MobileIron Core and Connector 11.0.0.0 Release and Upgrade Notes

Revised February 25, 2021

For complete product documentation see:
MobileIron Core Documentation Home Page

Revision history

TABLE 1. REVISION HISTORY

Date	Revision
December 8, 2020	Known issue VSP-64029 added.
December 16, 2020	Re-added Support and Compatibility section, deleted broken link.
December 21, 2020	Updated Support and Compatibility section.
February 25, 2021	Note added that Android anti-phishing requires MobileIron Tunnel 4.6.0.

Contents

Revision history **3**

About MobileIron Core **7**

Before you upgrade **7**

Understand the impact of TLS protocol changes 7

New features and enhancements summary **9**

General features and enhancements 9

Enhancements to the self-service user portal (SSP) 10

Additional enhancements 12

Android and Android enterprise features and enhancements 13

iOS and macOS features and enhancements 15

MobileIron Threat Defense features 16

Support and Compatibility **17**

Support policy 17

MobileIron end of sale and support policy 17

MobileIron Core support and compatibility 17

SAML / Identity Provider 18

LDAP 18

Hardware Appliances 19

Atlas 19

Reporting database 19

Monitor 19

Sentry 19

Access 20

Android 20

iOS 21

macOS 21

tvOS 22

Windows 22
Supported browsers 22
Supported browser resolutions 23
Language support 23
Language support for MobileIron Core messages 24
Language support on Android and Android enterprise devices 24
Language support on iOS and macOS devices 24
Language support on Windows devices 25
Resolved issues 26
Known issues 28
Limitations 29
MobileIron Core upgrade information 30
Support community 30
MobileIron Core upgrade readiness checklists 30
Pre-Upgrade checklist 30
Upgrade considerations 32
Post-Upgrade checklist 33
Check disk space availability 34
The CLI command: show system disk 34
The System Manager 34
MobileIron Core upgrade paths 34
MobileIron Core upgrade URL 35
Backing up MobileIron Core 35
MobileIron Core end of sale and support policy 35
Enterprise Connector upgrade information 36
Enterprise Connector upgrade overview 36
MobileIron Enterprise Connector upgrade paths 36
Enterprise Connector upgrade URL 37
Enterprise Connector upgrade notes 37

Documentation resources **37**

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.

NOTE: The Core 10.8.0.0 release was the last of the MobileIron Core 10-series releases. The next release in the Core series is 11.0.0.0.

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 CoreConnected Cloud. 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.

- **Microsoft Intune Device Compliance Support added:** MobileIron Core now supports Microsoft Intune device compliance. Organizations can update the device compliance status in the Microsoft Azure Active Directory (AAD.) Using conditional access from AAD, if the device is non-compliant, administrators can block the device from accessing apps. By connecting Core to Microsoft Azure, administrators will be able to use the device compliance status of MobileIron's managed devices for conditional access to Microsoft 365 apps. In Core, administrators will see the following changes:
  - The System Settings page has a new menu item in the left navigational pane > Microsoft Azure > Device Compliance for iOS & Android. There are new fields to assist with the reporting of device compliance status to Microsoft Azure.
  - Administrators can direct device users to a specific Enrollment URL and Remediation URL. If a URL is not provided, a default URL is automatically provided by Core.
  - Once the setup is completed, Core is connected to Microsoft Azure.
  - A Partner Device Compliance policy (under Policies) needs to be created and applied to the device group that reports the device compliance to Azure.
  - In Devices & Users > Devices > Advanced Search drop down > Common Fields section, five new fields have been added:

- Azure Client Status Code
- Azure Device Compliance Report Status
- Azure Device Compliance Report Time
- Azure Device Compliance Status
- Azure Device Identifier

- The ability to de-provision the Azure account has been added.
- All activity of adding, editing, and deactivating an account are recorded in the Logs.
  For more information, see "Azure Tenant" and "Advanced searching" in the *MobileIron Core Device Management Guide for Android and Android enterprise Devices* or in the *MobileIron Core Device Management Guide for iOS and macOS Devices*.

Enhancements to the self-service user portal (SSP)

- **Default language selection now includes self-service user portal pages**: From Core 11.0.0.0 through the most recently released version as supported by MobileIron, when you change the Core default language in the Settings > General > Language page, your selection also changes all the self-service user portal (SSP) pages, as well. This is an enhancement to previous releases, when not all SSP pages displayed in the selected language. For more information, see the Language Support section of the *MobileIron Core Device Management Guide* for your operating system.

  NOTE: The portal will, by default, attempt to detect the default language of the end user device and display the correct language. Otherwise, the portal displays the selected default language. To have all client devices view the SSP in the same language, regardless of the user device language, make sure the DETECT USER LANGUAGE option is OFF. This will force all users to the default language selection.

- **Option to "Trust" or "Untrust" mac and iOS devices in self-service user portal**: Mobile@Work users can temporarily elevate or downgrade the trust level of their device, depending upon the surrounding conditions. The following new options are available from the self-service user portal (SSP) **Devices** page:
  - **Untrust**: Select this option to temporarily remove confidential information and applications from the device. When the device is trusted (the default), the user will see the **Untrust** option. Use this option before entering a location where device security may be at higher than normal risk, such as in airports.
  - **Trust**: When the device is untrusted, the user will see the Trust option. Use this option when no unusual device security risks exist.

  For more information, see the section "Trust and Untrust options" in the "Self-service User Portal" chapter of the *MobileIron Core Device Management Guide for iOS and macOS Devices*.

- **Improved auto-detect of device type and browser during registration**: MobileIron has improved the auto-detection of devices and browsers as part of MobileIron client registration. Core uses this information to

provide appropriate guidance to users registering their devices.

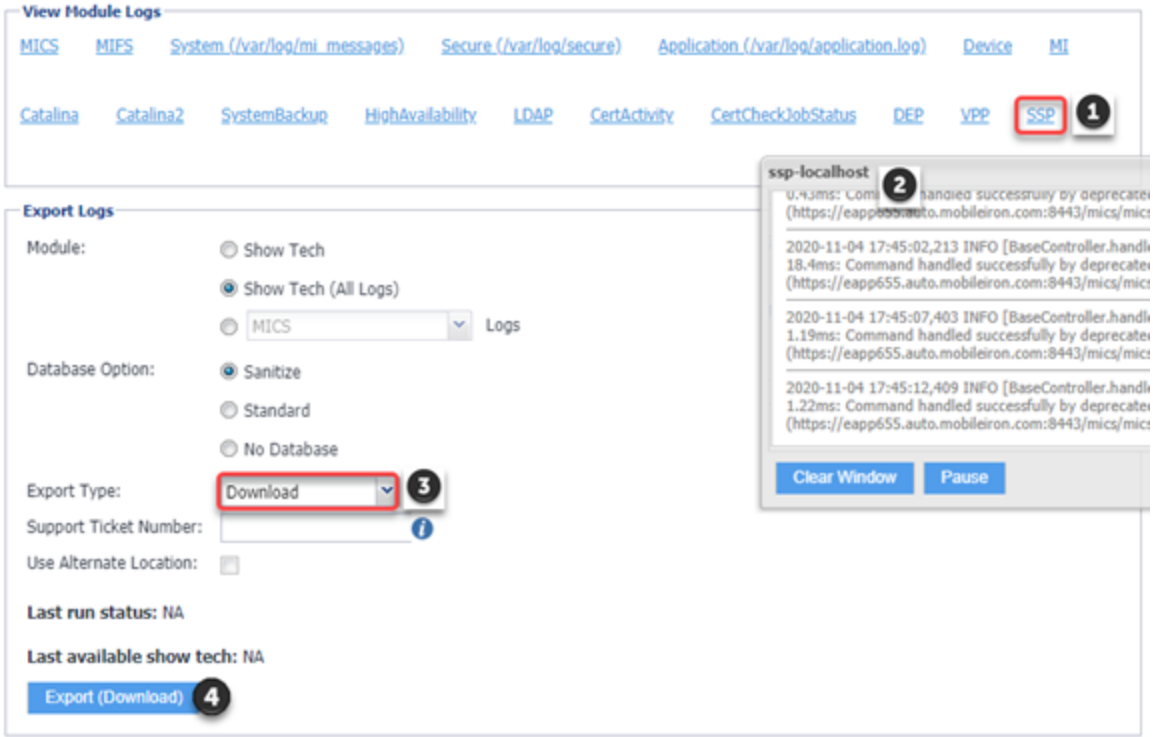
- **Customize iOS self-service user portal "Request Registration PIN" message**: You can now customize and set defaults in the "Request Registration PIN" page of the iOS self-service user portal. For more information, see "Customizing the request registration PIN page" in the *MobileIron Core Device Management Guide for iOS and macOS Devices*.

- **Self-service portal enhancements for ADA Section 508**: The self-service user portal (SSP) user interface in Core 11.0.0.0 through the latest release as supported by MobileIron has been enhanced to enable screen readers to render text and image content as intended. This is to increase compliance with the Americans with Disabilities Act (ADA) Section 508.

- **API support for self-service user portal**: This release provides several public APIs that you can use to provide self-service portal functionality from within your user interface. See the *MobileIron Core v2 API Guide* for complete details.

- **SSP-related log files now available**: With this release, you can view and download self-service user portal (SSP)-related log files from the **System Manager > Troubleshooting > View Module Logs** page.

FIGURE 1. VIEWING AND DOWNLOADING SSP LOG FILES



  - To view the SSP-related logs, click the new **SSP** link in the View Module Logs section. A scrolling window opens, displaying the log files.

- To download the SSP-related logs, enter your criteria in the Export Logs section. Select **Download** as the Export type (HTTP and SFTP are not supported at this time). Click **Export**.

For more information about log files, see "Working with logs" section of the *MobileIron Core System Manager Guide*.

- **Set Time Zone:** The administrator can now set the time zone for one or more devices from within the Device Details page using the Actions > Set Time Zone option. The time zone device action is also displayed in the Device Details page of a device. This feature is applicable to iOS 14.0 and tvOS 14.0 through the latest version as supported by MobileIron. For more information, see "Setting the time zone of a device" in the *MobileIron Core Device Management Guide* for your operating system.

- **Send email when using the Wipe or Cancel Wipe command on a device:** Administrators now have the ability to customize or suppress emails that are automatically generated when a **Wipe** command or **Cancel Wipe** command is sent. The **Send notification of wipe to registered user** field is useful for users that have multiple devices. The email notification helps prevent confusion to device users who may think Core is wiping their current, active device. For more information, see "Wipe" or "Cancel Wipe" in the *MobileIron Core Device Management Guide* for your operating system.

Additional enhancements

- **System Manager Self Diagnosis disabled after upgrade**: The System Manager feature Self Diagnosis (**System Manager >Maintenance > Self-Diagnosis**) is no longer supported, and has been removed with this release.

- **Sentry configuration updated to support OAuth redirect**: In MobileIron **Core > Services > Sentry**, under **Server Authentication**, whenever ActiveSync is enabled, the following options are available:
  - **Basic Auth** only
  - **OAuth Auth** only
  - **Basic Auth** and **OAuth**

  This feature is supported on MobileIron Sentry, targeted to release in December 2020. For more information about configuring OAuth on MobileIron Sentry, see "Device and Server Authentication" in the *MobileIron Sentry Guide for MobileIron Core*.

- **Support for VMWare ESXi 6.7 and ESXi 7.0 hypervisor software**: Core and Connector ISO can be deployed on VMWare ESXi 6.7 and ESXi 7.0 hypervisor software from Core 11.0.0.0 through the most recently released version as supported by MobileIron. For more information see "Virtual Core requirements" in the *On-Premise Installation Guide for MobileIron Core and Enterprise Connector 11.0.0.0*.

- **Help Desk telephone numbers now accept up to 24 digits**: In the **Settings > System Settings > General > Helpdesk > Contact(s)** field, the length of a valid telephone number has been expanded from

15 digits to 25 characters total:

- 24 digits for numbers beginning with the + symbol.
- 22 digits for numbers without the + symbol.

For more information, see "Configuring help desk contact information" in the *MobileIron Core Device Management Guide* for your operating system.

- **Support to enable/disable FIDO (Fast IDentity Online) authentication**: The new user interface for Zero Sign-on can be enabled from MobileIron **Core > Policies and Configs > Policies > SaaS**. Use the toggle button to enable or disable the interface. This feature is supported on Access 44, targeted to release in December 2020.

- **View 100+ Win32 apps on Windows 10 devices:** For Windows 10 devices with more than 100 Win32 apps, the App inventory is updated in the database. You can view this inventory in the Device Details > Apps page. For more information, see "Privacy policies" in *Getting Started with MobileIron Core* and "Installed Apps Device Details page" in the *MobileIron Core Apps@Work Guide*.

- **New options to restrict Device Registration:** New options for device registration are provided that allow administrators to restrict which devices can register with MobileIron Core. The restrictions are based on the enrollment type and the options are available on the Admin Portal in Settings > Users & Devices > Device Registration. For more information, see "Restricting device registration by enrollment type" in the *Getting Started with MobileIron Core*.

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.

- **Existing Tunnel configurations support MTD anti-phishing**: For devices that already have Tunnel for Android configured, you can continue to use the existing Tunnel configuration for anti-phishing support with MTD. Anti-phishing support with Tunnel and MTD is supported with Tunnel 4.6.0 for Android. For more information see *MobileIron Tunnel for Android Guide for Administrators*.

- **New field added to Privacy policies:** In the Privacy policy, a new field has been added - Prompt User to Enable Location Services if Wi-Fi/MTD configuration is pushed (Android enterprise.) Administrators have the ability to prompt device users to enable the device's location setting. This setting is useful if the device user resides in a country that has GDPR requirements. During the registration process, the device user is prompted to enable the location setting. If the device user does not grant permission, the configuration will fail. For more information, see "Enabling Android enterprise" in the *MobileIron Core Device Management Guide for Android and Android enterprise Devices*. See also "Privacy Policies" in the *Getting Started with MobileIron Core.*

- **Support for closed network / AOSP deployment:** There are situations where the onboarding, registration and management of devices is limited and requires a different approach. Examples of these kinds of situations are:
    - In an environment that does not have connectivity to Google mobile services (GMS) due to restrictions in the organization or due to a closed network.
    - In countries where Google mobile services are not available.
    - Where devices that do not have Google mobile services but vendors have enabled Android Enterprise AOSP (Android Open Source Project.)

  With the 11.0.0.0 release, MobileIron Core now supports a new mode of deployment:
    - Integrated deployment (GMS/Non-GMS) - the entire Core instance serves devices in full Android enterprise mode (for example, Samsung devices) and also devices that do not have GMS (for example, AR/VR devices.)

  This feature applies to Android 6 devices through the latest version as supported by MobileIron. For more information, see "Setting up Core with a closed network / AOSP deployment" in the *MobileIron Core Device Management Guide for Android and Android enterprise Devices*.

- **Support for app restrictions with in-house applications for Android non-GMS devices:** For devices registered to Core in a non-GMS mode, administrators can apply in-house app restrictions to these devices. Administrators can also distribute those apps and its configurations as in-house applications directly to Mobile@Work clients without using Google mobile services. For more information, see "App restrictions with in-house applications for Android" in the *MobileIron Core Apps@Work Guide*.

- **New warning banner added to Privacy Policy:** For Android devices, in the default Privacy Policy, administrators can add a warning banner that displays upon device reboot. This is helpful for companies that require all approved mobile operating systems, such as Android 9.0, to be managed according to a security baseline / guidance. Device users will see the warning banner upon device reboot and will have to acknowledge it before continuing use of the device. For more information, see "Privacy Policies" in *Getting Started with MobileIron Core*.

- **Limit Android device registration by Allowed or Blocked devices**: You can create Allowed or Blocked device registration lists from the **Settings > System Settings > Users & Devices > Device Registration > Restrictions for Android > Allow/Blocked devices** list. When you click either **Create a list of Allowed devices** or **Create a list of Blocked devices**, a device table opens, where you can enter specific device information that will, when matched, either allow the requesting device to register or block it. Blocked devices receive a pop-up message: "Unable to complete registration (Invalid Manufacturer). Please contact your administrator."

  For more information, see "Registering Android devices" in the *MobileIron Core Device Management Guide for Android and Android enterprise Devices*.

- **Common Criteria and alphanumeric device passcode:** An alphanumeric device password is no longer a requirement for Common Criteria mode for Android devices. The following settings are required to enable the Common Criteria mode:
    - Device Encryption is enabled
    - SD Card Encryption is enabled
    - Password history is disabled
    - Max password failed attempts is greater than 0

  For information about these settings, see Security policies in *Getting Started with MobileIron Core*.

iOS and macOS features and enhancements

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

- **Field name changed in Google Account configuration for iOS devices:** Previously, a field titled "Google User's Full Name," was added to the Google Account Configuration dialog box. This field name has been changed to "Google Account Name." When an email is sent from this Google account, the name entered here displays who the email is from. Upgrading from previous releases will fill in the name as per the configuration. This field used to be a required field, and it is now an optional field for adding or updating an iOS Google Account Configuration. For more information, see "Google Account" in the *MobileIron Core Device Management Guide for iOS and macOS Devices*.
- **Three new restrictions for iOS:** The following fields have been added to iOS restrictions in the iOS / tvOS > Restrictions configuration page.
    - **Allow Personalized Advertising** (iOS 14.1 through the latest version as supported by MobileIron)
    - **Allow NFC** (iOS 14.2 through the latest version as supported by MobileIron)
    - **Force Dictation Processing Only on Device** (iOS 14.3 through the latest version as supported by MobileIron)

  For more information, see "iOS and tvOS restrictions settings" in the *MobileIron Core Device Management Guide for iOS and macOS Devices*.
- **New Skip option for Device Enrollment Profiles:** A new option has been added to allow devices to **Skip the App Store pane** during the registration of an Automated Device enrollment device. For more information, see "Creating Apple Device Enrollment profiles" in the *MobileIron Core Device Management Guide for iOS and macOS Devices*.
- **New workflow to install management profile for macOS 11.0 and above:** During iReg device registration, when the device users begin registering their devices with macOS 11.0 and later versions as supported by MobileIron Core, users are prompted with a message that the management profile has been

downloaded. To install the profile, device users need to install the downloaded profile, go to System Preferences > Profiles, and then click Install. For more information, see "In-app Registration" in the *MobileIron Core Device Management Guide for iOS and macOS Devices*.

- **Notification preview type:** In the App Notifications Configuration, select a Preview Type to display in the device notification message previews. Select Never to prevent apps from displaying message previews in Notifications. Applicable to iOS 14.0 through the latest version as supported by MobileIron. For more information, see "Configuring notification settings" in the *MobileIron Core Device Management Guide for iOS and macOS Devices*.

- **New field in App Catalog - Prevent user from removing and offloading app:** Administrators can now prevent device users from removing a selected managed app (for example, Mobile@Work) and prevent the OS from offloading unused apps. When the device user tries to uninstall the app, a pop-up will state: "Uninstall Not Allowed - It is not possible to uninstall this app at this time." Administrators also have the option to allow device users to remove and uninstall the selected app. Applicable to iOS 14.0 through the latest version as supported by MobileIron. For more information, see "Using the wizard to import iOS apps from the Apple App Store" and "Using the wizard to add an in-house iOS or macOS app to the App Catalog" in the *MobileIron Core Apps@Work Guide*.

- **Extensible Single Sign-On:** MobileIron Core enables Extensible Single Sign-On with the following configurations: Extensible Single Sign-On and Extensible Single Sign-On Kerberos. The implementation requires an app extension, such as Microsoft Authenticator, from the identity provider. With an Extensible Single Sign-On implementation, device users need to only authenticate once when accessing enterprise resources. Device users are not prompted to authenticate for subsequent log in. A single sign-on configuration using Extensible Single Sign-On does not require a Tunnel or Sentry deployment. For more information, see "Extensible Single Sign-On" and "Extensible Single Sign-On Kerberos" in 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

The information in 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 2. DEFINITIONS FOR SUPPORTED AND COMPATIBLE

Supported product versions	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.
Compatible product versions	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

SAML / Identity Provider	Supported	Compatible
	• OpenSAML 3.3.0 • ADFS 3.0 • Okta - Developer Account 3.6.0 • Ping Identity – Trial version 1.3.0 • OneLogin – Developer Account	• Shibboleth

LDAP

LDAP	Supported	Compatible
	Windows Active Directory • Server OS: Windows Server 2003, Version: 5.2 • Server OS: Windows Server 2008, Version: 6.1 • Server OS: Windows Server 2012R2, Version: 6.3 **IBM Domino Server** • Server OS: Windows Server 2008, Version: 8.5.2	Not applicable

Hardware Appliances

Hardware Appliances	Supported	Compatible
	• M2200 (Core and Enterprise Connector) • M2250 (Core) • M2600 (Core)	Not applicable

Atlas

Atlas	Supported	Compatible
	End of Life. See https://community.mobileiron.com/docs/DOC-1666	Not applicable

Reporting database

Reporting Database	Supported	Compatible
	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

Monitor	Supported	Compatible
	2.0.0.2	1.1.0, 1.1.1, 1.2.0, 1.2.1, 2.0.0, 2.0.0.1

Sentry

Sentry	Supported	Compatible
Standalone Sentry	9.9.0	9.7.3, 9.8.1
Integrated Sentry	6.4.0	6.2.0–6.3.0

Access

Access	Supported	Compatible
MobileIron Access	R43	Not applicable, because only the latest version is available to all customers.

Android

Android	Supported	Compatible
Android	8.0, 8.1, 9.0, 10.0, 11.0	5.0–7.1
Mobile@Work	10.8.0.0, 11.0.0.0	9.3.0.0–10.7.0.0
Tunnel (Android native, Android enterprise, and Samsung Knox Workspace)	4.5.0	4.3.0, 4.3.2, 4.4.0
Secure Apps Manager	9.0.0.0	8.3.0.0–8.9.0.0
Email+ (Android AppConnect and Android enterprise)	2.19.0.0 3.7.0	2.2.0.0–2.18.3.0 3.0.0–3.6.0
Docs@Work (Android AppConnect and Android enterprise)	2.12.0	2.0.0–2.11.0
Web@Work (Android AppConnect)	2.5.0	2.1.0–2.4.2
Insight	End of Support. See https://community.mobileiron.com/docs/DOC-9343	Not applicable

iOS

iOS	Supported	Compatible
iOS	12.0.0–14.0.0	11.0.0
Mobile@Work	12.4.0, 12.5.0	12.0.0–12.3.0
Tunnel	4.1.0	2.4.1–4.0.0
Email+	3.15.1	2.6.0–3.15.0
Docs@Work	2.15.1	2.2.0–2.15.0
Web@Work	2.11.1	2.0.0–2.11.0
Apps@Work Container app	Not supported	• 1.1.2–1.2.0 when using Mobile@Work 8.6.0, 9.0.1, or 9.1.0 • 1.3.0 when using Mobile@Work 9.5.0
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 https://community.mobileiron.com/docs/DOC-9343.	Not applicable

macOS

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

tvOS

tvOS	Supported	Compatible
tvOS	13.4, 14.0	12.4-13.4

Windows

Windows	Supported	Compatible
Windows	Windows 10 Pro, Windows 10 Enterprise (versions 1909, 2004)	• Windows 10 Pro, Windows 10 Enterprise (versions 1703, 1709, 1809, 1903) • Windows HoloLens (versions 1701, 1803) Note The Following: • With 1803, Apps@Work cannot be pushed to the device because of a known Microsoft issue. • 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 https://support.microsoft.com/en-us/help/13853/windows-lifecycle-fact-sheet.
Apps@Work	9.6.0.256	Not applicable (All listed versions are tested and supported)
Tunnel	1.3.0	1.2.0, 1.2.2, 1.2.3

Supported browsers

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

TABLE 3. SUPPORTED BROWSERS AND BROWSER RESOLUTIONS

Browser	Supported	Compatible
Internet Explorer	11	9*, 10*
Chrome	86	85, 84, 83
Firefox	82	79, 80, 81
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

The current version of MobileIron Core supports the following browser resolutions:

TABLE 4. 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-63802**: There was an issue in which Core was unable to load Android Firmware Policy data correctly after upgrading from Core 10.7.0.0 to Core 10.8.0.0. This issue has been fixed.
- **VSP-63721**: There was an issue where the system would time out when retrieving log files relating to certificate management. This issue has been fixed. The timeout value for the retrieval of certificate management logs has been increased to 120 seconds.
- **VSP-63420**: There was an issue where the Assemble script was not able to connect to Core in release 10.8.0.0, due to changes in the login page. This issue has been fixed.
- **VSP-63375**: There was an issue with the "Auto Update this App" option in Android Apps, where it did not work as expected. This issue has been fixed. The "Auto Update this App" option in Android Apps is no longer available when adding or editing apps.
- **VSP-63366**: There was an issue where the Exchange configuration values **OAuthSignInURL** and **OAuthTokenRequestURL** were required fields when the OAuth option was selected. This issue has been fixed. These configuration values are optional, and no longer required fields when OAuth is selected.
- **VSP-63309**: There was an issue where, when multiple devices were selected from the user interface for a software update (Actions->iOS and Macos-> **Update OS Software**), the operation failed. This issue has been fixed.

  Workaround: To avoid this problem in earlier releases, update software on a single device, instead of multiple devices at a time.
- **VSP-63209**: There was an issue where the equipment identifier (EID) did not show up as an iOS attribute when a device list was exported to spreadsheet (CSV) format. This issue has been fixed. Now, the EID and mobile EID (MEID) (when present) are prefixed by an EID string or MEID string, respectively.
- **VSP-63120**: There was an issue where volume purchase plan (VPP) Apple license sync would fail if the license token value was more than 256 characters. This issue has been fixed.
- **VSP-63092**: There was an issue where Apps@Work would display a notification that an iOS app update was available when no update was available. This issue has been fixed.

- **VSP-63088**: Previously, when an admin assigned the roles "View device page" and "Device details" logged into the Spaces page, an erroneous pop-up message appeared, which the admin could dismiss. This issue has been fixed.

- **VSP-63027**: There was an issue where removing the Android enterprise configuration from a device that had the same reg_uuid number and username as another device did not retire the older device. This issue has been fixed.

- **VSP-63004**: There was an issue where MobileIron Core could not retrieve health attestation data from Microsoft Windows devices. This issue has been fixed.

- **VSP-62993**: There was an issue where status updates in Exchange using Integrated Sentry would fail if there were duplicate Device ID entries for the same mailbox in the Active Sync Association page. This issue has been fixed.

- **VSP-62967**: There was an issue where TeamViewer would fail its validation check when using Firefox or Chrome browsers. This issue has been fixed.

- **VSP-62937**: There was an issue where, when the Honeywell OEM configuration app was configured for wireless wide-area network (WWAN) settings and enabled for Android Enterprise devices, the App Details page did not display information correctly. This issue has been fixed.

- **VSP-62382**: There was an issue where, if the Sentry server could not be reached while updating compliance data, Core generated a NullPointer Exception error. The issue has been fixed.

- **VSP-62004**: There was an issue where Android device registrations were failing on Core servers with both Federal Information Processing Standards (FIPS) and SafetyNet Attestation API enabled. This issue has been resolved.

- **VSP-61009**: There was an issue where, when iOS or macOS devices performed a twice-a-day scan for operating system (OS) updates, the information was not captured, and the **Device Details > Available OS Updates** field displayed "Unavailable." This issue has been fixed. From Core 11.0.0.0 through the latest release as supported by MobileIron, iOS devices running OS 9 or higher, and macOS devices running OS 10.11 or higher can receive the results of the OS update scan and display the correct status information in the "Available OS Updates" field.

- **VSP-52178**: There was an issue where the HTTP OPTIONS method (which requests permitted communication options for a given URL or server) was being used in some situations, despite security concerns. This issue has been fixed. The HTTP OPTIONS method is now disabled in Core.

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-64029**: A Wi-Fi configuration cannot be saved or edited if it contains a proxy variable password setting.
- **VSP-63883**: If a device in Device Admin mode is assigned an Android Enterprise configuration with the Android Open Source Project (AOSP) flag enabled, the configuration remains in "Pending" state.
- **VSP-63848**: Administrators deploying devices in Airgapped/Android Open Source Project (AOSP) mode as a Shared Kiosk cannot initiate the admin device action to sign out of the Kiosk, due to the dependency of this capability on Google accounts.
- **VSP-63746**: Mobileiron Core deployments in Hybrid mode (both Android Open Source Project (AOSP) and Android Enterprise) will not see the AOSP badge displayed for in-house apps.
- **VSP-63713**: The Android application package (.APK) file for the Google Chrome app cannot be uploaded as an in-house app and generates the following error message: "App 'com.android.chrome_ xxxxxxxxx.apk' import failed: Error while handling file resources."
- **VSP-63628**: There is an issue with Microsoft Azure generating incorrect error messages during tenant onboarding when the property "Allow only TSL / SSL connection certified by trusted CA's" is enabled.
  Workaround: To avoid this error, add root certificates for all outbound request URLs to the Trusted Root Certificate page in MobileIron Core.
- **VSP-63413**: There is an issue when Core Administration pages are opened in a Chrome browser, on a Windows device with Integration Touch enabled. If you click the last entry of the **Safari Domains** list, you will be returned to the top of the page.
- **VSP-63303**: Core checks for iOS operating system updates every 12 hours in all iOS devices. Expected behavior is that only supervised iOS devices should be making this check.
- **VSP-58532**: The Terms of Service (ToS) page does not display during client registrations if the device has been previously registered, deleted, and then re-registered.

Limitations

For limitations found in previous releases, see the "Limitations" sections in the release notes for those releases, available in MobileIron Core Product Documentation.

This release includes the following third-party limitations.

- **VSP-63455**: The Microsoft Azure Consent page (the place where you sign in to Azure) might stop responding when accessed from the Safari browser, leaving the incorrect impression that consent was not successful. This is a Microsoft known issue.
  Workaround: Close the page and return to Core. To avoid the issue, use Chrome browser for accessing Azure.

- **VSP-63072**: On some Android devices, disabling Chrome from System Apps causes Mobile@Work to crash.
  Workaround: Exclude Chrome when attempting to disable, hide, or quarantine apps.

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 availablity
- 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 5. PRE-UPGRADE CHECKLIST

Check	Tasks	References
	Prepare and plan for downtime	• Core (1 - 3 hours) • Sentry (5 - 20 minutes)
	Review relevant documentation	Core product documentation page
	Check certificates	• iOS Enrollment, Portal HTTPS, Client TLS certificates 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 *MobileIron Core Device Management Guide*. • MDM Certificate (check a month before expires) • Local CA **Knowledge Base article**: Renewing an expired local CA certificate.
	Check Boot partition	Verify you have at least 35 MB free for /boot. See Check disk space availability in this document for details on how to perform this check. **Knowledge Base article**: Core Upgrade: Increase Boot Partition to 1GM if Avail Space is less than 35MB.
	Ensure there is enough disk space	• Old File System (2 GB /mi and 5 GB /mi/files) • New File System (10 GB /mi) **Knowledge Base article**: Resizing Disk Partition of a Core Virtual Machine.
	Check for new system requirements	• Minimum 80 GB hard drive • If there is insufficient storage, increase the available disk space using the procedure outlined in Resizing Disk Partition of a Core Virtual Machine • Call MobileIron support if issues persist when physical appliances and VMs have the minimum required disk space configured • Port 8443 for Summary MICS - MobileIron Configuration Service (that is, the service that supports System Manager.)
	Review your backup and high availability options	• Physical backup: built in backup, showtech all • VMware backup: VDMK backup, snapshot • High Availability: confirm HA version 2.0

TABLE 5. PRE-UPGRADE CHECKLIST (CONT.)

Check	Tasks	References
		Knowledge Base article: How to tell if your Core has HA 2.0 If using HA 1.0, contact MobileIron Professional Services to upgrade to 2.0.
	Set up your proxy configuration (if required)	Manually set the upgrade URL and use HTTP instead of HTTPS.
	Prepare test devices	• **Client**: Get clean test devices, open client and check-in, check iOS log • **Core**: Note the watchlist and label numbers

Upgrade considerations

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

TABLE 6. 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	• Download vs. Stage for install • Reboot when the system displays: Reboot to install https://<serverFQDN>:8443/upgrade/status
	Leverage CLI upgrade commands (as appropriate)	MobileIron Core Command Line Interface (CLI) Reference
	Understand scenario options	• Single server • High availability: **Option 1**: little downtime: 1) upgrade secondary 2) upgrade primary **Option 2**: zero downtime: 1) upgrade secondary 2) failover to secondary 3) upgrade primary 4) re-establish sync **Download guide**: *MobileIron Core High Availability Management Guide* **Review section**: HA Core Software Upgrade Procedures
	Monitor the upgrade	• Log into the Admin Portal • Select **Logs > MDM Logs > States > Waiting xml generation pending** • Monitor upgrade status using:

TABLE 6. UPGRADE CONSIDERATIONS (CONT.)

Check	Considerations	References
		https://<serverFQDN>:8443/upgrade/status
	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: https://help.mobileiron.com/s/article-detail-page?Id=kA134000000QxnLCAS
	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 7. POST-UPGRADE CHECKLIST

Check	Tasks	References
	Testing and troubleshooting	• Log into the System Manager • Select Maintenance > Software Updates > Software Version • Verify that the new version is listed • DO NOT re-boot the system once the upgrade process has begun • Call MobileIron Support for further investigation
	Verify services	• Log into the Admin Portal • Select Services > Overview • Click Verify All
	Verify devices	• Register a new device • Re-enroll/check-in existing devices
	HA system cleanup	• Set secondary back to secondary • Confirm sync

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.

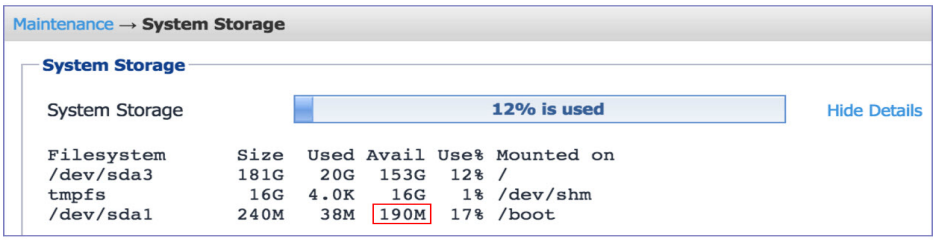
```
CORE(8.5.0.1a-6)@host.company.com#show system disk
Filesystem Size Used Avail Use% Mounted on
/dev/sda3 181G 20G 153G 12% /
tmpfs 16G 4.0K 16G 1% /dev/shm
/dev/sda1 95M 76M 15M 84% /boot
```

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.



MobileIron Core upgrade paths

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

Supported upgrade paths to Core 11.0.0.0

- 10.7.0.0 → 11.0.0.0
- 10.7.0.1 → 11.0.0.0
- 10.8.0.0 → 11.0.0.0
- 11.0.0.0 (GMRC) → 11.0.0.0

MobileIron Core upgrade URL

To upgrade MobileIron Core:

Use the following URL if you specify an alternate URL:

https://support.mobileiron.com/mi/vsp/11.0.0.0-30/mobileiron-11.0.0.0-30

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 11.0.0.0 is supported:

Supported upgrade paths to 11.0.0.0

- 10.7.0.0 → 11.0.0.0
- 10.7.0.1 → 11.0.0.0
- 10.8.0.0 → 11.0.0.0
- 11.0.0.0 (GMRC) → 11.0.0.0

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/11.0.0.0-30/mobileiron-11.0.0.0-30

Enterprise Connector upgrade notes

There are no Enterprise Connector upgrade notes for this release.

Documentation resources

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