android AppConnect and Android Enterprise)	2.19.0.0 3.9.0	2.2.0.0–2.18.3.0 3.0.0–3.8.0
Docs@Work (Android AppConnect and Android Enterprise)	2.13.0	2.0.0–2.12.0
Web@Work (Android AppConnect)	2.5.1	2.1.0–2.4.2
Insight	End of support. See <a href="https://community.mobileiron.com/docs/DOC-9343">https://community.mobileiron.com/docs/DOC-9343</a>	Not applicable

## iOS

TABLE 11. iOS SUPPORTED AND COMPATIBLE PRODUCTS AND COMPONENTS

Product / Component	Supported	Compatible
iOS	12.0.0–14.0.0	11.0.0
Mobile@Work	12.11.1, 12.11.10* * Mobile@Work 12.11.10 for iOS is targeted to release on March 3, 2021.	12.0.0–12.4.0
Tunnel	4.1.0	2.4.1–4.0.0
Email+	3.16.0	2.6.0–3.15.1





TABLE 11. iOS SUPPORTED AND COMPATIBLE PRODUCTS AND COMPONENTS (CONT.)

Product / Component	Supported	Compatible
Docs@Work	2.16.0	2.2.0–2.15.1
Web@Work	2.12.0	2.0.0–2.11.1
Apps@Work Container app	Not supported	<ul style="list-style-type: none"> <li>• 1.1.2–1.2.0 when using Mobile@Work 8.6.0, 9.0.1, or 9.1.0</li> <li>• 1.3.0 when using Mobile@Work 9.5.0</li> </ul>
Help@Work	NOTE: Help@Work does not work on iOS 10 through the latest release as supported by MobileIron. Use TeamViewer App instead for Help@Work support.	2.0.2–2.1.1
Insight	End of support  See <a href="https://community.mobileiron.com/docs/DOC-9343">https://community.mobileiron.com/docs/DOC-9343</a> .	Not applicable

## macOS

TABLE 12. macOS SUPPORTED AND COMPATIBLE PRODUCTS AND COMPONENTS

Product / Component	Supported	Compatible
macOS/OS X	11.0	10.1–10.15
Tunnel	4.1.0	3.0.0, 4.0.0

## tvOS

TABLE 13. tvOS SUPPORTED AND COMPATIBLE PRODUCTS AND COMPONENTS

Product / Component	Supported	Compatible
tvOS	13.4, 14.0	12.4–13.4



## Windows

TABLE 14. WINDOWS SUPPORTED AND COMPATIBLE PRODUCTS AND COMPONENTS

Product / Component	Supported	Compatible
Windows	Windows 10 Pro, Windows 10 Enterprise (version 20H2)	<ul style="list-style-type: none"> <li>• Windows 10 Pro, Windows 10 Enterprise (versions 1703, 1709, 1809, 1903, 1909, 2004)</li> <li>• Windows HoloLens (versions 1701, 1803)</li> </ul> <p>Note The Following:</p> <ul style="list-style-type: none"> <li>• With 1803, Apps@Work cannot be pushed to the device because of a known Microsoft issue.</li> <li>• MobileIron recommends that customers stay on the 09 branches of Windows 10 to ensure a longer support lifecycle. The 09 versions of the OS have a 30-month support lifecycle from Microsoft, while the 03 versions only have an 18-month support lifecycle. For more information, see <a href="https://support.microsoft.com/en-us/help/13853/windows-lifecycle-fact-sheet">https://support.microsoft.com/en-us/help/13853/windows-lifecycle-fact-sheet</a>.</li> </ul>
Apps@Work	9.6.0.256	Not applicable (all listed versions are tested and supported)
Tunnel	1.2.3	1.2.0, 1.2.2



# Supported browsers and browser resolutions

The current version of MobileIron Core has the following browser support:

TABLE 15. SUPPORTED BROWSERS AND BROWSER RESOLUTIONS

Browser	Supported	Compatible
Internet Explorer	11	9*, 10*
Chrome	88	85, 86, 87
Firefox	85	82, 83, 84
Safari	Not supported	10.1*
Edge	Not supported	Not compatible
Chrome - iPad	Not supported	Not compatible
Safari - iPad	Not supported	Not compatible

\* This configuration is not covered under the MobileIron product warranty.

## Supported browser resolutions

TABLE 16. SUPPORTED BROWSER RESOLUTIONS

Browser resolution	Supported	Compatible
800x600	No	No
1024x768	No	Yes*
1280x1024	Yes	Yes
1366x768	Yes	Yes
1440x900	Yes	Yes
Higher resolutions	No	Yes

\* This configuration is not covered under the MobileIron product warranty.



# Language support

MobileIron Core supports the following languages on devices for messages and apps:

- [Language support for MobileIron Core messages](#)
- [Language support on Android and Android Enterprise devices](#)
- [Language support on iOS and macOS devices](#)
- [Language support on Windows devices](#)

## Language support for MobileIron Core messages

MobileIron Core supports the following languages for messages sent to devices:

- Chinese (Simplified)
- Chinese (Traditional)
- Dutch (Netherlands)
- English
- French (France)
- German (Germany)
- Italian (Italy)
- Japanese
- Korean
- Polish
- Portuguese (Brazilian)
- Romanian (Romania)
- Russian
- Slovak
- Spanish (Latin American)



## Language support on Android and Android Enterprise devices

Refer to *Mobile@Work for Android Release Notes* for a complete list of supported languages for Android and Android Enterprise devices.

## Language support on iOS and macOS devices

Refer to *Mobile@Work for iOS Release Notes* for a complete list of supported languages for iOS and macOS devices.

## Language support on Windows devices

MobileIron Core supports the following languages in client apps on Windows devices:

- Chinese (Simplified)
- Chinese (Traditional)
- English
- French (France)
- German (Germany)
- Japanese
- Korean
- Portuguese (Brazilian)
- Russian
- Spanish (Latin American)



# Resolved issues

For resolved issues provided in previous releases, see the "Resolved issues" sections in the release notes for those releases, available in [MobileIron Core Product Documentation](#).

This release includes the following resolved issues:

- **VSP-64477:** There was an issue where the Apps@Work page was not displaying correctly on iOS 13.5.1 and 14.3 devices. This issue has been fixed. The Apps@Work page now displays correctly on iOS 13.5.1 and 14.3 devices.
- **VSP-64374:** There was an issue where failure by the Core server to obtain an authentication token during Android Enterprise device registration was automatically considered as a maximum number of devices registered for the user account error. This has been fixed. A generic failure message is sent to the Mobile@Work client if the failure to obtain the authentication token is not related to the maximum number of devices error.
- **VSP-64293:** There was an issue where the Core server required a Google Play enterprise mobile management (EMM) API call to ensure that Mobile@Work for Android Enterprise (AE) devices would upgrade automatically. Failure of this call could lead to a failed AE registration. This issue has been fixed in Core 11.0.0.1 through the most recently released version as supported by MobileIron. The API call is no longer required, reducing the chance of AE registration failure.
- **VSP-64248:** There was an issue when Google Account configuration was pushed to devices, there were problems with the account name and account description. The issue has been fixed. Google Account configuration information can be pushed to devices successfully.
- **VSP-64227:** There was an issue with the Apps@Work "Featured" banner not working in Apple devices running iOS 14.2. This issue has been fixed. Devices running iOS 14.2 can see the Featured banner from Core 11.1.0.0 through the most recently released version as supported by MobileIron.
- **VSP-64156:** There was an issue where simple message service (SMS) and call log archives required a Tomcat process restart to update. This issue has been fixed. SMS and call log archives update without restarting.
- **VSP-64065:** There was an issue with a possible memory leak when sending simple message service (SMS) logs and call logs to a Simple File Transfer Protocol (SFTP) server. This issue has been fixed. You can send SMS and call logs to an SFTP server without incident.



- **VSP-64029:** There was an issue where a Wi-Fi configuration could not be saved or edited if it contained a proxy variable password setting. This issue has been fixed. Wi-Fi configurations can now be saved and edited when containing a proxy variable password setting.
- **VSP-63942:** There was an issue with Core showing the device password status for some Android 11.0 devices as non-compliant, although the device password was compliant. This issue has been fixed. Core correctly reports the password compliance status for these Android devices, from Core 11.1.0.0 through the most recently released version as supported by MobileIron.
- **VSP-63852:** There was an issue with Core using hypertext transfer protocol (HTTP) for Apple iTunes lookup and search requests. This issue has been fixed. Apple iTunes lookup and search request are now sent using secure HTTP (HTTPS) protocol.
- **VSP-63822:** There was an issue where internal delays were causing the Tomcat process to time out when restarting Core. This issue has been fixed. Tomcat now starts up as expected when restarting.
- **VSP-63749:** There was an issue in which devices running iOS 14 have Wi-Fi MAC address randomization on by default, which is not supported for Mobile@Work managed devices. This issue has been fixed. When clients upgrade to iOS 14, a Wi-Fi configuration with MAC address randomization disabled will be re-pushed to the device to disable the option.
- **VSP-63746:** MobileIron Core deployments in Hybrid mode (both Android Open Source Project (AOSP) and Android Enterprise) were not displaying the AOSP badge for in-house apps. This issue has been fixed. The AOSP badge now displays as expected.
- **VSP-63599:** There was an issue where, when a security policy was saved for the first time (with or without changes), it would re-push the Wi-Fi profile and regenerate certificates. This issue has been fixed. The first time you save a security policy, it behaves as expected, from Core 11.1.0.0 through the most recently released version as supported by MobileIron.
- **VSP-63588:** There was an issue with out-of-date iOS system apps. This issue has been fixed. The updated iOS system apps list can be reinstalled from Core.
- **VSP-63303:** There was an issue where Core was checking for iOS operating system updates in all iOS devices. This issue has been fixed. Core now checks for iOS operating system updates in all supervised iOS devices.
- **VSP-62936:** There was an issue where Mobile@Work clients registered to a Connected Cloud server displayed the **My Devices** tab when it was not expected behavior to display. This issue has been fixed.
- **VSP-46090:** There was an issue where Core was not rejecting passwords longer than the value configured for max-allowed-length (currently 32 characters). This issue has been fixed. Core checks that passwords



are not longer than the configured maximum allowed length, providing better protection against denial of service (DOS) attacks.

## Known issues

For known issues found in previous releases, see the "Known issues" sections in the release notes for those releases, available in [MobileIron Core Product Documentation](#).

This release includes the following known issues:

- **VSP-64632:** There is an issue whereby macOS devices registered using International Roaming Expert Group (iREG) or Apple Automated Device Enrollment (DEP) cannot subsequently register to Mobile@Work, because the Wi-Fi MAC address is not reported properly to Core. There is no workaround.  
**NOTE:** Other macOS devices are not affected.
- **VSP-64566:** There is an issue where Android Open Source Project (AOSP) devices are unable to set up Email+ because a required identity certificate is not being pushed to Mobile@Work. There is no workaround.
- **VSP-64583:** There is an issue where Core 11.1.0.0 can support no more than 10,000 Lightweight Directory Access Protocol (LDAP) group edit requests. There is no workaround. For more information about LDAP groups, see the "Managing Users" chapter of *Getting Started with MobileIron Core*.
- **VSP-64521:** There is an issue with Security Assertion Markup Language (SAML)-enabled devices where, if "Anonymous" is the authentication type selected in their enrollment profile, Core incorrectly registers the device user as "Anonymous."  
**Workaround:** Select either Password or PIN authentication type to avoid this error.
- **VSP-64471:** There is an issue where new Mobile@Work options to enable Zips anti-phishing protection on the personal side of devices are not accessible when added as a Public App and enabled for Android Enterprise.  
**Workaround:** If Mobile@Work is added as an in-house app, these restrictions are displayed in Android Open Source Project (AOSP) mode.
- **VSP-64390:** There is an issue where, when an LDAP configuration is associated with 10,000 or more groups, there may sometimes be a slow response or timeout of the user interface while rendering the list.
- **VSP-64375:** There is an issue where Core fails to save Android device details, which could break the Android Enterprise, MTD activation, and other functions which rely on device details. This issue occurs





when:

- An invalid license key is used in the MTD activation configuration
- A colon ( : ) character is used in the configuration name

**Workaround:** Enter a valid license key for MTD, and do not use colons in the configuration file name.

- **VSP-64191:** The LDAP Sync function cannot import more than 1000 organizational unit (OU) objects. Thus, some OU objects can be missing on the LDAP user management page.

**Workaround:** Assign roles based on LDAP group.

- **VSP-64188:** There is an issue where, if there are MobileIron Sentry devices on the network that have attachment control enabled, Core also sends the encryption key in the Docs@Work configuration to Sentry devices that do not have attachment control enabled.
- **VSP-64123:** There is an issue where bulk enrollment of iOS devices fails after the Core to Cloud migration service upgrade.
- **VSP-63798:** There is an issue in the Core App Catalog, in which only the primary "version" value of an app displays, and the "alt\_version" value does not. This can occasionally cause the App Catalog page to list what looks like the same app twice, even though their alt\_version values differ.



# MobileIron Core upgrade information

This section describes the following upgrade information for the current release of MobileIron Core.

NOTE: MobileIron Core and Enterprise Connector should be running the same version and the same build.

- [Support community](#)
- [MobileIron Core upgrade readiness checklists](#)
- [Check disk space availability](#)
- [MobileIron Core upgrade paths](#)
- [MobileIron Core upgrade URL](#)
- [Backing up MobileIron Core](#)
- [MobileIron Core end of sale and support policy](#)

## Before you begin

Read [Before you upgrade](#) .

## Support community

Use the information in this section for upgrade information specific to this release. For detailed instructions on how to upgrade MobileIron Core using this upgrade information, refer to the MobileIron Core System Manager Guide, available in [MobileIron Core Product Documentation](#).

## MobileIron Core upgrade readiness checklists

This section provides checklists to help you successfully complete the upgrade process for Core and Sentry software. The checklists include:

- [Pre-Upgrade checklist](#)
- [Upgrade considerations](#)
- [Post-Upgrade checklist](#)

### Pre-Upgrade checklist

Before you upgrade, we encourage you to do a pre-upgrade checklist.



TABLE 17. PRE-UPGRADE CHECKLIST

Check	Tasks	References
	Prepare and plan for downtime	<ul style="list-style-type: none"> <li>• Core (1 - 3 hours)</li> <li>• Sentry (5 - 20 minutes)</li> </ul>
	Review relevant documentation	<a href="#">Core product documentation page</a>
	Check certificates	<ul style="list-style-type: none"> <li>• iOS Enrollment, Portal HTTPS, Client TLS certificates</li> </ul> <p>NOTE: When using mutual authentication, the Portal HTTPS certificate must be a publicly trusted certificate from a well-known Certificate Authority. For details, see "Mutual authentication between devices and MobileIron Core" in the <i>MobileIron Core Device Management Guide</i>.</p> <ul style="list-style-type: none"> <li>• MDM Certificate (check a month before expires)</li> <li>• Local CA</li> </ul> <p><b>Knowledge Base article:</b> <a href="#">Renewing an expired local CA certificate.</a></p>
	Check Boot partition	<p>Verify you have at least 35 MB free for /boot. See <a href="#">Check disk space availability</a> in this document for details on how to perform this check.</p> <p><b>Knowledge Base article:</b> <a href="#">Core Upgrade: Increase Boot Partition to 1GM if Avail Space is less than 35MB.</a></p>
	Ensure there is enough disk space	<ul style="list-style-type: none"> <li>• Old File System (2 GB /mi and 5 GB /mi/files)</li> <li>• New File System (10 GB /mi)</li> </ul> <p><b>Knowledge Base article:</b> <a href="#">Resizing Disk Partition of a Core Virtual Machine.</a></p>
	Check for new system requirements	<ul style="list-style-type: none"> <li>• Minimum 80 GB hard drive</li> <li>• If there is insufficient storage, increase the available disk space using the procedure outlined in <a href="#">Resizing Disk Partition of a Core Virtual Machine</a></li> <li>• Call MobileIron support if issues persist when physical appliances and VMs have the minimum required disk space configured</li> <li>• Port 8443 for Summary MICS - MobileIron Configuration Service (that is, the service that supports System Manager.)</li> </ul>
	Review your backup and high availability options	<ul style="list-style-type: none"> <li>• Physical backup: built in backup, showtech all</li> <li>• VMware backup: VDMK backup, snapshot</li> <li>• High Availability: confirm HA version 2.0</li> </ul>



TABLE 17. PRE-UPGRADE CHECKLIST (CONT.)

Check	Tasks	References
		<p><b>Knowledge Base article:</b> <a href="#">How to tell if your Core has HA 2.0</a>                      If using HA 1.0, contact MobileIron Professional Services to upgrade to 2.0.</p>
	Set up your proxy configuration (if required)	Manually set the upgrade URL and use HTTP instead of HTTPS.
	Prepare test devices	<ul style="list-style-type: none"> <li>• <b>Client:</b> Get clean test devices, open client and check-in, check iOS log</li> <li>• <b>Core:</b> Note the watchlist and label numbers</li> </ul>

## Upgrade considerations

After the pre-upgrade planning, we recommend you review the following considerations:

TABLE 18. UPGRADE CONSIDERATIONS

Check	Considerations	References
	DB Schema and Data	Run pre-validation check after downloading the repository from System Manager. If this task fails, contact MobileIron Support.
	Understand the stages	<ul style="list-style-type: none"> <li>• Download vs. Stage for install</li> <li>• Reboot when the system displays: Reboot to install <a href="https://&lt;serverFQDN&gt;:8443/upgrade/status">https://&lt;serverFQDN&gt;:8443/upgrade/status</a></li> </ul>
	Leverage CLI upgrade commands (as appropriate)	<a href="#">MobileIron Core Command Line Interface (CLI) Reference</a>
	Understand scenario options	<ul style="list-style-type: none"> <li>• Single server</li> <li>• High availability:                             <ul style="list-style-type: none"> <li><b>Option 1:</b> little downtime: 1) upgrade secondary 2) upgrade primary</li> <li><b>Option 2:</b> zero downtime: 1) upgrade secondary 2) failover to secondary 3) upgrade primary 4) re-establish sync</li> </ul> </li> </ul> <p><b>Download guide:</b> <i>MobileIron Core High Availability Management Guide</i>  <b>Review section:</b> HA Core Software Upgrade Procedures</p>
	Monitor the upgrade	<ul style="list-style-type: none"> <li>• Log into the Admin Portal</li> <li>• Select <b>Logs &gt; MDM Logs &gt; States &gt; Waiting xml generation pending</b></li> <li>• Monitor upgrade status using:</li> </ul>



TABLE 18. UPGRADE CONSIDERATIONS (CONT.)

Check	Considerations	References
		<a href="https://&lt;serverFQDN&gt;:8443/upgrade/status">https://&lt;serverFQDN&gt;:8443/upgrade/status</a>
	Additional reboot	Due to a kernel upgrade, an additional reboot is performed when you upgrade. It may take longer than expected for MobileIron Core to become available on the network.
	Upgrade impact on Windows devices	In some cases, when an administrator initiates Reset PIN for a Windows Phone 10 device, the device does not return a new pin for that device.  For more information, see the following knowledge base article: <a href="https://help.mobileiron.com/s/article-detail-page?id=kA134000000QxnLCAS">https://help.mobileiron.com/s/article-detail-page?id=kA134000000QxnLCAS</a>
	Ports	HTTPS/ port 443 is the default port for fresh installations, but upgraded environments keep the previous port open, for example, port 8080.

## Post-Upgrade checklist

MobileIron recommends the following checklist after completion of the upgrade.

TABLE 19. POST-UPGRADE CHECKLIST

Check	Tasks	References
	Testing and troubleshooting	<ul style="list-style-type: none"> <li>Log into the System Manager</li> <li>Select Maintenance &gt; Software Updates &gt; Software Version</li> <li>Verify that the new version is listed</li> <li>DO NOT re-boot the system once the upgrade process has begun</li> <li>Call MobileIron Support for further investigation</li> </ul>
	Verify services	<ul style="list-style-type: none"> <li>Log into the Admin Portal</li> <li>Select Services &gt; Overview</li> <li>Click Verify All</li> </ul>
	Verify devices	<ul style="list-style-type: none"> <li>Register a new device</li> <li>Re-enroll/check-in existing devices</li> </ul>
	HA system cleanup	<ul style="list-style-type: none"> <li>Set secondary back to secondary</li> <li>Confirm sync</li> </ul>



# Check disk space availability

Before you upgrade, check disk space availability. **At least 35 MB of disk space must be available in the /boot folder for an upgrade to be successful.**

If at least 35 MB of disk space is not available in the /boot folder, contact MobileIron Technical Support before proceeding with the upgrade.

Use one of the following methods to check disk space availability:

## The CLI command: show system disk

The following sample output shows the available disk space in the last line. It is 15M in this example.

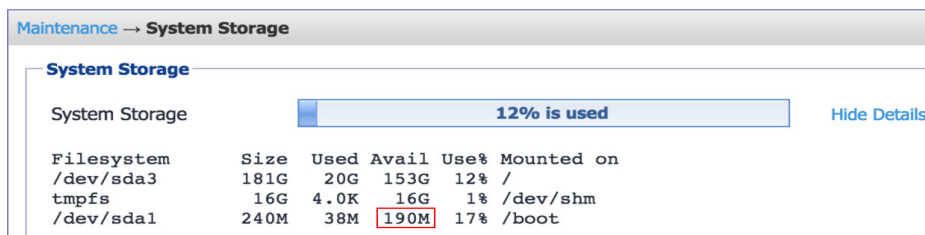
```
CORE(8.5.0.1a-6)@host.company.com#show system disk
Filesystem Size Used Avail Use% Mounted on
/dev/sda3 181G 20G 153G 12% /
tmpfs 16G 4.0K 16G 1% /dev/shm
/dev/sda1 95M 76M 15M 84% /boot
```

## The System Manager

The System Manager > Maintenance > System Storage menu shows you how much Core system storage you are using, and how much is still available.

### Procedure

1. In the System Manager, go to **Maintenance > System storage**.
2. Click **More Details** next to the System Storage bar that shows percent used.
3. In this example, the available disk space is 190M.



Filesystem	Size	Used	Avail	Use%	Mounted on
/dev/sda3	181G	20G	153G	12%	/
tmpfs	16G	4.0K	16G	1%	/dev/shm
/dev/sda1	240M	38M	190M	17%	/boot



## MobileIron Core upgrade paths

MobileIron recommends the following upgrade paths, which are fully tested and supported.

### Supported upgrade paths to Core 11.1.0.0

- 10.8.0.0 → 11.1.0.0
- 10.8.0.1 → 11.1.0.0
- 11.0.0.0 → 11.1.0.0
- 11.0.0.1 → 11.1.0.0
- 11.1.0.0 (GMRC) → 11.1.0.0

## MobileIron Core upgrade URL

To upgrade MobileIron Core:

Use the following URL if you specify an alternate URL:

<https://support.mobileiron.com/mi/vsp/11.1.0.0-32/mobileiron-11.1.0.0-32>

## Backing up MobileIron Core

MobileIron recommends you make a local backup of MobileIron Core before starting an upgrade. For more information on backing up MobileIron Core, see the [MobileIron Core System Manager Guide](#).

## MobileIron Core end of sale and support policy

For details on the MobileIron Core end of sale and support policy, go to: <https://help.mobileiron.com/s/article-detail-page?Id=kA134000000QyXYCA0>



# Enterprise Connector upgrade information

This section describes the following upgrade information for the current release of Enterprise Connector.

- [Enterprise Connector upgrade overview](#)
- [MobileIron Enterprise Connector upgrade paths](#)
- [Enterprise Connector upgrade URL](#)
- [Enterprise Connector upgrade notes](#)

## Enterprise Connector upgrade overview

Use the information in this section for upgrade information specific to this release. In most cases, Enterprise Connector is upgraded automatically after a MobileIron Core upgrade. Core upgrades include any new service package necessary for Enterprise Connector. If Connector needs to be updated, then Core prompts Connector to access the new package and complete an in-place upgrade. In most cases, this process completes successfully, and Connector restarts.

If there is a problem with the in-place upgrade, then Connector makes two additional attempts to complete the upgrade. Connector reboots before attempting to upgrade again. If the upgrade is still not successful, then Connector reverts to the previous version and begins running in compatibility mode. In this case, you must complete the manual upgrade steps detailed in the [On-Premise Installation Guide](#).

## MobileIron Enterprise Connector upgrade paths

Direct upgrade from only the following Enterprise Connector versions to version 11.1.0.0 is supported:

### Supported upgrade paths to 11.1.0.0

- 10.8.0.0 → 11.1.0.0
- 10.8.0.1 → 11.1.0.0
- 11.0.0.0 → 11.1.0.0
- 11.0.0.1 → 11.1.0.0
- 11.1.0.0 (GMRC) → 11.1.0.0

If you are upgrading from a version not listed here, then you need to complete one or more previous upgrades first. See the upgrade guide for that version.





## Enterprise Connector upgrade URL

Use the following URL if you specify an alternate URL:

Upgrades from supported Connector releases:

<https://support.mobileiron.com/mi/connector/11.1.0.0-32/mobileiron-11.1.0.0-32>

## Enterprise Connector upgrade notes

There are no Enterprise Connector upgrade notes for this release.



## Documentation errata

This section includes content updates that were made after the current version of the *MobileIron Core Device Management Guide for iOS and macOS Devices* had been finalized. These updates are detailed here for reference, and will be available in the next version of the *MobileIron Core Device Management Guide*.

### Correction to Apple device enrollment profile settings

This section describes the changes made to the description of the "Apple device enrollment profile settings" table in the "Managing Devices Enrolled in Apple Device Enrollment" section in the *MobileIron Core Device Management Guide for iOS and macOS Devices*.

TABLE 20. INCORRECT DESCRIPTION (HIGHLIGHTED)

<b>Enable SAML</b>	<p>As part of DEP profile, the MDM server provides custom enrollment URL along with standard URL to get the MDM profile to Apple server. This URL can be used to enforce your own authentication model or to provide any other information.</p> <p>Select this to support external IdP with DEP enrollment.</p> <p>This feature is applicable for iOS 13.0 and macOS 10.15 devices through the latest version as supported by MobileIron.</p> <p>Note The Following:</p> <ul style="list-style-type: none"><li>• You must have SAML enabled. (See "Configuring SAML/IdP support" in the <i>MobileIron Core System Manager Guide</i>.) If the IdP has not been configured properly, and is not reachable, the <b>Enable SAML</b> check box will not display.</li><li>• Once set up for SAML on iReg or DEP devices, you will not be able to disable SAML from the System Manager. You must first de-select <b>SAML-based registration</b> in the Device Registration page before you can disable the IdP SAML connection in the System Manager.</li></ul>



TABLE 21. CORRECT DESCRIPTION (HIGHLIGHTED)

<b>Enable SAML</b>	<p>As part of DEP profile, the MDM server provides custom enrollment URL along with standard URL to get the MDM profile to Apple server. This URL can be used to enforce your own authentication model or to provide any other information.</p> <p>Select this to support external IdP with DEP enrollment.</p> <p>This feature is applicable for iOS 13.0 and macOS 10.15 devices through the latest version as supported by MobileIron.</p> <p>Note The Following:</p> <ul style="list-style-type: none"> <li>• You must have SAML enabled. (See "Configuring SAML/IdP support" in the <i>MobileIron Core System Manager Guide</i>.) If the IdP has not been configured properly, and is not reachable, the <b>Enable SAML</b> check box will not display.</li> <li>• Once set up for SAML on iReg or DEP devices, you will not be able to disable SAML from the System Manager. You must first de-select <b>Enable SAML</b> in the Device Registration page before you can disable the IdP SAML connection in the System Manager.</li> </ul>

## Documentation resources

MobileIron product documentation is available at <https://help.mobileiron.com/s/mil-productdocumentation>.

