MobileIron Core and Connector 10.8.0.0 Release and Upgrade Notes

Revised: December 21, 2020

For complete product documentation see:
MobileIron Core Documentation Home Page

Revision history

TABLE 1. REVISION HISTORY

Date	Revision
October 29, 2020	Updated Support and compatibility section.
December 21, 2020	Updated Support and compatibility section.

Contents

Revision history **3**

About MobileIron Core **6**

Before you upgrade **6**

Understand the impact of TLS protocol changes 6

New features and enhancements summary **7**

General features and enhancements 8

Android and Android enterprise features and enhancements 11

iOS and macOS features and enhancements 13

MobileIron Threat Defense features 15

Support and compatibility **16**

Support policy 16

MobileIron end of sale and support policy 16

MobileIron Core support and compatibility 17

SAML / Identity Provider 17

LDAP 17

Hardware Appliances 18

Atlas 18

Reporting database 18

Monitor 18

Sentry 19

Access 19

Android 19

iOS 20

macOS 21

tvOS 21

Windows 22

Supported browsers and browser resolutions 22

Supported browser resolution 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 24
Resolved issues **25**
Known issues **27**
Limitations **28**
MobileIron Core upgrade information **29**
Support community 30
MobileIron Core upgrade readiness checklists 30
Pre-Upgrade checklist 30
Upgrade considerations 31
Post-Upgrade checklist 32
Check disk space availability 33
The CLI command: show system disk 33
The System Manager 33
MobileIron Core upgrade paths 34
MobileIron Core upgrade URL 34
Backing up MobileIron Core 34
MobileIron Core end of sale and support policy 34
Enterprise Connector upgrade information **34**
Enterprise Connector upgrade overview 35
MobileIron Enterprise Connector upgrade paths 35
Enterprise Connector upgrade URL 35
Enterprise Connector upgrade notes 36
Documentation resources **36**

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.

NOTE: Upgrade to Integrated Sentry 6.4.0 before upgrading to Core 10.3.0.0. Integrated Sentry 6.4.0 supports 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.

- **Filter users by LDAP OU in device registration, Spaces, and Labels**: You can now include Lightweight Directory Access Protocol (LDAP) Organizational Units (OU) within Space and Label criteria, restricting the results to the users in that OU. This feature set includes the following updates:

  - **Updated LDAP Sync**: LDAP Sync now returns all LDAP OU information. This information is used to correlate users in the Core to their OU's. It syncs only the OU information itself, not all the OU user information, which would affect performance. See "Synchronizing with the LDAP server" in *Getting Started with MobileIron Core*.

    NOTE: This behavior differs from sync to a Group, which does fetch all the group user information.

  - **LDAP OUs in space and label criteria**: You can now create device spaces and labels based on LDAP OUs. There is a new attribute in the **Admin > Device Spaces > New Admin Space >** “Field” menu: **Organizational Units > LDAP Organizational Unit Distinguished Name** (OUDN). If you select this option, a list of LDAP Organizational Units populates the right-hand drop-down menu, from which you can configure your criteria. See "Searchable fields" in the "Creating device spaces and assigning administrators" section of the *MobileIron Delegated Administration Guide*.

  - **LDAP OUs in device criteria for single device registrations**: You can now restrict single device registration queries to users within an LDAP OU. If there is an LDAP OU included in the Space criteria, the **Devices & Users > Devices > Add Device > User** field will be constrained to that OU (similar to Group behavior). See "Single device registration" in the "Managing Devices" section of *Getting Started with MobileIron Core.*

    Similarly, if an LDAP OU is part of the space criteria, the following LDAP Entities listing pages will also limit the entries to users within that LDAP OU:

    - LDAP Entities > LDAP Users
    - LDAP Entities > Authorized LDAP Entities
    - LDAP Entities > LDAP OU
    - LDAP Entities > LDAP group (only those belonging to the LDAP OU)

    For more information, see:

    - "Filtering users by OUs and groups" in the *MobileIron Core Delegated Administration Guide*.
    - "Single device registration" in the Managing Devices section of *Getting Started with MobileIron Core*.

  - **LDAP OUs in device criteria for bulk device registrations**: If an LDAP OU or Group is part of the Space criteria, the users in the comma-separated values (CSV) file will be matched against it. From

the **Devices & Users > Devices > Add Multiple Devices** menu, enter a CSV file and click **Apply** to see the restricted list of users. If the user isn't in the OU, "User not found" displays in the Message column for that user. For more information, see "Bulk device registration" in the *MobileIron Core Getting Started Guide*.

NOTE: Bulk device registration fails when using a comma-separated values (CSV) file with more than 2000 device entries.

- **Automatic device retirement capability for unused devices**: MobileIron Core now supports automatic device retirement for unused devices. You can enable this feature from the **Settings > Users & Devices > Retire and Delete Devices > Retire and Delete Retired Devices** page. You have the following device retirement options:
  - Retire devices that have been inactive for more than 30 days (this field is configurable).
  - Open a list of devices that have not checked in.
  - Retire up to a configured maximum number of devices per session (default is 100).
  - Create a schedule to retire devices going forward.

  Scheduling options include:
  - **Frequency**: Daily, weekly, or monthly
  - **Start time**: Default start time is midnight.

  Retired and deleted devices are listed in the Admin portal Devices page. The Devices page also includes a link to a list of qualified devices that can be retired. For more information, see "Retiring and deleting unused and retired devices" in the *MobileIron Core Device Management Guide* for your operating system.

- **MobileIron Core banner informing of desktop capability on Cloud:** If there are any Windows or Mac devices enrolled in Core, a banner displays along the top of the Core UI: "MobileIron offers comprehensive features for Desktop Management on Cloud platform. Try our Cloud solution today." Clicking on the supplied link opens to the MobileIron 30-day free UEM Cloud software page. Administrators can dismiss the banner by selecting the check box "Don't show again" and clicking the "Close" button.

- **Shorter certification lifetimes for self-signed TLS certificates**: Beginning September 1, 2020, Apple requires that valid Transport Layer Security (TLS) certificates expire in 397 days or less. From Core 10.8.0.0 through the latest release supported by MobileIron, the lifespan of self-signed TLS certificates will be limited to fewer than 398 days. See "Certificates you configure in the System Manager" section of the *MobileIron Core System Manager Guide*.

- **Mobile@Work self-service user portal customization improvements**: The Mobile@Work self-service user portal (SSP) has new customization options and capabilities for enabled users. This feature set includes the following updates:

- **QR code-based device registration**: A new option to the Mobile@Work Self-service home page allows users to scan a QR code that will take them through device registration. Users now have the option of receiving registration information by SMS message and email, or by scanning a generated QR code. When users log into the self-service user portal home page, they can click one of two registration buttons:
  - **Send Invitation** – Receive registration information by SMS message and email.
  - **Generate QR Code** – Scan to be redirected to the appropriate registration page.

  Users scan the QR code and are redirected to a browser to enter their pin or password:
  - iOS users: Once authenticated, iReg profile installation starts, completing device registration.
  - Android users: Once authenticated, the user is redirected to Google Play to download the registration app. Users open the app to complete device registration.

  NOTE: Users must be assigned appropriate roles to use the SSP. See "Assigning user portal device management roles" in the Self-service user portal chapter of the *MobileIron Core Device Management Guide* for your operating system.

  For more information, see "If QR-code registration is enabled" in the Self-service user portal chapter of the *MobileIron Core Device Management Guide* for your operating system.

- **Cascading style sheets and custom background colors**: The self-service user portal has new customization options, including editable cascading style sheets (CSS) and custom background colors. The features are available on the **Settings > System Settings > Users & Devices > Registration** page. For full information, see "Customizing the self-service user portal" in the *MobileIron Core Device Management Guide* for your operating system.

- **End User Terms of Service agreements support text and language customization**: The Mobile@Work End User Terms of Service page can now be customized to conform to the languages and regulations in your operating region. From the **Settings > Users & Devices > Registration** page, click **Add+** in the End User Terms of Service section to open the **Add End User Terms of Service** dialog box. From here, you can select the language, country or region, agreement type, and agreement content text. An email address is required. Core generates an audit email when the user accepts the terms and conditions. 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.

- **Multiple alias and friendly name support for PFX/P12 user certificates**: MobileIron Core now supports the use of aliases and "friendly names" for .pfx and .p12 user certificates in the self-service user portal. For more information, see "About uploading certificates in the user portal" in the Self-service user portal chapter of the *MobileIron Core Device Management Guide* for your operating system.

- **View Activity displays user device history**: Mobile@Work users can access their audit/device history logs from the user portal. From the user portal **Welcome** drop-down menu, select **View Activity**. The device activity page opens, displaying search tools and a scrolling table of log entries. Users can access this page from their laptop and mobile devices. For more information, see "Viewing device history logs" in the Self-service user portal chapter of the *MobileIron Core Device Management Guide* for your operating system.

NOTE: Users must be assigned appropriate roles to use the SSP. See "Assigning user portal device management roles" in the Self-service user portal chapter of the *MobileIron Core Device Management Guide* for your operating system.

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 Android enterprise work profile mode**: With the introduction of Android 11, a new Android enterprise mode of deployment called **Work Profile on Company Owned Devices** has been added. The purpose of his new mode is to improve work profile support for company-owned devices by bringing robust asset management and personal usage restrictions to the work profile, while retaining the same privacy protections provided on personally-owned devices. Now IT organizations can deploy the work profile across all their devices regardless of who owns the device. This provides a consistent device user experience and privacy offering to all their employees, along with the management capabilities appropriate to the ownership of the device.

  The key benefit of this mode is to help IT organizations with two difficult choices:

  - Deploying work profiles to enable private personal use, at the expense of asset management and device usage controls crucial to keeping track of their costly devices
  - Deploying fully managed devices to retain those device-level controls, while sacrificing the privacy of personal use valued by organizations and employees alike

  This change only affects devices configured with Managed Device with Work Profile (COPE), provisioned on, or upgraded to Android 11. Work profiles are otherwise unaffected.

  Within Core, the naming terminology has changed. They are as follows:

  - Android versions 8-10: Managed Device with Work Profile (COPE)
  - Android 11 through the latest version as supported by MobileIron: Work Profile on Company Owned Device.

  Upon upgrade to Android 11, legacy work profiles on fully managed devices will be migrated automatically to the new work profile experience. Additionally, Android 11 will not support the provisioning of work profiles in Managed Device with Work Profile mode. Instead, customers can provision a work profile directly from a new or factory reset device and receive the asset management benefits and device controls required for managing company-owned devices, without the need to provision as a Managed Device with Work Profile as well.

For more information, see:

- *MobileIron Core Device Management Guide for Android and Android enterprise Devices*
- *MobileIron Core Apps@Work Guide*
- *Getting Started with MobileIron Core*

- **New registration status added to accommodate "Work Profile on Company Owned Devices" for Android 11 devices:** With the introduction of a new Android enterprise mode of deployment called Work Profile on Company Owned Devices for Android 11 devices, a new Registration Status is now supported in the Advanced Search, Tier Compliance policy and Label Evaluation. For more information, see "Advanced searching" in the *MobileIron Core Device Management Guide for Android and Android enterprise Devices*.
- **Mobile@Work client no longer supports in-house apps for Managed device with Work profile mode on Android 11 devices**: Upon upgrade to Android 11, the MobileIron Mobile@Work client no longer supports in-house apps for devices that migrate from Work Profile mode to Work Profile on Company Owned Devices mode. This also applies to new Android 11 devices provisioned as Work Profile on Company Owned Devices. For more information, see the following sections in the *MobileIron Core Apps@Work Guide*:
  - Features specific to Android enterprise apps
  - Adding in-house apps for Android
  - Public and private Android enterprise app deployment

- **Support for freeze period in system update:** Administrators can now freeze firmware updates for up to 90 days. This is helpful if your company needs time to figure out the migration plan for changing from Managed Device with Work profile (COPE) mode to Work Profile for Company Owned Device mode. Applicable to Android 11 devices in Device Owner mode and Android 9+ devices in Managed Device with Work Profile (COPE) mode. For more information, see "Setting the system update policy for Android devices" in the *MobileIron Core Device Management Guide for Android and Android enterprise Devices*.

- **Advanced Lock Task Features added:** The following advanced settings have been added to the **Enable Lock Task Mode** field in the New Android Kiosk App Setting Policy dialog box. These options are only applicable to Android 9 devices in Device Owner (DO) mode.
  - System Info: When selected, displays the date/time, connectivity, battery, vibration mode on the status bar.
  - Keyguard: Enables the keyguard in lock task mode.
  - Global Actions: Enables the menu that is displayed when the user long-presses the power button. If this option is disabled, the user may not be able to power off the device.
  - Home button: When enabled, displays the following sub-options:
    - Overview: Enables the Overview button and the Overview screen during lock task mode.
    - Notifications: Enables notifications during lock task mode.

  This includes notification icons on the status bar, heads-up. notifications, and the expandable notification shade.

Upon upgrade, existing policies get the above default settings. For more information, see "Setting kiosk policy for Android Managed devices" in the *MobileIron Core Device Management Guide for Android and Android enterprise Devices.*

- **Field name change:** The field titled **Enter Kiosk Mode Immediately** has been changed to **Enter Kiosk Mode Immediately on registration**. When selected, the device will go to Kiosk mode automatically upon registration. For more information, see "Setting kiosk policy for Android Managed devices" in the *MobileIron Core Device Management Guide for Android and Android enterprise Devices*.

iOS and macOS features and enhancements

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

- **GDPR-compliant SIM EID field added to Device Details page**: Administrators can now search for the SIM EID of a device by using the Advanced Search in Devices & Users > Device Detail page. The EID allows the carriers to assign the SIM to a specific device. Applicable to iOS 14.0 through the latest version of MobileIron.

  New GDPR fields (such as IP Address and SIM EID) are added over MobileIron Core releases. If administrators want to hide the new fields, the GDPR profile will need to be updated.

  For more information, see "Advanced Searching" in the *MobileIron Core Device Management Guide for iOS and macOS Devices.*

- **New field added to Google Account configuration for iOS devices:** A new field, **Google User's Full Name**, has been added to the Google Account Configuration dialog box. 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 is required when 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*.

- **Custom Device Enrollment added:** You can now use your own custom web interfaces to authenticate users during Device Enrollment. Display custom information such as authentication type, branding, consent text, and privacy policy in your custom web interface. For more information, see "Creating Apple Device Enrollment profiles" in the *MobileIron Core Device Management Guide for iOS and macOS Devices.*

- **Enrollment Customization added:** A new option is available in the Apple Device Enrollment profile that gives the option to provide a Custom Enrollment URL for authentication and any custom messaging (corporate messaging, privacy info, etc.) during Apple Device Enrollment. For more information, see "Adding a custom Automated Device Enrollment web page" in the *MobileIron Core Device Management Guide for iOS and macOS Devices*.

- **Two new distribution options added to configurations:** For macOS devices, administrators now have the option to choose to distribute the Wi-Fi and VPN configurations to either the **Device Channel** (effective for all users on a device) or the **User Channel** (effective only for the currently registered user on a device). Upon upgrade, for Wi-Fi configurations, the User Channel is the default selection. For VPN configurations, Device Channel is the default selection. For more information, see "Configuring new VPN settings" and "Wi-Fi settings" in the *MobileIron Core Device Management Guide for iOS and macOS Devices*.

- **Ability to specify individual syncing of Outlook Exchange items added:** A new field **Items to Synchronize (iOS)** was added to allow the administrator to specify individual syncing of Outlook items such as Email, Calendar, Contacts, Notes, and Reminders. For more information, see "Exchange Settings" in the *MobileIron Core Device Management Guide for iOS and macOS Devices*.

- **New restriction added for iOS 14.0 devices:** A new restriction has been added to **Configurations > Apple > iOS / tvOS > Restrictions: Allow App Clips**. This allows the device user to add App Clips onto the device.

  Upon upgrade, the new restriction displays in existing iOS configuration and are deselected by default. For more information, see "iOS and tvOS restrictions settings" in the *MobileIron Core Device Management Guide for iOS and macOS Devices*.

- **New restriction added for macOS 11.0 devices:** A new restriction has been added to **Configurations > Apple > macOS Only > macOS Restrictions: Delay App Software Update for x days.** This allows the administrator to specify the number of days to delay software updates. Upon upgrade, the new restriction displays in existing macOS configuration and are deselected by default. For more information, see "macOS settings" in the *MobileIron Core Device Management Guide for iOS and macOS Devices*.

- **New fields added to Device Enrollment Profile:** Three new fields have been added to the Apple Device Enrollment Profile dialog box. These features apply to Apple School Manager and Apple Business Manager:

  - **Skip the Accessibility pane** - Applicable to macOS 11.0 through the most recently released version as supported by MobileIron.
  - **Skip the Restore Completed pane** - Applicable to iOS 14.0 through the most recently released version as supported by MobileIron.
  - **Skip the Software Update Complete pane** - Applicable to iOS 14.0 through the most recently released version as supported by MobileIron.

  For more information, see "Creating Apple Device Enrollment profiles" in the *MobileIron Core Device Management Guide for iOS and macOS Devices*.

- **Disable Wi-Fi MAC address randomization field added**: In iOS 14.0, Apple changed the default behavior for a device reporting its Wi-Fi MAC address to report a random address for new connections

instead of the device's actual Wi-Fi MAC address. In Core, a new option has been added to the Wi-Fi configuration to turn off this randomization. Upon upgrade, this option will be disabled. Administrators can turn off the randomization of the Wi-Fi MAC address by editing the Wi-Fi configuration and selecting the check the box labeled **Disable MAC address randomization**. This will cause the Wi-Fi configuration to be re-pushed to all devices.

Device users will see a "Privacy Warning" message on their Wi-Fi settings indicating that the network has reduced privacy protections. The device user will still have the ability to set the device to report a random address for new connections instead of the device's actual Wi-Fi MAC address.

- For more information, see "Wi-Fi Settings" in *MobileIron Core Device Management Guide for iOS and macOS Devices*.
- Also see KB article: https://help.mobileiron.com/s/article-detail-page?urlname=iOS-14-Devices-may-fail-to-join-WiFi-networks-using-enterprise-security.

- **Authentication using OAuth**: For email apps that support authentication using OAuth, the following additional settings are provided in the Exchange configuration: **OAuth Sign In URL** and **OAuth Token Request URL**. The settings are visible if **Use OAuth for Authentication** in the Exchange configuration is enabled. For more information see the "Exchange settings" table in the "Exchange settings" section in the *MobileIron Core Device Management Guide for iOS and macOS Devices*.

- **AppConfig XML Upload**: For an iOS app in the App Catalog, administrators can add a managed app configuration from one of the following:
  - **AppConfig Community**: Use this option if the app has an AppConfig specification in the community repository. This is the default option.
  - **Upload .xml spec**: Use this option to upload an XML schema to push a particular version of app configuration for the app.

  For more information, see "Adding a new managed app setting for an app" in the *MobileIron Core Apps@Work Guide*.

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 product.

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
	• ADFS 3.0	• PingOne • 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	9.8.1, 9.9.0	9.3.0–9.8.0, 9.8.5 NOTE: The new Email+ Notification Service requires Standalone Sentry. Refer to Email+ VIP Notifications for iOS 13 and above for information on the Standalone Sentry version required for this feature. An upgrade from Standalone Sentry 9.8.0 to the Sentry version of Email+ Notification Service is not supported.
Integrated Sentry	6.4.0	6.2.0–6.3.0

Access

Access	Supported	Compatible
MobileIron Access	R41	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	10.7.0.0, 10.8.0.0	9.3.0.0–10.6.0.0
Tunnel (Android native, Android enterprise, and Samsung Knox Workspace)	4.4.0	4.3.0, 4.3.2
Secure Apps Manager	8.9.0.0	8.3.0.0–8.8.0.0
Email+ (Android AppConnect and Android enterprise)	• 2.18.3.0 • 3.6.0	• 2.2.0.0–2.18.2.0 • 3.0.0–3.5.0

Android	Supported	Compatible
Docs@Work (Android AppConnect and Android enterprise)	2.11.0	2.0.0–2.11.0
Web@Work (Android AppConnect)	2.4.2	2.1.0–2.4.1
Insight	End of Support See https://community.mobileiron.com/docs/DOC-9343	Not applicable

iOS

iOS	Supported	Compatible
iOS	11.0.0–14.0.0	10.0.0
Mobile@Work	12.3.0, 12.4.0* * Mobile@Work 12.4.0 is targeted to release September 15, 2020.	12.0.0–12.2.2
Tunnel	4.1.0	2.4.1–4.0.0
Email+	3.13.0	2.6.0–3.12.0
Docs@Work	2.14.0	2.2.0-2.13.0
Web@Work	2.9.1, 2.10.0	2.0.0–2.9.0

iOS	Supported	Compatible
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 and above. 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	10.15, 11.0	10.12, 10.14
Tunnel	4.0.1	3.0.0

tvOS

tvOS	Supported	Compatible
tvOS	12.4.1, 13.4, 14.0	11.0–11.4

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 version 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	1.2.3	1.2.0, 1.2.2

Supported browsers and browser resolutions

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

TABLE 3. SUPPORTED BROWSERS AND BROWSER RESOLUTIONS

Browser	Supported	Compatible
Internet Explorer	11	9*, 10*
Chrome	84	80, 81, 83
Firefox	79	76, 77, 78

TABLE 3. SUPPORTED BROWSERS AND BROWSER RESOLUTIONS (CONT.)

Browser	Supported	Compatible
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 resolution

TABLE 4. SUPPORTED BROWSER RESOLUTION

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-63003**: MobileIron Access registration would fail when a Secure Hypertext Transfer Protocol (HTTPS) proxy server was enabled on the outbound proxy. This issue has been fixed.
- **VSP-62993**: If there were duplicate Device ID entries for the same mailbox in the Active Sync Association page, status updates in Exchange using Integrated Sentry would fail. This issue has been fixed.
- **VSP-62891**: The Quarantine Device compliance action was missing an information icon with this message: "Once the device is quarantined, AppConnect apps must be reinstalled on the device before they will work." This issue has been fixed.
- **VSP-62874**: There was an issue where Internet Explorer 11 would stop responding when editing and saving an Apple Automated Device Enrollment account. This issue has been fixed.
- **VSP-62615**: Admins were unable to see supervised macOS devices in the Device Details section of the Devices page. This issue has been fixed.
- **VSP-62564**: The Mobile Threat Defense (MTD) anti-phishing VPN was not being pushed to devices when MTD was activated through the managed app configuration. This issue has been fixed.
- **VSP-62536**: As a result of a Core configuration change, event template settings were failing to load. This issue has been fixed.
- **VSP-62436**: When transferring all licenses for a particular app from one Volume Purchase Program (VPP) location to another, the licenses were not deleted from the old location. The issue has been fixed.

- **VSP-62419**: When being edited, Android enterprise managed app configurations could show an incorrect value for a configuration key. This resulted from a difference between the order of the configurations in the UI and the database. This issue has been fixed.

- **VSP-62300**: Previously, when a filter label for a custom attribute was assigned to a device and then removed, MobileIron Core created duplicate audit logs for some API requests. This issue has been fixed.

- **VSP-62248**: Previously, multi-user log in or log out actions would intermittently time out after 30 seconds. The timeout value has been increased to 120 seconds.

- **VSP-62211**: There was an issue where forcing an app update for devices with managed app configurations generated an app installation status of "Not Installed." This issue has been fixed.

- **VSP-62166**: Removing a label that was applied to both a wallpaper policy and a default policy would incorrectly re-push the wallpaper policy. This issue has been fixed.

- **VSP-62154**: Previously, the Audit log incorrectly reported that the administrator with the API role rather than the misystem user removed a filter label for a custom attribute. This issue has been fixed. The misystem user is the built-in MobileIron Core user that creates default rules and policies, and executes system maintenance tasks. This user does not appear the Admin Portal and has no assigned roles.

- **VSP-62014, VSP-62182**: Certificate authentication to the Admin and System Manager portal was blocked when the Certificate Revocation List (CRL) was inaccessible. A new option has been added to control whether to allow or block certificate authentication in this situation. By default, the system will allow the authentication when the CRL is inaccessible. The Core Admin portal will attempt to reconnect with the CRL every 24 hours, and the Core System Manager portal will attempt to reconnect with the CRL every hour. To change the option to block certificate authentication when out of touch with the CRL, contact MobileIron technical support.

- **VSP-62002**: Previously, there was an issue where labels applied to the AppConnect app would intermittently fail to apply the label to the provisioning profile. This issue has been fixed.

- **VSP-61993**: Previously, devices would sometimes be incorrectly quarantined after device registration, because data protection/encryption had not yet been enabled on the device. This issue has been fixed.

- **VSP-61947**: Previously, labels created using custom attributes were not being applied to the devices because labels were not being updated as a part of client check-in. This issue has been fixed.

- **VSP-61934**: Previously, there were some audit logs that did not display when selected in a search on the Audit Logs page. Application Started and Application Stopped searches were not returning correct results. This issue has been fixed.

- **VSP-61893**: Previously, when App catalog records were purged, sometimes not all of the necessary files were being deleted. This issue has been fixed.

- **VSP-61643**: Previously, when context-based logging was enabled, Core would continue context-based logging, even when a different mode was selected. A "Clear" button has been added to Core System Manager > Troubleshooting > Logs > Context based logging page to disable context-based logging.

- **VSP-60900**: Previously, when a device requested that Core renew its mutual authentication certificate, Core would generate the certificate with the following hard-coded subject, irrespective of what was entered in the Simple Certificate Enrollment Protocol (SCEP) setting Subject field: System Default Mutual Auth SCEP "Mutual Auth Enrollment-$RANDOM_32$". The issue has been fixed.

- **VSP-60303**: Previously, the Apps@Work page did not fully display when rendered in full screen on devices running iOS 13.0 through the most recently released version as supported by MobileIron. This issue has been fixed.

- **VSP-59576**: Apple Push Notification Service (APNS) diagnosis check now goes through HTTP outbound proxy, if configured. Note that unlike prior versions, the test does *not* use the mobile device management (MDM) certificate for the test, so it will not detect Secure Sockets Layer (SSL) failures due to an expired MDM certificate. This issue will be fixed in a future version.

- **VSP-52101**: Previously, the Core product version was displayed on the login screen, which is visible to unauthorized users. This issue has been fixed.

- **VSP-46061**: Previously, bulk email notification recipients could see the names of the other recipients in the To field. This issue has been fixed. Core now enters recipient email addresses in the BCC (blind carbon copy) field, so recipient privacy is maintained.

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-63140**: Mobile@Work for macOS might unexpectedly run a script and report execution results more than once. This can happen if Mobile@Work for macOS checks in with the server before the server confirms that it has received the script configuration, resulting in the server sending the script again.

- **VSP-63104**: The sample cascading style sheet (CSS) for the self-service user portal in the **Settings > System Settings > Users & Devices > Registration** page is not working.

Workaround: Admins can copy and paste the MobileIron sample CSS in manually, or use another valid CSS file. For sample CSS text that you can cut-and-paste, see the Self-service user portal chapter of the *MobileIron Core Device Management Guide* for your operating system.

- **VSP-63088**: When an admin enabled with the following specific roles logs into the Spaces page, an erroneous Unauthorized pop-up message appears:
  - View device page
  - Device details

  Workaround: Click **OK** on the pop-up message to continue.

- **VSP-63039**: The software as a service (SaaS) policy is erroneously re-pushed to devices when the label is removed, and the devices change from non-compliant to compliant state.

- **VSP-63038**: The admin portal > User > Local User > Assign Roles configuration page does not open in Internet Explorer 11.

  Workaround: Use a different browser when assigning roles.

- **VSP-63019**: An Admin must be enabled for the role "Delete retired device" to use the "Automatically Retire Devices on a Schedule" feature in the Settings > System Settings > Users & Devices > Retire and Delete Retired Devices page.

- **VSP-62971**: When in the command line shell for NTP configuration, if you enter a hypen (-) to move higher in the Core configuration, the operation fails.

- **VSP-62967**: Help@Work validation fails in Firefox or Chrome browsers.

  Workaround: Use a different browser to initiate validation.

- **VSP-62816**: MobileIron Core is currently unable to modify any existing Graph API configuration or add a Graph API Configuration with more than one key-value pair.

- **VSP-62642**: In the Core managed app configuration settings, a managed app configuration using Boolean logic must be set to True or False. There is no "Not Set" state.

- **VSP-61195**: The "Touchdown" app is no longer available on the Google Play store.

  Workaround: Remove the app from the Exchange configuration.

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

- **VSP-63004**: MobileIron Core cannot retrieve health attestation data from Microsoft Windows devices. This is a Microsoft issue.

- **VSP-62796**: A Lightweight Directory Access Protocol (LDAP) server containing a nested Organizational Unit (OU) depth of more than 10 will be ignored in the LDAP sync. A log entry is generated when this issue occurs. MobileIron recommends that you not use more than 10 nested OUs.

- **VSP-62222**: Copyright text might overlap with instructions when the "Request Desktop Website" option is enabled on Safari on iPhone or iPad devices during Apple web-based device registration. This issue is observed only in portrait mode.

- **VSP-61865**: When installing a specific version of OS update for iOS devices, you must select a version that is available for the device. If an invalid or unavailable update is selected, the device will update to the latest available iOS version for that device.
  Workaround: Disable the "Request Desktop Website" option on the device before starting an Apple web-based device.

MobileIron Core upgrade information

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

- Support community
- MobileIron Core upgrade readiness checklists
- MobileIron Core upgrade paths
- MobileIron Core upgrade URL
- Backing up MobileIron Core
- MobileIron end of sale and support policy

IMPORTANT: See Before you upgrade .

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

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.

TABLE 5. PRE-UPGRADE CHECKLIST (CONT.)

Check	Tasks	References
	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 (i.e., 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 **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:

TABLE 6. UPGRADE CONSIDERATIONS (CONT.)

Check	Considerations	References
		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: 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

TABLE 7. POST-UPGRADE CHECKLIST (CONT.)

Check	Tasks	References
		• 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
```

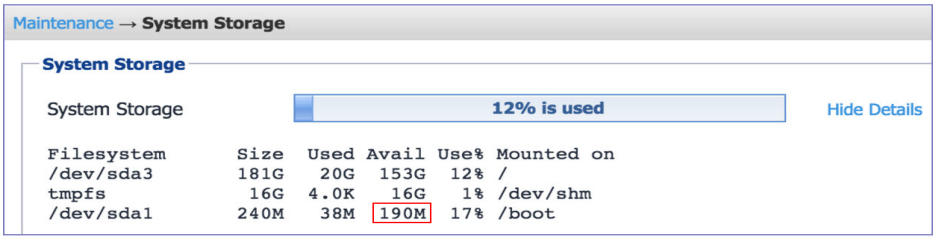
The System Manager

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 10.8.0.0

- 10.6.0.1 → 10.8.0.0
- 10.7.0.0 → 10.8.0.0
- 10.8.0.0 (GMRC) → 10.8.0.0

MobileIron Core upgrade URL

To upgrade MobileIron Core:

Use the following URL if you specify an alternate URL:

https://support.mobileiron.com/mi/vsp/10.8.0.0-34/mobileiron-10.8.0.0-34

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 10.8.0.0 is supported:

Supported upgrade paths to 10.8.0.0

- 10.6.0.1 → 10.8.0.0
- 10.7.0.0 → 10.8.0.0
- 10.8.0.0 (GMRC) → 10.8.0.0

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/10.8.0.0-34/mobileiron-10.8.0.0-34

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.