MobileIron Core and Connector 10.7.0.0 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.

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

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 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*.

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
	• 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 • 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	9.7.3, 9.8.1, 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.	9.3.0–9.7.2
Integrated Sentry	6.4.0	6.2.0–6.3.0

Access

Access	Supported	Compatible
MobileIron Access	R39	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, 10.7.0.0	9.3.0.0–10.5.0.0
Tunnel (Android native, Android enterprise, and Samsung Knox	4.3.2	4.3.0, 4.3.1

Android	Supported	Compatible
Workspace)		
Secure Apps Manager	8.9.0.0	8.3.0.0–8.8.0.0
Email+ (Android AppConnect and Android enterprise)	• 2.18.2.0 • 3.5.0	• 2.2.0.0–2.18.1.0 • 3.0.0–3.4.0
Docs@Work (Android AppConnect and Android enterprise)	2.10.0	2.0.0–2.9.0
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	10.0.0–13.5.0	9.0.0
Mobile@Work	12.2.2, 12.3.0	8.0.2–12.2.1
Tunnel	4.1.0	2.4.1–4.0.0
Email+	3.13.0	2.6.0–3.12.0
Docs@Work	2.13.0	2.2.0-2.12.1
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	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	10.14, 10.15	10.12, 10.13
Tunnel	4.1.0	3.0.0–4.0.1

tvOS

tvOS	Supported	Compatible
tvOS	12.1, 12.2, 12.2.4, 13.0	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

Windows	Supported	Compatible
		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	83	79, 80, 81
Firefox	77	74, 75, 76
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.

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.

- **Enable Authenticator Only Role**: The Enable Authenticator Only Role user role is added to designate an unmanaged mobile device as the user's identity and authentication factor. Designating a mobile device as the user's identity allows users to take advantage of zero sign-on features, which allow passwordless access to software as a service (SaaS) applications and other business services. In addition to the Enable Authenticator Only Role user role, the following are visible in MobileIron Core to support Authenticator Only mode:
  - **Authenticator Only** field: A new field is added in the MobileIron Core Admin Portal in Devices & Users > Devices.

    NOTE: The value for Authenticator Only displays as Yes if the device is registered as an Authenticator Only device.
  - **Authenticator Only** device: The label displays for Authenticator Only devices on the user portal and in Device Details on the Admin Portal.

  The feature requires MobileIron Access 40 and a supported Mobile@Work client. The supported client versions are Mobile@Work 12.3.0 for iOS or Mobile@Work 10.7.0.0 for Android.
  For information about how to deploy and register a device in Authenticator Only mode, see "Authenticator Only with MobileIron Access" in the *MobileIron Access Guide*.

- **MobileIron Connector support for LDAP over Strict SSL**: The MobileIron Connector now supports Lightweight Directory Access Protocol (LDAP) over Strict Secure Sockets Layer (SSL) security. Beginning in March 2020, Microsoft began enforcing LDAP Channel Binding and LDAP Signing on existing Active Directory (AD) servers. This update supports those changes. The configuration is available through the Admin portal LDAP preferences page when MobileIron Connector service is enabled. The configuration option does not display if the Connector service is disabled. For more information on LDAP configuration, see the *On-Premise Installation Guide for MobileIron Core and Enterprise Connector*.

- **Replacement SSD is equivalent to previous M2600 component**: From version 10.7.0.0 through the most recently released version as supported by MobileIron, the solid-state drive (SSD) for new M2600 appliances includes a Seagate XS1600 SSD component with a capacity of 960GB (equivalent to the previous component). For more information about MobileIron appliances, see "MobileIron M2600 Series appliance" in the *On-Premise Installation Guide*.

- **Simple Certificate Enrollment Protocol test user**: MobileIron Core 10.7.0.0 now supports the creation of a configurable test user specifically for requesting test certificates. This feature is compatible in a Simple Certificate Enrollment Protocol (SCEP) environment, because it negates the need for a preset dummy user, which can be a security risk.

- **Correlate configuration changes with change tickets in audit logs**: Core audit logs can now be configured to correlate configuration changes with an approved change ticket, which may be required by auditors in some environments.

- **Log support for LDAP changes**: You can now enable audit log support for LDAP attributes and group names changes, making LDAP and Label troubleshooting easier.

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.

- **Allow work calendar sharing with personal profile:** Administrators can now allow calendar sharing of work calendar information with the personal profile. This is so apps can display work events alongside personal events in device user's personal profile. Applicable to Managed devices with work profiles. For more information, see "Lockdown Policies" in *Getting Started with MobileIron Core.*

- **Custom Access Point Name (APN) with Android devices:** In addition to being able to configure custom APNs on Samsung devices, you can now configure a custom APN on Android devices. This applies to Work managed device mode (DO) and Managed device with work profile mode (COMP) on Android devices version 9.0 through the most recently released version as supported by MobileIron. For more information, see "Using custom APN with Android devices" in the *MobileIron Core Device Management Guide for Android and Android enterprise Devices*.

- **Password policy attributes shows legacy devices as "Unsupported"**: Android 10 devices provisioned in legacy Device Admin mode (releases prior to Core 10.6.0.0), will display as "Unsupported" in the Devices & Users > Devices > Device tab. "Unsupported" will display for the following password policy attributes:
  - Password
  - Password Type
  - Minimum Password Length
  - Maximum Password Age

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

- **Administrators can now grant additional delegation permissions**: For Android 8.0 and above devices, Mobile@Work allows delegation permissions for apps in Managed device with Work profile (COPE) mode.
  - For Public or Self Hosted Apps (Google Play Private channel apps) pushed by Managed Google Play or regular Google Play:

        - Apps are assigned to device in Managed device with Work profile (COPE) mode and will be pushed and installed silently by Google Play services inside the managed work profile.
        - After the app is installed in the Managed device with Work profile, delegated permissions is applied by Mobile@Work.
        - This is supported for Samsung and non-Samsung devices running Android 8.0 through the latest version as supported by MobileIron.
    - For In house Apps (Apps pushed by Core):
        - Apps are assigned to devices in Managed device with Work profile (COPE) mode and will be installed silently by Mobile@Work on the personal (device owner) side.
        - After the app is installed, delegated permissions are applied by Mobile@Work.
        - This is supported for Samsung and non-Samsung devices running Android 8.0 through the latest version as supported by MobileIron.
    - For In house Apps on Samsung Knox V3 devices (Android 8.0 and above):
        - Apps are assigned to device in Managed device with Work profile (COPE) mode and whitelisted for Knox V3 workspace.
        - Apps are silently installed by Mobile@Work on the personal (device owner) side and then immediately hidden and moved to the Knox V3 workspace (managed profile.)
        - At the time the app is moved into the Knox V3 workspace, delegated permissions are applied.

    NOTE: Installing regular In house apps inside the Managed device with Work profile is not supported.

    MobileIron Core version 10.4.0.0 through the latest version and Moble@Work for Android version 10.7.0.0 are required for this feature. For more information, see "Delegated permissions for Google Play apps" or "Delegated permissions for in-house apps" in the *MobileIron Apps@Work Guide*.

iOS and macOS features and enhancements

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

NOTE: To avoid unexpected behavior, MobileIron recommends that Admins retire any existing devices for a user when moving the user from User Enrollments to Device Enrollments.

- **User Enrollment for Apple Business Manager added:** An enrollment option designed for companies implementing BYOD (Bring Your Own Device). User Enrollment is a modified version of the MDM protocol with a much greater focus on user privacy, implemented with a level of security that enterprises need.

User Enrollment allows the administrator to:

- Install and remove managed applications
- Install and remove network configurations
- Install a partial VPN scoped to managed apps and accounts

User Enrollment utilizes the user's managed Apple ID, which is required and associated with all enterprise apps and data on the device and in iCloud Drive. Managed Apple IDs were first utilized by Apple School Manager and are now utilized by Apple Business Manager for User Enrollment.

User Enrollment is not to be confused with device enrollment. User Enrollment applies to devices iOS 13.0 through the latest version as supported by MobileIron. Devices lower than iOS 13.0 will be considered "device enrollment" regardless if the device user has been enabled for User Enrollment.

NOTE: Only VPP tokens that are from an Apple Business Manager or Apple School Manager account will work. Old deprecated tokens that are in the original VPP portal will not work for User Enrolled Devices for Apple Business Manager.

For more information, see "User Enrollment with Apple Business Manager" in the *MobileIron Core Device Management Guide for iOS and macOS Devices.*

- **User Enrollment support for managed Apple IDs with LDAP users and groups**: In Devices & Users > Users > Edit User, a new option was added to the Assign Roles dialog box called "Use Apple User Enrollment (For Apple unsupervised device only)." After selecting this check box, enter the "Managed Apple ID" for the user in the text field provided. Substitution variables can be used.

  You can also configure LDAP group member to inherit Apple User Enrollment roles. Device users who are synced to LDAP can be assigned to a device management role and associated with a Managed Apple ID. For more information, see "Create users to enable User Enrollment for local users and LDAP users" and "Configure LDAP group members to inherit Apple User Enrollment Roles" in the *MobileIron Core Device Management Guide for iOS and macOS*.

- **Restrictions tab added to Device Details page**: For all iOS and tvOS devices that Core supports, a new "Restrictions" tab has been added to the Device Details page. This displays the restrictions applied to the selected device. If there are no restrictions, the Restrictions tab displays "No Data." The key benefit to this feature is that the administrator is no longer required to manually look at the specific device to confirm if restrictions have been applied. For more information, see "iOS and tvOS restrictions settings" in the *MobileIron Core Device Management Guide for iOS and macOS Devices*.

- **Auto update support for iOS B2B apps now available internationally**: Automatic updating (Auto Update) of iOS Custom Apps (B2B Apps) for countries other than US is now supported. For more information see "Using the wizard to import iOS apps from the Apple App Store" in the *MobileIron Core Apps@Work Guide*.

- **Enable split tunneling using MobileIron Tunnel**: iOS only. If you are transitioning from UIWebView to WKWebView and your app currently uses AppTunnel rules, a new option, Enable Split Tunneling using

MobileIron Tunnel, is available on the MobileIron Core Admin Portal. The new option is available in the AppConnect App Configuration, Docs@Work configuration, and Web@Work configuration. The feature requires Mobile@Work 12.3.0 and MobileIron Tunnel 4.1.0 for iOS.

Before enabling the option, ensure that MobileIron Tunnel is deployed. Enabling the option allows the configured AppTunnel rules to be managed through MobileIron Tunnel rather than through AppTunnel. The workaround is available due to the planned deprecation of the UIWebView API by Apple.

For information about the UIWebView API deprecation, see UIWebView Deprecation and AppConnect Compatibility. For information about configuring AppConnect App Configuration, see "AppConnect app configuration" in the *MobileIron Core AppConnect and AppTunnel Guide*.

Windows features and enhancements

This release does not include new Windows-specific features or enhancements.

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.

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-62114:** The Apple B2B applications were not updating via MobileIron Core because the auto-update for VPP was not working. This issue has been fixed.
- **VSP-62038:** MobileIron Core was removing the Mobile@Work for Android configuration from a quarantined device. This issue has been fixed.
- **VSP-61994:** Updates to Google Store Layout for Android enterprise devices were failing after Feb 2020. This issue has been fixed.
- **VSP-61906:** When a new Android in-house or market app was imported into the App Catalog, a new app record was created. However, the in-house Android app and Android enterprise app had the same APP_ID so it caused the APP_INVENTORY records to be inaccurate. This issue has been fixed.
- **VSP-61798:** For newly-registered devices, Core was adding the already-existing cert extensions into the local CA cache. This issue has been fixed. For devices with duplicate cert extensions, you must re-push the certificate to the device after upgrade.
- **VSP-61768:** The Registration page for iPad in portrait mode was not aligning properly. This issue has been fixed.
- **VSP-61718:** VPN Configurations with Tunnel would sometimes show on device as "UNKNOWN_PAYLOAD," but would not have any loss of functionality. This issue has been fixed. Upgrade will not re-push the configuration. To fix the UNKNOWN_PAYLOAD status, re-push the VPN configuration.
- **VSP-61548:** When an Android enterprise app contained an empty BUNDLE_ARRAY, the administrator was unable to edit the app. This issue has been fixed.

- **VSP-61429**: The Entrust Certificate Enrollment Configuration did not support the creation of Subject Alternative Name NT_PRINCIPAL_NAME (also referred to as User Principal Name). This issue has been fixed with the addition of "NT Principal Name" field to Subject Alternative Name section. To find this, go to Policies & Configurations > Configurations > Add New Certificate Enrollment > Entrust. In the Subject Alternative Names section, select the "NT Principal Name" type and in the Values drop-down, select either $EMAIL$ or $USER_UPN$.

- **VSP-61369:** MDM profiles were not pushed through PIN-based registration for iReg for iOS 13 devices. This issue has been fixed.

- **VSP-61339:** Previously, Android enterprise managed app configurations had a limit of 100 configurations per app. This limit has been increased to 500.

- **VSP-61291:** iOS 13 iPhone iReg registrations using Safari desktop mode were treated as a macOS device. This issue has been fixed.

- **VSP-61288:** The Device details page > Compliance tab was only displaying "Required" violations rather than all violated app control rules. This issue has been fixed.

- **VSP-61256:** New updates of public iOS apps would not reset the counter in the Apps@Work container badge count. This issue has been fixed.

- **VSP-61250:** An issue that caused the iOS MDM profile installation to fail has been fixed.

- **VSP-61221:** Android and iOS devices were being retired from Core due to missing mutual authentication certificate renewal properties in the Sync policy. This issue has been fixed.

- **VSP-61177:** Starting in Core 10.7.0.0, custom attribute values for Zero Touch enrollment key value pairs will no longer override for devices that do not have Zero Touch.

  NOTE: Zero Touch enrollment with custom attributes require Core 10.6.0.0 through the latest version as supported by MobileIron.

- **VSP-61135:** When the same provisioning profile was associated with multiple apps, updating the app with the same provisioning triggered an install provisioning profile request for existing devices. This issue has been fixed.

- **VSP-61068:** In Policies & Configurations > Configurations > Wi-Fi Setting, the "Proxy PAC URL" field was mandatory for an automatic proxy type. This is now an optional field.

- **VSP-61015:** Handling special characters in the password field of Software Repository configuration, passwords with a trailing "%" did not work. This issue has been fixed.

- **VSP-60958**: There was an issue with Event Center templates which causes the page to freeze when a `<head>` tag was added. The response for the **eventTemplateDetails POST** command was not sent in a JSON format, which kept the page from loading correctly. This issue has been fixed.

- **VSP-60865**: There was an issue whereby Admin portal log-in failures were not being logged. This issue has been fixed.

- **VSP-60862**: Previously, an Automated Device Enrollment device had an initial default value of iOS 9, until the device checked in and the correct model and OS version was returned. The new initial default value for Automated Device Enrollment devices is iOS 11.

- **VSP-60839**: The drag and drop action to add images to the Wallpaper Policy was not working. This issue has been fixed.

- **VSP-60826**: There was an issue during VPN configuration, where "Sentry Services" were not rendering. This issue has been fixed.

- **VSP-59252**: Android enterprise devices in Kiosk mode did not automatically update any app in the foreground, even when there was a force auto update policy for that app. 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-62373**: For Apple-licensed apps that will be used by both User Enrolled devices and Device Enrolled devices, the license type should be set to Device-based licenses. Devices enrolled with DEP or Device Enrollment where the Apple-licensed app is set to user-based licenses will show the app as "Free" instead of "Prepaid" and the app will fail to install. User enrolled devices will always have the Apple-licensed app assigned as a user-based license regardless of this setting.

- **VSP-62367**: When an MTD anti-phishing configuration with Content Blocker enabled is created and pushed to an iOS device running Mobile@Work prior to release 12.3.0, the user receives a prompt to enable the Content Blocker. If Content Blocker is enabled on the device but is later disabled, the user does not receive another prompt to enable it.

  Workaround: Upgrade to Mobile@Work release 12.3.0.

- **VSP-62314**: When Content Blocker is disabled for a device, the updated status for that device on the Core > Devices > Devices & Users page should be "N/A" and not "Active." The device displays "N/A" when the

anti-phishing policy is removed from the device.

- **VSP-62263**: There is an issue when pushing the Security Policy for macOS version 10.13 or later to devices with "Enabling Enforce Password Rule at Next Login" enabled. Any modification of the security policy will require users to change their password when it is pushed to their device.

- **VSP-62256**: In a few cases, MobileIron Access-enabled Tunnel profiles are not displayed or synced on Access. Please contact the MobileIron support team to determine if any of the Android Enterprise configuration IDs match the missing Tunnel profile ID. If yes, delete and recreate the Tunnel configuration on Core.

- **VSP-62233**: When an Apple Device Enrollment client is installed as a Sideloaded App, and the client is Authenticator Only enabled, two device entries are created—one as an Apple Device Enrollment device, and another as an Authenticator Only client device.

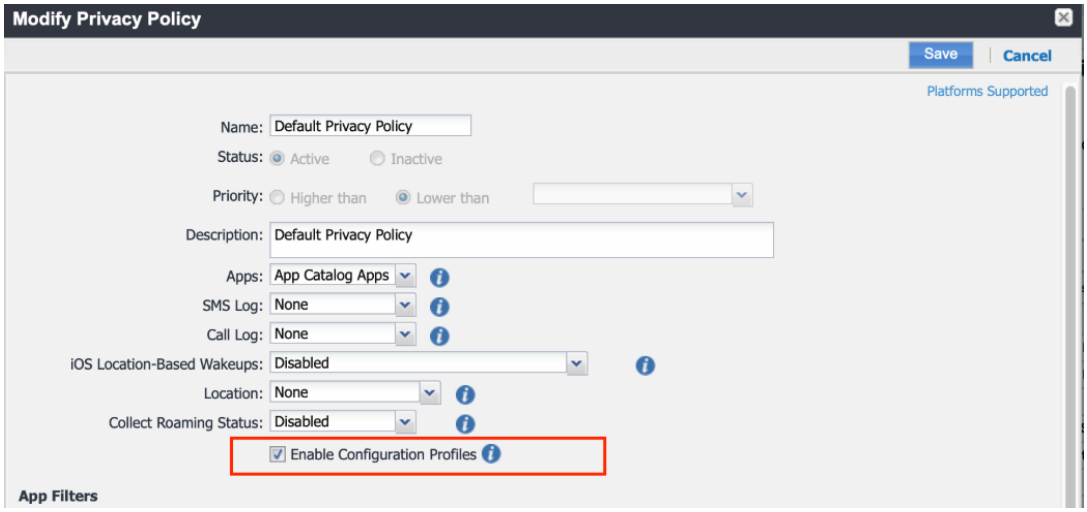
- **VSP-62216**: If transport layer security (TLS) is enabled for the MobileIron Connector, the root certification must be uploaded to Core. Without this certification, Core will display an error message.

- **VSP-62209**: Core does not display or allow the re-upload of certificates in .pfx and .p12 formats that are uploaded using LDAP certificate-based authentication.

- **VSP-62183**: The System Manager's certificate-based authentication does not make a Certificate Revocation List (CRL) check after a CRL download request fails.
  Workaround: Restart the Tomcat2 (System Manager) service, so it will attempt to download the CRL again.

- **VSP-62182**: The MobileIron System Manager allows certificate-based authentication when a Certificate Revocation List (CRL) is not accessible. There is currently no option to configure allowing or blocking certificates when a CRL is not accessible.

- **VSP-62007**: For threat detection and mitigation to work for devices in mobile application management (MAM)-only mode, you must click **Enable Configuration Profiles** in the Policies & Configs > Policies > Privacy Policy menu.



- **VSP-62004**: Android device registrations fail on Core servers with both FIPS mode and SafetyNet enabled. The only workaround is to disable SafetyNet attestation.

- **VSP-61962**: MobileIron Access Session Revocation Service (SRS) will fail to revoke Office 365 session tokens if the LDAP user principal configured in MobileIron Core contains uppercase letters.

  Workaround: Change the LDAP user principal to lowercase letters.

- **VSP-61699**: The MTD sinkhole VPN and the MTD anti-phishing VPN are not removed from the device when the MTD License is inactivated.

- **VSP-61552**: When Samsung Knox devices are enabled on the same Core server as AppConnect, the devices are erroneously deployed as Authenticator Only devices.

- **VSP-61539**: If a supervised device is enabled for Authenticator Only mode, the device registers as Authenticator Only. It will register as supervised once Core updates.

- **VSP-60688**: There is an issue with Apps@Work and AppConnect, where if the Certificate Expiry duration is shorter than the Renew duration, they become inaccessible.

  Workaround: Ensure that the Certificate Expiry duration is greater than the Renew duration.

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-62334**: When an end user logs on to the user portal with certificate authentication and requests a registration PIN, the UI may not show the PIN. The end user will have to ask the admin for the PIN.

- **VSP-62043**: There is a vendor issue that is blocking Core from accessing restrictions set on macOS devices. A ticket has been filed with the vendor.

- **VSP-62005**: MobileIron Tunnel Per-App VPN does not work on User Enrollment devices due to an Apple limitation, because the Tunnel app cannot find the identity certificate in the keystore. VPNs that use password-based authentication function correctly.

- **VSP-61865**: When choosing a specific version of OS update for iOS devices, the specified version must be a version that is available for the device. If an invalid or unavailable update is specified, the device will update to the latest available iOS version for that device.

- **VSP-61659**: The delete duplicate devices service will not detect duplicate User Enrollment devices, because there is no uniquely identifiable information for User Enrollment devices to use to distinguish duplicates. It is up to administrators to delete any devices they feel are duplicate.

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.
	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	• Minimum 80 GB hard drive

TABLE 5. PRE-UPGRADE CHECKLIST (CONT.)

Check	Tasks	References
	requirements	• 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: 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

TABLE 6. UPGRADE CONSIDERATIONS (CONT.)

Check	Considerations	References
		• 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 • 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

TABLE 7. POST-UPGRADE CHECKLIST (CONT.)

Check	Tasks	References
		• 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
```

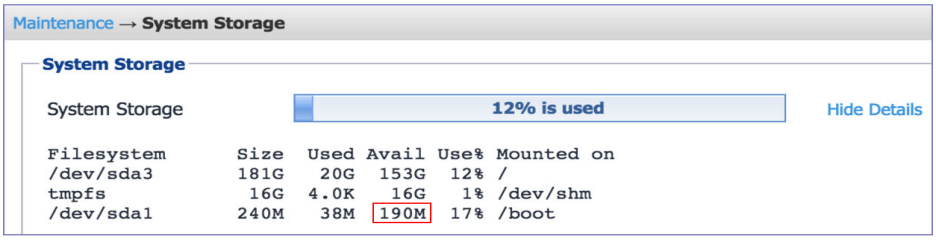
The System Manager

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 10.7.0.0

10.5.1.1 → 10.7.0.0

10.5.2.1 → 10.7.0.0

10.6.0.0 → 10.7.0.0

10.6.0.1 → 10.7.0.0

10.7.0.0 (GMRC) → 10.7.0.0

MobileIron Core upgrade URL

To upgrade MobileIron Core:

Use the following URL if you specify an alternate URL:

https://support.mobileiron.com/mi/vsp/10.7.0.0-28/mobileiron-10.7.0.0-28

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

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 10.7.0.0 is supported:

Supported upgrade paths to 10.7.0.0

10.5.1.1 → 10.7.0.0

10.5.2.1 → 10.7.0.0

10.6.0.0 → 10.7.0.0

10.6.0.1 → 10.7.0.0

10.7.0.0 GMRC → 10.7.0.0

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/10.7.0.0-28/mobileiron-10.7.0.0-28

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.