MobileIron Core and Connector 10.6.0.0 Release and Upgrade Notes

Revised: October 28, 2020

For complete product documentation see:
MobileIron Core Documentation Home Page

Revision history

TABLE 1. REVISION HISTORY

Date	Revision
October 28, 2020	Updated Windows Support and Compatibility information.
April 24, 2020	Updated Support and compatibility > Sentry > Supported version information.
April 16, 2020	Updated Tunnel version supported for Mail, Calendar and Contact payload for per-app VPNs.
March 16, 2020	Removed references to Mobile@Work 12.2.0 for iOS support for the Block/Retire feature and from Support and Compatibility tables. The Block/Retire feature is only supported on Android devices.

Contents

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

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.

> Upgrade to Integrated Sentry 6.4 before upgrading to Core 10.3.0.0. Integrated Sentry 6.4 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
- 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.

- **Support for enabling Notes for Audit Logs:** Administrators can enable or disable the Notes for Audit Logs. For more information, see "Enabling Notes for Audit Logs" in *Getting Started with MobileIron Core*.

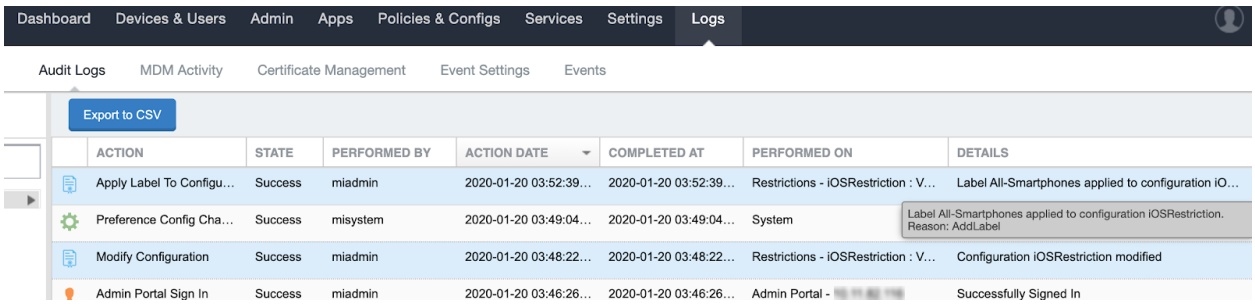
- **Using Notes for Audit Logs to track administrator-made changes to labels:** A best practice is to use Notes for Audit Logs to track administrator-made changes to labels. When enabled, a text box displays for the administrator to provide a reason for the change.

  This affects the following label-related activities:

  - Add/Edit/Delete/Save Label (Both filter and manual)
  - In Devices & Users > Devices > Advanced Search > Save to Label
  - Add/Edit/Remove Label to devices
  - Add/Edit/Remove Label to configurations
  - Add/Edit/Remove Label to policies
  - Add/Edit/Remove Label to apps
  - Add/Edit/Remove Label to iBooks

  Example text to enter would be a change ticket order number. This information then displays in the Audit logs, in the Details column as "Reason."

  FIGURE 1. AUDIT LOG NOTES



  To enable this feature, see "Setup tasks" in *Getting Started with MobileIron Core*. For information on how to use this feature, see "Best practices: label management" in the *MobileIron Core Device Management Guide*.

- **Enabling Notes for Audit Logs to track administrator-made changes to iOS and macOS restrictions:** For best practices, you can enable Notes for Audit Logs to track administrator-made changes to iOS and macOS restrictions. Whenever an administrator adds, edits or deletes iOS and macOS restrictions, a text dialog box appears for the administrator to enter a reason for the change. To enable this feature, see "Setup tasks" in *Getting Started with MobileIron Core.*

- **Notify administrator when PIN expiration prompt was skipped by device user:** Administrators can identify devices that have prompted the device user to change the password / PIN but the device user skipped the prompt. By setting the value in the Maximum Password Age field the number of days a password is valid for and creating a compliance action indicating a grace period before taking action, the administrator can create a search that searches for devices that are less than 7 days (for example) of the device's password expiration date. This advanced search utilizes two new fields that have been added: Screenlock PIN Change Prompt – Showing and Password/PIN Days Before Expiring. If the search is saved to a label, an alert will display indicating any device users that have not updated the password on the device. For more information, see "Setting an alert that a device's PIN change request was skipped" and "Advanced Searching" in the *MobileIron Core Device Management Guide*.

- **New Mobile@Work per-user device limit**: You can now limit the number of devices per user, using LDAP group membership as the conditional limiter. Previously, you could only configure per-user device limits globally.

  From the Settings > System Settings > Users & Devices > Registration page Per-User Device Limit section, you can take the following actions:

  - Select a global device limit of 0-50 devices per user
  - Add LDAP user groups to the LDAP group-specific device limit table
  - Edit LDAP user groups
  - Delete LDAP user groups from the device limit table
  - Set the device limit precedence setting: you can choose whether the standard device limit takes precedence over LDAP membership-specific device limits, or LDAP group-specific device limits take precedence over the standard device limit (for all applicable users)

  For example, you could set a global device limit of four devices, but restrict members of specific LDAP groups to one or two devices. For more information, see "Self-service User Portal" in the *MobileIron Core Device Management Guide*.

- **Core automatically deletes unused Apps during scheduled data purge**: After upgrading to MobileIron Core release 10.6, the server will automatically delete any app directories corresponding to app records that have been deleted from the app catalog.

- **App Catalog branding updates:** The App Catalog > Apps@Work Settings page includes updated customization options to make the App Catalog appearance more familiar to your end users for iPhone, iPad, and Mac devices. For more information, see "Configuring Apps@Work branding" in the *MobileIron Core Apps@Work Guide*.

- **Customize the Mobile@Work Self-Service Portal login page**: You can customize the logo, company name, and message for your Mobile@Work self-service user portal. From the Settings > System Settings > General > Self-Service Portal page, you can upload a logo, change the company name, and create a login page message that is customized for your Enterprise. For more information, see "Customizing the

Mobile@Work self-service user portal" in the *MobileIron Core Device Management Guide*.

- **Enhancement to registration enrollment options:** Increased ability for administrators to provide different registration enrollment options (PIN/password), based on enrollment types (In-App, Zero Touch, Samsung Knox Mobile Enrollment (KME), and QR code.) For more information see "Registering Android devices" in the *MobileIron Core Device Management Guide for Android and Android enterprise Devices*.

Android and Android enterprise features and enhancements

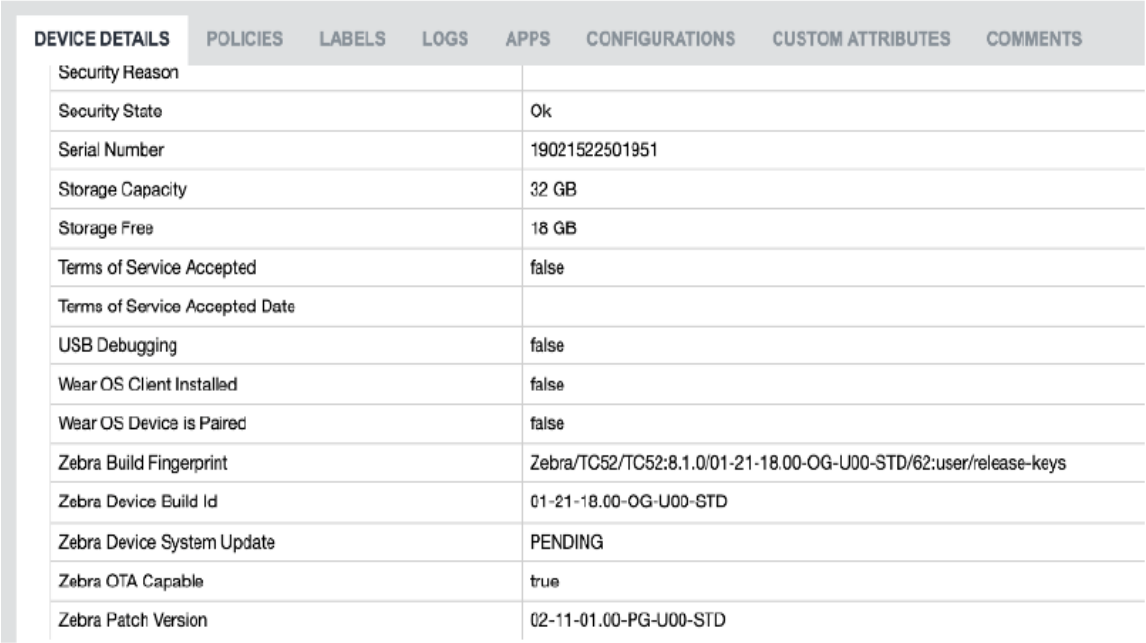
This release includes the following new features and enhancements that are specific to the Android and Android enterprise platforms.

- **Zebra OTA support added:** You can now enroll clients with Zebra OTA (Over the Air) service. This allows the administrator to configure and apply Zebra's OTA firmware policies. You can also apply a schedule for downloading the policy to the client. Administrators can also determine and select whether a full update or partial update is pushed to the Zebra devices. NOTE: Upgrades from Android 7 to Android 8 is not supported. However, upgrades from Android 8 to Android 9 and Android 9 to Android 10 are supported for Zebra. For more information, see "Zebra Support" in the *MobileIron Core Device Management Guide for Android and Android enterprise Devices*.

- **Provide Capability for admin to refresh Zebra OTA Credentials:** IT administrators can now refresh tokens that bind MobileIron Core to Zebra OTA (Over the Air) service and help recover from intermittent read timeouts that could be caused due to network connectivity. For more information, see "Enrolling in the Zebra OTA (Over The Air) service" in the *MobileIron Core Device Management Guide for Android and Android enterprise Devices*.

- **Check the device firmware download status for Zebra and Android devices:** Once you have enabled Zebra OTA service and pushed the related firmware policy, you can run an advanced search to check the status of the Zebra device system update, along with other Zebra-related items. Details that are searchable include: Zebra Build Fingerprint, Zebra Device Build Id, Zebra Device System Update, Zebra OTA Capable and Zebra Patch Version. Values returned are Available, Downloading, Pending, Current and Unknown.

FIGURE 2. CHECKING THE DEVICE FIRMWARE DOWNLOAD STATUS



For more information, see "Checking the Zebra device firmware download status" in the *MobileIron Core Device Management Guide for Android and Android enterprise Devices*.

> Zebra support runs on Mobile@Work for Android 10.6.0.0 through the latest version as supported by MobileIron. This is slated for release in March, 2020.

- **Zero Touch enrollment with custom attributes extends to Boolean and Integer types:** In addition to String, Zero Touch enrollment with custom attributes now supports Boolean and Integer for custom attributes of type. For more information, see "Zero Touch enrollment with custom attributes" in the *MobileIron Core Device Management Guide for Android and Android enterprise Devices*.

- **Enhancement to registration enrollment options:** Increased ability for administrators to provide different registration enrollment options (PIN/password), based on enrollment types (In-App, Zero Touch, Samsung Knox Mobile Enrollment (KME), and QR code.) For more information see "Registering Android devices" in the *MobileIron Core Device Management Guide for Android and Android enterprise Devices*.

- **Block or retire the AppConnect app if password retry count exceeds the maximum number of retry attempts**: Administrators can configure the "Maximum number of failed attempts" action to either "Block" or "Retire" AppConnect apps if the AppConnect passcode retry attempts exceed the configured "Maximum Number of Failed Attempts." The setting is available in the AppConnect Passcode section of the AppConnect Global policy.

- For Android devices, this feature requires MobileIron AppConnect 8.9.0.0 for Android and Mobile@Work 10.6.0.0 for Android.
- For information about configuring the AppConnect Global policy, see the*MobileIron Core AppConnect and AppTunnel Guide*.

iOS and macOS features and enhancements

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

- **Managing Duplicate Devices:** Administrators now can set duplicate active devices to the “Unknown” status and set a daily, weekly and monthly scanning schedule for duplicate devices. For more information, see "Managing Duplicate Devices" in the *MobileIron Core Device Management Guide for iOS and macOS Devices.*

- **Support for WPA3 security type:** Wi-Fi configuration now supports WPA3 Personal and WPA3 Enterprise security methods to access Wi-Fi network on iOS 13 devices. For more information, see "WPA2 / WPA3 Enterprise authentication" and "WPA2 / WPA3 Personal authentication" in the *MobileIron Core Device Management Guide for iOS and macOS Devices*.

- **Support for Mail, Calendar and Contact payload for Per-app VPNs:** Enter one or more domains that will trigger the configured per-app VPN connection in Mail, Contacts, and Calendar apps. Support with Tunnel VPN is available with MobileIron Tunnel 4.0.0 for iOS and macOS. For more information, see "Managing VPN Settings" in the *MobileIron Core Device Management Guide for iOS and macOS Devices*. For information about MobileIron Tunnel VPN, see the *MobileIron Tunnel Guide for iOS for Administrators* or the *MobileIron Tunnel guide for macOS for Administrators*.

- **Ability to mark VPP account as shared across multiple Cores and to sync two types of licenses:** A new option was added to the Apps > Apple Licenses page to mark if the VPP account is shared across multiple Cores. If it is, then the delta sync will be slower as it will get all new and updated licenses. If the Apple Licenses are shared, then the delta sync will only get newly-assigned licenses. In addition, Core will no longer do a full sync automatically. Full syncs will only be available via the new menu option: Sync All Licenses. Additionally, in the Apps > Apple Licenses page, the "Last sync Time" field was renamed "Details Sync Time." A new field, "Count Sync Time," was added to indicate the last time the license count was synced. For more information, see "Managing your Apple license accounts" and "Importing licensed apps from an Apple licensed account" 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.

> 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.

> 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
- Android
- iOS
- macOS
- tvOS
- Windows

SAML / Identity Provider

SAML / Identity Provider	Supported	Compatible
	• OpenSAML 3.3.0 • ADFS 3.0	• PingOne • Shibboleth

LDAP

LDAP	Supported	Compatible

	Windows Active Directory
	• Server OS: Windows Server 2008
	  ◦ Version: 6.1
	• Server OS: Windows Server 2003
	  ◦ Version: 5.2
	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
	1.9.0.0, 1.9.1.0, 2.0.0.0, 2.0.0.1	1.8.0.0, 1.8.0.2

Monitor

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

Sentry

Sentry	Supported	Compatible
Standalone Sentry	9.8.0 **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.	9.3.0–9.7.2
Integrated Sentry	6.4.0	6.2.0–6.3.0
MobileIron Access	R37	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	5.0–7.1
Mobile@Work	10.5.1.0, 10.6.0.0	9.3.0.0–10.3.0.2, 10.3.0.3, 10.4.0.0, 10.4.0.1, 10.5.0.0
Tunnel (Android native, Android enterprise, and Samsung Knox Workspace)	4.3.2.0	4.3.0, 4.3.1
Secure Apps Manager	8.8.0.0	8.3.0.0–8.7.0.0
Email+ (Android AppConnect and Android enterprise)	• 2.18.0.1, 3.3.0 (AppConnect enabled) • 2.18.0.1, 3.3.0 (Android enterprise)	• 2.2.0.0–2.17.0.0 and 3.0.0–3.1.3 (AppConnect

Android	Supported	Compatible
		enabled) • 2.2.0.0–2.17.0.0 and 3.0.0–3.1.3 (Android enterprise)
Docs@Work (Android AppConnect and Android enterprise)	2.9.1	2.0.0–2.9.0.1
Web@Work (Android AppConnect)	2.4.1	2.1.0–2.4.0
Insight	End of Support See https://community.mobileiron.com/docs/DOC-9343	Not applicable

iOS

iOS	Supported	Compatible
iOS	10.0.0–13.0.0	9.0.0
Mobile@Work	12.1.1, 12.2.2	8.0.2–12.1.0
Tunnel	4.0.0	2.4.1–3.1.0
Email+	3.12.0	2.6.0–3.11.0
Docs@Work	2.12.1	2.2.0–2.12.0
Web@Work	2.9.1	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	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	10.14, 10.15	10.10–10.13
Tunnel	4.0.1	3.0.0

tvOS

tvOS	Supported	Compatible
tvOS	12.1, 12.2, 12.2.4	11.0–11.4

Windows

Windows	Supported	Compatible
Windows	Windows 10 Pro, Windows 10 Enterprise (versions 1809, 1903, 1909)	• Windows 10 Mobile (versions 1607, 1703) • Windows 10 Pro, Windows 10 Enterprise (versions 1703, 1709) • Windows HoloLens (versions 1701, 1803) Note The Following: • Not all Windows 10 Mobile devices can be upgraded to version 1703. The currently known list can be found at https://www.windowscentral.com/windows-10-mobile-creators-update-only-coming-11-eligible-handsets. • 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	80	77,78,79
Firefox	73	70, 71, 72
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 MobileIron's 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 MobileIron's 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 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-61173**: Custom attributes with special key names like 'mode', 'cookie' and 'wifi_mac' can being overridden with device-reported values. This has been fixed.
- **VSP-61017**: In certain cases, devices were not able to install Android Enterprise apps on any device, and an error would be shown in logs. This issue has been fixed.
- **VSP-60929**: When using the map to locate a device, the "Back" button, "Update Location" button, the heading, and the device title were not displaying properly. This issue has been fixed.
- **VSP-60886**: Previously, Core was validating the client certificate subject with the old certificate subject. The issue has been fixed.
- **VSP-60861**: The mutual authentication certificate needed for new enrollment was not updating to the new cert. This issue has been fixed.
- **VSP-60850**: When an Android enterprise profile was removed, the app configuration was also removed, but it didn't always clean up correctly in the server database. This caused issues with getting the app configuration on the device if the app was installed again later. This issue has been fixed.
- **VSP-60736**: When the Wear OS policy was in SENT state, the Wear OS tab in Device Details was disappearing until the policy state changed to APPLIED. This has now been fixed.
- **VSP-60687**: MobileIron Core was generating more than one audit log when an App was deleted from the App Catalog. This issue has been fixed.

- **VSP-60652**: For new installations, the default value for the certification revocation list (CRL) is protocol HTTP and port 8080. The need to change the default port is rare. However, if you do modify the CRL port, verify that no other Core service is using that port. For example, port 9997 is the default value for Sync TLS, and using the same port for CRL will result in service disruptions.
- **VSP-60650**: Proxy Diagnosis was failing to connect to http://support.mobileiron.com. The link was changed to secure HTTP: https://support.mobileiron.com, and the issue has been fixed.
- **VSP-60624**: When reinstalling iOS system apps from Core, users were being prompted for an iTunes log in. This issue has been fixed.
- **VSP-60610**: There was an issue which caused SafetyNet Attestation to stick in 'Unknown' state. This issue has been fixed.
- **VSP-60557**: Mobile@Work Windows 10 devices registered with Azure active directory (AAD) could not be wiped if the user was not logged into the device. This issue has been fixed.
- **VSP-60556**: Previously, the MobileIron Core Device Details page sometimes displayed the Mobile Equipment Identifier (MEID) for a device in the International Mobile Equipment Identity (IMEI) field, even when the IMEI value was reported. When the IMEI was not reported, the MEID value displayed in both fields. This issue has been fixed.
- **VSP-60444**: When there was an overlap of TrackID (Production, Alpha, Beta) for an app with different labels to the same device, then Core pushed the app with highest version to the device. This issue has been fixed.
- **VSP-60405**: Previously, when a device was retired or non-compliant, Core was not able to notify Access to invalidate the MSFT tokens when the principal didn't match the UPN/Email prefix. This issue has been fixed.
- **VSP-60376**: Previously, when an in-house App was deleted that had invalid records associated with that app, it was uninstalled and then re-installed on the next device check-in. This issue has been fixed.
- **VSP-60342**: When using a combination of different Audit Log search controls within one search session, Core was rendering incorrect results. This issue has been fixed.
- **VSP-60303**: Previously, the Apps@Work screen did not fully display on iOS 13 devices, and users needed to scroll down to access the icons on the bottom of the page. This issue has been fixed.
- **VSP-60301**: The Data Execution Prevention (DEP) configuration profile page was not rendering umlaut characters properly. This issue has been fixed.
- **VSP-60300**: Previously, the iREG registration URL page text was displaying incorrect device information before registering the device. This issue has been fixed.
- **VSP-60268**: After restarting Core, the UI would time out while saving the LDAP settings, if the LDAP configuration had a large number (more than 9000) of LDAP groups. The issue has been fixed.
- **VSP-60218**: Previously, compliance checks on the basis of Mandatory/Required App Control rules could be triggered during an app update due to intermittent app update states. As a result, when querying app

inventory for mandatory apps, it was required to cover these intermittent app update states as installed/found apps. This issue has been fixed.

- **VSP-60155**: Previously, elastic search heap size increased on large deployments. This issue has been fixed.
- **VSP-60093**: Occasionally, attempts to create or edit the Android Firmware policy would return an internal server error. This issue has been fixed.
- **VSP-60092**: The iOS upgrade policy was not starting at the configured start time. This issue has been fixed.
- **VSP-60075**: In some rare cases, when the Google Play store catalog option was set to Yes, it reverted to No. This issue has been fixed.
- **VSP-60061**: When editing Android enterprise-managed apps, the configuration could not be modified when editing the SERVICE_BO key. This issue has been fixed.
- **VSP-60055**: Previously, the Update License option from App Licenses and the /fullsync API were not performing a full sync, and instead only performed a delta sync. This issue has been fixed.
- **VSP-60021**: Apple Device Enrollment Program (DEP)-registered devices running iOS 13 and above could have their Activation Lock Bypass Code overwritten with "Only generated for supervised devices." This issue has been fixed.
- **VSP-59973**: When an Application Install request was made for a device that has a license for that app, if the license data had not been retrieved or was missing from the database, the end user was prompted to log in to iTunes, and there was an error in the logs stating "Couldn't assign a device license. 9616 : License already assigned" This issue has been fixed. This release fixes this issue by recognizing the error as a valid license and allowing the VPP application installation to continue.
- **VSP-59867**: Previously, the Apps@Work installation process would hang in the "processing" state. This issue has been fixed.
- **VSP-59738**: Previously, when the substitution variable was changed in Samsung Knox container VPN/Exchange for Simple Certificate Enrollment Protocol (SCEP), the changes didn't trigger Core to generate a new certificate during LDAP sync. This issue has been fixed.
- **VSP-59571**: Web apps created and distributed through the App Catalog were not being deleted from the iOS device during label removal. This issue has been fixed.
- **VSP-59448**: Devices were displayed as "roaming," even when Collect Roaming Status was disabled in the Privacy policy. This issue has been fixed.
- **VSP-59000**: Previously, rebooting a physical appliance would sometimes result in network interface card (NIC) swapping, which can cause problems with interface configuration. This issue has been fixed.
- **VSP-58745**: Core was not validating the Android enterprise configuration to match the Core branding. This issue has been fixed.

- **VSP-50922**: Out of contact messages sent to user's device were not including identifying information, such as external hostname and/or IP address. This issue has been fixed.

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-61306**: When iOS devices are marked as LOST (Devices -> Select device -> More actions -> LOST), Core is not retaining the status. The device status changes to Active at the next check-in.
- **VSP-61276**: The last hour of the day cannot be selected when applying Download Schedule for Zebra Devices.
- **VSP-61275**: The App Catalog page for Outlook app may fail to load if the the app is disabled for Android Enterprise.
- **VSP-61029**: When renewing local CA authentication, Apps@Work does not automatically update the HTTP Daemon.
  Workaround: Reboot MobileIron Core from the System Manager portal.
- **VSP-61015**: When creating passwords for the MobileIron Software Repository, passwords ending with percent (%) will not be accepted. Avoid making "%" the last character in your password.
- **VSP-60928**: When configuring certificate enrollment settings for Simple Certificate Enrollment Protocol (SCEP), if the selected field value is changed in the Active Directory, Core does not generate a new certificate with updated details.
- **VSP-60793**: If you delete a Label when the setting "Notes for Audit Logs" is enabled (Settings > System Settings > General), the words "LARGE DEVICE IMPACT :" display at the beginning of the log message.
- **VSP-60652**: For new installations, the default value for the certification revocation list (CRL) is protocol HTTP and port 8080. The need to change the default port is rare. However, if you do modify the CRL port, verify that no other Core service is using that port. For example, port 9997 is the default value for Sync TLS, and using the same port for CRL will result in service disruptions.
- **VSP-60174**: For new installations, the default value for the Certificate Revocation List (CRL) is protocol HTTP and port 8080. The need to change the default port is rare. However, if you do modify the CRL port, verify that no other Core service is using that port. For example, port 9997 is the default value for Sync

TLS, and using the same port for CRL will result in service disruptions. Note that Core supports your last two configured ports (current and most recent past).

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-60763**: Wifi Configuration for Wi-Fi Protected Access 3 (WPA3) is not supported for Android and macOS.
- **VSP-60338**: Update the Azure Active Directory (AAD) URL redirect pattern in MobileIron Core to allow AAD enrollments to work. This update is needed due to a change in the Microsoft URL pattern during AAD enrollment.
- **VSP-60171**: If the Email+ B2B app **com.mobileiron.ios.emailplusshare** was added prior to MobileIron Core release 10.5.0.0, an admin will need to add the following keys and values as part of the Custom Data of the corresponding AppConnect configuration file:

```
Key
email_address
Value
$EMAIL$

Key
email_exchange_username
Value
$USERID$

Key
email_device_id
Value
$DEVICE_UUID_NO_DASHES$
```

- **VSP-60045**: Existing iPads are identified as "iPad Pro-12.9 inch" instead of "iPad 7th Gen."
  Workaround: Retire the device and re-register using IREG to enable the device to identify correctly as iPad 7th Gen.
- **VSP-59601**: When an Appstore app is uninstalled from a device Home screen, MobileIron Core does not report the app as uninstalled, because iOS is currently designed not to report uninstalled web apps.
- **VSP-57908**: User channel profiles are not pushed if the Admin account is set, and "Skip primary account setup" is enabled in the DEP profile.
  Background: Apple Automated Device Enrollment (formally known as DEP) allows the admin to select the following actions when a macOS DEP device is first powered on:
  - Which accounts should be created automatically
  - Whether or not the end user can create a primary account

Limitation: If an admin account is setup on the device, but the end user is not given the ability to create a primary account, Core can only send profiles and configurations that are device-specific. Because there is no primary account, user-specific profiles and configurations cannot be pushed to the 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 .

> 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.
	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

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: https://<serverFQDN>:8443/upgrade/status
	Additional reboot	Due to a kernel upgrade, an additional reboot is performed when you

TABLE 6. UPGRADE CONSIDERATIONS (CONT.)

Check	Considerations	References
		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 knowledge base article at 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.

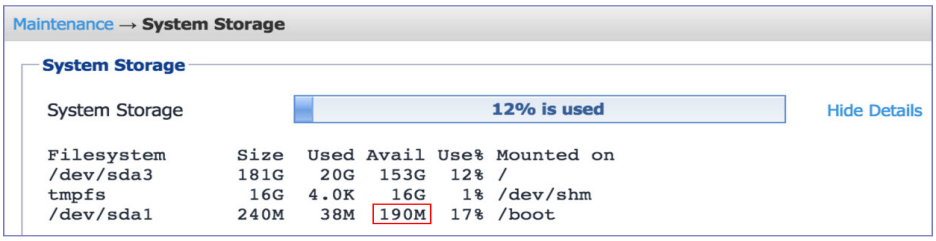
```
CORE(8.5.0.1a-6)@host.company.com#show system disk
Filesystem Size Used Avail Use% Mounted on
/dev/sda3 181G 20G 153G 12% /
tmpfs 16G 4.0K 16G 1% /dev/shm
/dev/sda1 95M 76M 15M 84% /boot
```

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.

> For MobileIron Core release 10.6.0.0, **the GA build is the same as the GMRC build**. Customers who have upgraded to the GMRC build do not require any additional upgrades, and have the latest GA build.

Supported upgrade paths to Core 10.6.0.0

10.4.0.0 → 10.6.0.0

10.4.0.1 → 10.6.0.0

10.4.0.2 → 10.6.0.0

10.4.0.3 → 10.6.0.0

10.5.0.0 → 10.6.0.0

10.5.1.0 → 10.6.0.0

10.5.2.0 → 10.6.0.0

10.6.0.0 GMRC → 10.6.0.0 GA

MobileIron Core upgrade URL

To upgrade MobileIron Core:

Use the following URL if you specify an alternate URL:

https://support.mobileiron.com/mi/vsp/10.6.0.0-23/mobileiron-10.6.0.0-23

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 10.6.0.0 is supported:

> For MobileIron Core release 10.6.0.0, **the GA build is the same as the GMRC build**. Customers who have upgraded to the GMRC build do not require any additional upgrades, and have the latest GA build.

10.4.0.0 --> 10.6.0.0

10.4.0.1 --> 10.6.0.0

10.4.0.2 --> 10.6.0.0

10.4.0.3 --> 10.6.0.0

10.5.0.0 --> 10.6.0.0

10.5.1.0 --> 10.6.0.0

10.5.2.0 --> 10.6.0.0

10.6.0.0 GMRC → 10.6.0.0 GA

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/10.6.0.0-23/mobileiron-10.6.0.0-23

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.