# Core and Connector 11.4.0.0 – 11.7.0.0 Release and Upgrade Notes

**July 2022**

For complete product documentation, see:
Ivanti Documentation Home Page

# Revision history

For the complete revision history, see the online version of this document.

# Contents

# About Core

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 Core 10.3.0.0 or supported newer versions, 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 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
- Connector
- SCEP servers
- LDAP servers
- Core Gateway
- Apple Push Notification Service (APNS)
- Content Delivery Network servers
- Core support server (support.ivanti.com)
- Outbound proxy for Gateway transactions and system updates
- SMTPS servers
- Public app stores (Apple, Google, Windows)

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

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

To determine TLS protocol usage with external servers:

- **For outgoing connections from Core to external servers**, use the Ivanti utility explained in the following article to determine the TLS protocol usage with those servers: https://forums.ivanti.com/s/article/Core-10-2-upgrade-disables-TLS-1-0-and-TLS-1-1-by-default-9256
- **For incoming connections to Core from external servers**, determine each server's TLS protocol usage (no Core 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 *Core System Manager Guide*.

# New features summary

These are cumulative release notes. If a release does not appear in this section, then there were no associated new features and enhancements.

## General features

- **Changes to instructions in Mobile@Work**: In Mobile@Work, the instructions in the enrollment and remediation pages have been updated.
- **Run Reporting Database reports on user and device attributes**: The Reporting Database now includes user and device attributes in its reports. See the latest *Reporting Database Essentials* guide for more information.
- **Ability to delete multiple local users:** Administrators can now delete multiple users. You cannot delete multiple users if:
    - a user you are trying to delete is currently logged in (administrator)
    - a user is an administrator user - you first need to remove the administrator role of the user
    - there is a non-retired device associated to the user

      For more information, see Deleting multiple local users in the admin portal in the *Getting Started with Core* guide.
- **Registration passcode expiry maximum time increased**: You can now customize the number of hours the registration password is valid, from 4 hours (default) to a maximum of 4320 hours (6 months). For more information, see Setting passcode and registration code defaults in the *Getting Started with Core* guide.
- **Symantec name change updated in user interface**: Symantec Web Services Managed PKI has changed its name to DigiCert PKI Platform, therefore, you may note associated textual changes in the Core user interface.

- **Support for optional KVP on Email+:** The KVP email_user_certificate_self_service can optionally be set to the ‘retired’ certificate value for a device user by prefixing it with [optional].(email_user_certificate_self_service is a mandatorily configurable KVP for all the Core users.) [optional]email_user_certificate_self_service is an alternative configurable KVP for applicable device users that Core will push to the user’s device only when the value is non-empty. Developers of AppConnect apps now have the option to create [optional] keys so that if the value is null/empty, it will not send that key/value to the AppCconnect app.
  For more information, see the *Email+ for Android Guide*.

- **New Force Retire Option:** Usually, when you issue a Retire command for a device, it is moved to a Retired state and is considered "Retire Pending." Sometimes the devices remain in the Retire Pending state. Core offers a Force Retire check box to make sure the device is Retired. You can also schedule the retirement of Retire Pending devices. In Core, go to Settings > Users and Devices > Retire and Delete. In the retire devices section, there are settings that allow you to retire the retire pending devices, based on the last check-in time, with on-demand actions and scheduled actions. For more information, see "Retiring a device" and "Retiring the Retire Pending devices" in the Core Device Management Guide of your OS.

- **Client ID added to Device Details:** For troubleshooting purposes, Client ID has been added to the Device Details page. Administrators can also search for Client ID as well. For more information, see "Advanced Searching" in the Core Device Management Guide of your OS.

- **Ability to remove profiles from individual devices:** Similar to the Push Profiles option is a new feature that allows administrators to manually Remove Profiles from specific devices. This feature is helpful for troubleshooting specific devices, for example, overriding the default label for that device. For more information, see "Pushing and removing device profiles" in the Core Device Management Guide of your OS.

- **Hyper-V 2019 server is supported for core and enterprise connector installations**: With this release, Core can be installed on a Microsoft Hyper-V 2019 server. The Hyper-V 2019 includes Windows Hypervisor, a Windows server driver model, and virtualization components. Hyper-V is delivered as part of Microsoft Windows Server 2019. For more Hyper-V information, see Virtual Core requirements in the *On-Premise Installation Guide for Core and Enterprise Connector* guide.

- **Advanced search enhancements**: In Apps > Installed Apps, Administrators can search apps with specific criteria according to attributes combinations, in addition to searching a specified term in different attributes. For more information, see Managing app inventory in the *Core Apps@Work Guide* guide.

- **Send device compliance data to multiple Microsoft Office 365 tenants**: Administrator can configure device compliance data to be sent to multiple Microsoft Office 365 tenants in standard environments. For more information, see "Connecting Microsoft Azure to Core" in the Core Device Management Guide for your OS.

- **New Global Policy to configure apps per label in bulk:** Administrators can create global policies with different app settings (silent install, auto-update, mandatory, etc.) and can assign it to different labels. By creating a global policy, administrators can avoid editing each app and configuring the settings. When viewing and editing the per-label settings, administrators can set the app to default to the global setting so only the settings that are different for that label need to be changed. For more information, see Global App Config Settings policy in the *Core Device Management Guide for Android and Android Enterprise Devices*.

- **Create a default label name:** Starting with the 11.6.0.0 release, administrators had the ability to manually create a label (for Windows, Windows Phone or macOS) that does not contain any criteria. After it is created, the label automatically becomes a default label and cannot be removed or edited. Upon upgrade to version 11.7.0.0, Core does not apply these labels to devices because they do not contain criteria. Administrators must apply the labels manually.

## Android features

- **Support for Private DNS:** On fully-managed devices running Android 10 or later, the administrator can specify whether the device should use a private DNS server for encrypted domain name resolution, and if so, which one. Applicable to: Android 10+ devices in Work Managed Device mode. For more information, see Lockdown policy fields for Android Enterprise devices in Work Profile mode in the *Getting Started with Core* guide.

- **File Transfer Configuration**: A new configuration File Transfer is available for Android devices. This configuration can be used to transfer files to the device and these files can be shared from Mobile@Work to other apps on the same device. Target apps consuming these files must support ContentURI to access files locally on the device.

  For more information, see Android File Transfer Configuration in the *Core Device Management Guide for Android and Android Enterprise Devices.*

- **Mobile@Work auto-granted permissions reduced on all Android device versions:** Administrators can provide device users more choice on Android 11 and below Work Profile devices by allowing the device user to choose whether Mobile@Work should be granted location permissions. The default behavior allows Mobile@Work to automatically grant this permission. In Core 11.7.0.0, when the Mobile@Work auto-grant location permission check box is selected, the administrator would see a warning in Core and device users would receive a prompt to grant Mobile@Work location permission during registration of devices in Work Profile mode.

  Phone permission is required to collect device information. Phone permission allows Mobile@Work to get information about device identifiers such as IMEI. This permission was originally only available in Device Admin mode, but has been extended to Work Profile mode. Device user consent is required for Mobile@Work to have phone permission.

  For more information, see Privacy policies and Understanding the Registration page in the *Getting Started with Core* guide.

- **Shared kiosk mode app settings:** Upon upgrade, two new settings for Shared kiosk mode can be utilized in the New Android Kiosk App Setting Policy dialog box > Kiosk Mode Allowed Apps section:

  - Clear App Data is indicated by a "broom" icon. A broom with check mark icon indicates to clear the app data when the device user logs out of shared kiosk. A broom with a "not allowed" icon indicates do not clear app data when the user logs out of shared kiosk.

  - Android settings are indicated by a "gear" icon. A gear with check mark icon means allows device-wide settings for the selected app to be made available to the device user. A gear with a "not allowed" icon means disallow it.

    For more information, see Configuring the Android shared-kiosk mode in the *Core Device Management Guide for Android and Android Enterprise Devices*.

- **Android Bulk Enrollment:** Administrators can do registration of Android 7+ devices in batches (1000+) by uploading a CSV file. For each profile, a token will be generated with a default expiration time of 7 days. This token can be further extended for 7 days minimum to 99 days maximum. Optionally, the token can be regenerated (a completely new token is created for the profile with a default of 7 days of expiration.) Applicable to Work Managed Device mode, Managed Device with Work Profile mode, Work Profile on Company Owned Device mode, and AOSP mode.

  For more information, see Android Bulk Enrollment in the *Core Device Management Guide for Android and Android Enterprise Devices*.

- **Additional battery health information provided:** Additional battery health statistics per-device are now provided:
  - Android Battery Charging Status
  - Android Battery Health Status
  - Battery Charge Cycles (OEM)*
  - Battery Health Percentage (OEM)*
  - Battery Manufacture Date (OEM)*

  For more information, see Advanced searching in the *Core Device Management Guide for Android and Android Enterprise Devices*.

  *The OEM fields will only populate if the device is a Zebra device. For more information, see Advanced searching in the *Core Device Management Guide for Android and Android Enterprise Devices*.

- **MobileIron Cloud is now Ivanti Neurons for MDM:** All the instances of Cloud in Core documentation have been updated to Ivanti Neurons for MDM.

## iOS features

- **Update iOS Software Version button allows administrators to update iOS devices to a specific OS version:** The Device Details page has a new "Software Version Update" button for administrators to update specific devices to any supervised DEP and non-DEP iOS versions. A list of only the applicable iOS versions to the device displays for the administrator to choose, and then execute the update. For more information, see Updating the iOS manually on a single supervised iOS device in the *Core Device Management Guide for iOS and macOS Devices*.

- **New macOS restrictions:** New macOS restrictions have been added to help administrators delay when device users can download software updates. There are three types of delay options, each with additional options for setting the number of days of delay.

    - Delay OS Software Update - you can set the delay of a software update on the device and set the delay of minor software updates to the device. The device user will not see a software update until the set number of days after the software release date.

    - Delay App Software Update - you can set the delay of a software update on the device and set the delay of non-OS software updates to the device. The device user will not see a non-OS software update until the set number of days after the software release date.

    - Delay Major Software Upgrade - you can set the delay of a major software upgrade on the device. The device user will not see the major software upgrade until the set number of days after the software release date.

      Available in macOS 11.3 and later.

      Additionally, Allow Erase All Content and Setting was added for resetting of iOS devices. Applicable to iOS 8+ and macOS 12+. For more information, see macOS settings and iOS and tvOS restrictions settings in the *Core Device Management Guide for iOS and macOS Devices*.

      ℹ Upon upgrade, the new restrictions will not be pushed to the devices. The easiest way to do this is to open the restriction and then save it. This will force-push to all the devices.

- **Skip options added to Device Enrollment Profile:** To assist with easy installation, two additional options were added to Device Enrollment Profile:

    - Skips Device to Device Migration pane. Availability: iOS 13+.

    - Skips the iMessage pane. Availability: iOS 10+.

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

- **macOS registration configurations enabled upon upgrade:** For new Core deployments, Ivanti's support for macOS device management is available in Core, Ivanti EPM, and Ivanti Neurons for MDM.

- **Version number updated**: Core applications have received the version numbers that are being updated: AppleTV, iOS 15.5 and 15.5.X, macOS 12.4.

- **New iOS Restrictions added to Configurations > New Restrictions Setting dialog box:**
  - Allow Apple TV's automatic screen saver restriction
  - Allow Mail Privacy Protection - helps protect device users' privacy by preventing senders from learning about device users' email activities. When the Allow Mail Privacy Protection configuration is installed and enabled from Core, the Protect Mail Activity toggle is enabled on the device and the following options are visible to the device user:
    - Hide IP Address - The email sender cannot link the email to the device user's online activity or determine location.
    - Block All Remote Content - Prevents the email sender from seeing the device user's email activities.

  For more information, see iOS and tvOS restrictions settings in the *Core Device Management Guide for iOS and macOS Devices*.

## Windows features

- **Windows registration configurations enabled upon upgrade:** For new Core deployments, Ivanti’s support for Windows device management is available in Core, Ivanti EPM, and Ivanti Neurons for MDM.

## Related information from previous releases

If a release does not appear in this section, then there were no associated new features and enhancements.

- Core 11.6.0.1 - New features summary
- Core 11.6.0.0 - New features summary
- Core 11.5.0.0 - New features summary
- Core 11.4.0.0 - New features summary

## Mobile Threat Defense features

Mobile Threat Defense (MTD) protects managed devices from mobile threats and vulnerabilities affecting device, network, and applications. For information on MTD-related features, as applicable for the current release, see the *Mobile Threat Defense Solution Guide* for your platform, available under the **MOBILE THREAT DEFENSE** section on the Ivanti Product Documentation page.

ⓘ Each version of the MTD guide contains all Mobile 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, new versions of the MTD guide are made available with the final release in the series when the features are fully functional.

# Support and compatibility

These are cumulative release notes. If a release does not appear in this section, then the support and compatibility values from the nearest listed older release apply to the missing release.

## SAML / Identity Provider

TABLE 1. SAML / IDENTITY PROVIDER SUPPORTED AND COMPATIBLE PRODUCTS AND COMPONENTS

| Product / Component | Supported | Compatible |
|---|---|---|
| SAML / Identity Provider | • OpenSAML 3.3.0<br>• ADFS<br>• Okta<br>• Ping Identity<br>• OneLogin | • Shibboleth |

## LDAP

TABLE 2. LDAP SUPPORTED AND COMPATIBLE PRODUCTS AND COMPONENTS

| Product / Component | Supported | Compatible |
|---|---|---|
| LDAP | **Windows Active Directory**<br>• Server OS: Windows Server 2012R2, Version 6.3<br>• Server OS: Windows Server 2016, 2019<br>**IBM Domino Server**<br>Server OS: Windows Server 2008, Version: 8.5.2 | **Windows Active Directory**<br>• Server OS: Windows Server 2003, Version: 5.2<br>• Server OS: Windows Server 2008, Version: 6.1 |

## Hardware appliances

TABLE 3. HARDWARE APPLIANCES SUPPORTED AND COMPATIBLE PRODUCTS AND COMPONENTS

| Product / Component | Supported | Compatible |
|---|---|---|
| Hardware appliances | • M2250 (Core)<br>• M2600 (Core)<br>• M2700 (Core) | Not applicable |

## Reporting database

TABLE 4. REPORTING DATABASE SUPPORTED AND COMPATIBLE PRODUCTS AND COMPONENTS

| Product / Component | Supported | Compatible |
|---|---|---|
| Reporting Database | 2.2.0.0 | 2.0.0.2, 2.1.0.0 |

## Monitor

TABLE 5. MONITOR SUPPORTED AND COMPATIBLE PRODUCTS AND COMPONENTS

| Product / Component | Supported | Compatible |
|---|---|---|
| Monitor | 2.2.0.0 | 2.0.0.2, 2.1.0.0 |

## Sentry

TABLE 6. SENTRY SUPPORTED AND COMPATIBLE PRODUCTS AND COMPONENTS

| Product / Component | Supported | Compatible |
|---|---|---|
| Standalone Sentry | 9.15.0, 9.16.0 | 9.4.0–9.14.0 |

## Access

TABLE 7. ACCESS SUPPORTED AND COMPATIBLE PRODUCTS AND COMPONENTS

| Product / Component | Supported | Compatible |
|---|---|---|
| Access | R53 | Not applicable, because only the latest version is available to all customers. |

## Android

TABLE 8. ANDROID SUPPORTED AND COMPATIBLE PRODUCTS AND COMPONENTS

| Product / Component | Supported | Compatible |
|---|---|---|
| Android | 7.0, 8.0, 8.1, 9.0, 10.0, 11.0, 12.0 | |
| Mobile@Work | 11.6.0.0, 11.7.0.0 | 9.3.0.0–11.5.0.0 |
| Ivanti Tunnel (Android native, Android Enterprise, and Samsung Knox Workspace) | 4.7.0 | 4.3.0, 4.3.2, 4.4.0, 4.5.0, 4.6.0, 4.6.1, 4.6.2 |
| Secure Apps Manager | 9.4.0.0 | 8.3.0.0–9.3.0.0 |
| Email+ (Android AppConnect and Android Enterprise) | 4.3.0, 4.4.0 | 3.0.0-4.2.0 |
| Docs@Work (Android AppConnect and Android Enterprise) | 2.19.0, 2.20.0 | 2.0.0-2.18.0 |
| Web@Work (Android AppConnect) | 2.6.1 | 2.1.0–2.6.0 |

## iOS

TABLE 9. IOS SUPPORTED AND COMPATIBLE PRODUCTS AND COMPONENTS

| Product / Component | Supported | Compatible |
|---|---|---|
| iOS | iOS 13.0–iOS 15.5 | iOS 12.0 |
| Mobile@Work | 12.11.60, 12.11.70 | 12.0.0–12.11.50 |

TABLE 9. IOS SUPPORTED AND COMPATIBLE PRODUCTS AND COMPONENTS (CONT.)

| Product / Component | Supported | Compatible |
|---|---|---|
| Ivanti Tunnel | 4.3.1 | 2.4.1-4.1.5, 4.2.0 |
| Email+ | 4.3.0, 4.4.0 | 2.6.0–4.2.0 |
| Docs@Work | 2.20.1 | 2.2.0–2.19.0 |
| Web@Work | 2.15.2 | 2.0.0–2.14.0 |
| Apps@Work Container app | Not supported | • 1.1.2–1.2.0 when using Mobile@Work 8.6.0, 9.0.1, or 9.1.0<br>• 1.3.0 when using Mobile@Work 9.5.0 |
| Help@Work | Help@Work does not work on iOS 10 and newer versions. Use the TeamViewer app for Help@Work support. | 2.0.2–2.1.1 |

## macOS

TABLE 10. MACOS SUPPORTED AND COMPATIBLE PRODUCTS AND COMPONENTS

| Product / Component | Supported | Compatible |
|---|---|---|
| macOS/OS X | 12.4<br>Support for macOS management will be transitioned to Ivanti Endpoint Manager and Ivanti Neurons for MDM. | 10.1–12.3 |
| Ivanti Tunnel | 4.3.1 | 2.4.1-4.1.5, 4.2.0 |

## tvOS

TABLE 11. TVOS SUPPORTED AND COMPATIBLE PRODUCTS AND COMPONENTS

| Product / Component | Supported | Compatible |
|---|---|---|
| tvOS | 15.5.1 | 12.4-15.5 |

## Windows

TABLE 12. WINDOWS SUPPORTED AND COMPATIBLE PRODUCTS AND COMPONENTS

| Product / Component | Supported | Compatible |
|---|---|---|
| Windows | • Windows 10 Pro, Windows 10 Enterprise (version 21H1)<br>• Windows 11 | • Windows 10 Pro, Windows 10 Enterprise (versions 1703, 1709, 1809, 1903, 1909, 2004)<br>• Windows HoloLens (versions 1701, 1803) |
| | **Notes**<br>• Support for Windows management will be transitioned to Ivanti Endpoint Manager and Ivanti Neurons for MDM.<br>• With 1803, Apps@Work cannot be pushed to the device because of a known Microsoft issue. We recommend that customers stay on the H2 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 | 9.6.0.262 | Not applicable (all listed versions are tested and supported) |
| Ivanti Tunnel | 1.2.3 | 1.2.0, 1.2.2 |

## Supported browsers

This version of Core supports the following browsers:

TABLE 13. SUPPORTED BROWSERS

| Browser | Supported | Compatible |
|---|---|---|
| Internet Explorer | 11 | 9*, 10* |
| Chrome | 103 | 100, 101, 102 |
| Firefox | 102 | 99, 100, 101 |
| 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 Ivanti product warranty.

## Supported browser resolutions

TABLE 14. SUPPORTED BROWSER RESOLUTIONS

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

* This configuration is not covered under the Ivanti product warranty.

## Related information from previous releases

If a release does not appear in this section, then the support and compatibility values from the nearest listed older release apply to the missing release.

- Core 11.6.0.0 - Support and compatibility
- Core 11.5.0.0 - Support and compatibility
- Core 11.4.0.0 - Support and compatibility

## Support Policy

TABLE 15. 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. |

# Supported languages

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

## Related information from previous releases

If a release does not appear in this section, then the supported languages from the nearest listed older release apply to the missing release.

- Core 11.6.0.0 - Supported languages
- Core 11.5.0.0 - Supported languages
- Core 11.4.0.0 - Supported languages

## 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 devices and macOS devices (legacy features)

See *Mobile@Work for iOS Release Notes* for a complete list of supported languages for iOS devices.

See *Mobile@Work for macOS Release Notes* for a complete list of supported languages for macOS devices.

## Language support on Windows devices (legacy features)

Core supports the following languages and locales 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

These are cumulative release notes. If a release does not appear in this section, then there are no associated resolved issues.

- **VSP-67777**: In previous releases, when you tried to register an iOS device in iReg using an email address as the username and RegMode as the password, a Role Lookup error occurred. In this release, registration with an email username and RegMode as password proceeds as expected.
- **VSP-67582:** When adding a single device, there were JSON parsing errors. This issue has been fixed.
- **VSP-67503**: In previous releases, custom apps from the Apple Business manager sometimes failed to update the latest details and versions in the App Catalog. In this release, app detail and version updates occur correctly.
- **VSP-67300**: In previous releases, the iOS Trusted Operating System (TOS) email to the admin was not delivered. In this release, email delivery occurs normally.
- **VSP-67285**: In previous releases, copying an existing managed app configuration with the default app configuration failed. In this release, copying the app configuration works as expected.
- **VSP-67267**: In previous releases, Apps@Work on the iPad did not start in full-screen mode even though it was configured correctly. In this release, Apps@Work opens in full-screen mode.
- **VSP-67244**: In previous releases, a blank page and an invalid JSON string were sometimes displayed when accessing the Labels tab in the Core UI. In this release, the Labels tab is displayed correctly.
- **VSP-67238**: In previous releases, on the Android platform, when the browser language is German, the user portal did not display the registration PIN when the Request Registration PIN operation was performed. In this release, the PIN is displayed as expected.
- **VSP-67234**: In previous releases, using iReg to download the Mobile@Work client failed if the admin portal was not configured to run on port 443. In this release, the download is successful.

- **VSP-67225**: In previous releases, entering information in the Notes field of the Devices dialog box automatically enabled the Retire action button. In this release, you must specifically select the new checkbox to enable the button.
- **VSP-67204:** In previous releases, licenses corresponding to retired devices were erroneously displayed as still in use, and Apple continued to associate the license with the retired device. In this release, these licensing issues no longer occur.
- **VSP-67174**: In previous releases, quotes and angle bracket errors in the syslog templates caused incorrectly generated syslog configuration files. In this release, the configuration files are generated correctly.
- **VSP-67141**: In previous releases, failover client-connection commands that disable or enable client connections were only successful on non-mutual-auth cores. In this release, the commands are also successful on mutual-auth cores.  
  **Note**: After disabling client connections on mutual-auth cores, the connections can become spontaneously reenabled if you make changes that affect the port 443 listener configuration, such as when adding or removing ciphers.
- **VSP-67113**: In previous releases, the Core server erroneously sent uninstall requests for Android apps that were not in a device's inventory. In this release, only apps that are in the device's inventory receive uninstall requests.
- **VSP-67082**: In previous releases, when you registered an Android 10 or above device in DA mode on a mutual-auth core, entries in the Devices page were deleted. In addition, LDAP and Space syncs failed. In the current release, the entries are no longer deleted and the syncs occur successfully.
- **VSP-67046**: In previous releases, an authentication error occurred when you sent emails from System Manager through a StartTLS-required Simple Mail Transfer Protocol (SMTP) server. In this release, no error occurs and the emails are sent out as expected.
- **VSP-66937**: In previous releases, certificate expiry warnings were issued to all certificates in a certificate chain. In this release, certificate expiry warnings are only issued to the certificates that are actually expiring.
- **VSP-66907**: In previous releases, when an Apple Device Name policy was attached to a Label and later removed, the Device page continued to show the policy as Pending. In this release, the policy is removed from the device as expected.

- **VSP-66905**: In previous releases, when you selected the Data Sweeper app from the App Catalog, you received an internal server error if the restriction field for `restriction_type="BUNDLE"` was empty. In this release, no internal error occurs and the values are parsed correctly.

- **VSP-66771**: In previous releases, an APN configuration failed to be applied to a device if that device was registered to a user who did not have mail. In this release, the configuration is applied successfully.

- **VSP-66509**: In previous releases, upgrading a FIPS or Common Criteria system using the validate feature could cause a package verification failure and render the system unbootable. In this release, the process works as expected as long as you use the re-validate function instead of the resume validation function during the upgrade.

- **VSP-66278**: In previous releases, on Windows 10 Desktop touch devices, there was no Core Admin Portal scroll bar. In this release, the scroll bar is visible.
  **Note**: To scroll through tables and lists, scroll while holding down the left button on the track pad or mouse.

- **VSP-66002**: In previous releases, the `purgedb` operation failed when it did not receive a number of days parameter from the `optimizedb` operation. In this release, when the optimizedb script does not send a number of days parameter, purgedb purges the records that are older than 7 days.

- **VSP-65679**: In previous releases, if an administrator specified `Auto` as the configuration proxy type in the Device Wi-Fi configuration, but did not provide a proxy automatic configuration (PAC) URL, the generated Wi-Fi configuration set the type as `None`. In this release, the Wi-Fi configuration does not require a proxy automatic configuration URL to generate an `Auto` configuration type.

  **Note**: To correct the error in a legacy device whose configuration proxy was already erroneously interpreted in the Device Wi-Fi configuration, repush the configuration proxy.

- **VSP-65554**: In previous releases, iOS device users could complete the Apple User Enrollment process even if they did not have enrollment privileges. In this release, unenrolled users cannot complete the enrollment.

- **VSP-65283**: In previous releases, the Storage Capacity and Storage Free fields in the Device Details page were shown only with a power of 10 divisor (for example, MB, GB). In this release, the fields now also shown with a power of 2 divisor (for example, MiB, GiB). For more information, see "Advanced Searching" in the Core Device Management Guide of your OS.

- **VSP-64912**: In previous releases, when the Core Admin portal was configured to access port 8443, the self-service user portal text was misaligned due to a stylesheet issue. In this release, the text is no longer misaligned.

## Related information from previous releases

If a release does not appear in this section, then there were no associated resolved issues.

- Core 11.6.0.1 - Resolved issues
- Core 11.6.0.0 - Resolved issues
- Core 11.5.0.0 - Resolved issues
- Core 11.4.1.0 - Resolved issues
- Core 11.4.0.0 - Resolved issues

# Known issues

These are cumulative release notes. If a release does not appear in this section, then there are no associated known issues.

- **VSP-67818**: Apple-driven UE registration fails when the email ID is used as the username.
  **Workaround**: None.

- **VSP-67696**: Currently, the `Use Tunnel for Anti-phishing only` option is not saved as the default configuration in the Tunnel app.
  **Workaround**: Add another configuration (other than the default), set it to Anti-Phishing only, and then select **Save**.

- **VSP-67686**: Currently, you receive an "`Internal Server Error`" message if you try to enter a special character in the Custom Attribute field. This field does not accept special characters.
  **Workaround**: None.

- **VSP-67672**: Currently, when you try to edit a VPN with a Device Channel type in the configuration view, the channel type is erroneously displayed as a User Channel type. If you try to change the User Channel type back to a Device Channel type the system displays the following error: "`Nothing has changed`." The channel type is correctly displayed in the Configuration Details pane on the configuration page.
  **Workaround**: None.

- **VSP-67619**: Currently, you are unable to save sentry settings after disabling an ActiveSync service that was enabled with Kerberos authentication.
  **Workaround**:

  a. Edit the Sentry Settings.

  b. Enable the **ActiveSync service> scroll down > Change the Authentication to Pass Thru** page.

  c. Disable **ActiveSync**.

  d. Delete the **Certificate Mapping** field.

  e. Save the **Sentry** settings.

- **VSP-67603**: Currently, no confirmation message pops up when you perform **Force retire the retire pending devices now** and **Force retire all the retire pending devices** actions.
  **Workaround**: None.

- **VSP-67600**: Currently, the Core server erroneously creates SCEP certificates even though the device VPN configuration has been deleted.
  **Workaround**: None.

- **VSP-67598**: Currently, using the Advanced search criteria for the RETIRE_PENDING status in combination with other criteria results in an error.
  **Workaround**: Enclose the RETIRE_PENDING status search criteria in parentheses: `("common.status" = "RETIRE_PENDING") AND "common.platform" = "macOS"`.

- **VSP-67557**: Currently, the VPP app license is revoked even though a device is in a Retire Pending state.
  **Workaround**: None.

- **VSP-67421**: Currently, when you apply multiple Single-App Mode policies to a device, only the policy that arrives first is applied, even if another policy with higher prioritization is applied later.
  **Workaround**: None.

- **VSP-67389**: When the administrator adds devices through the Android Bulk Enrollment profile, information is displayed, even if all the devices fail to import.
  **Workaround**: None.

- **VSP-67386**: Currently, the Device Detail window shows software version update options for devices that are in the Active state, in addition to devices that are in the Retire Pending state. The window should only show options for devices in Active state.
  **Workaround**: None.

- **VSP-67361**: Currently, multi-user webclips fail to install because they are not supported in this version.
  **Workaround**: None.

- **VSP-67353**: Currently, software update information for a device is unavailable when there is a error communicating with Apple.
  **Workaround**: None.

## Related information from previous releases

If a release does not appear in this section, then there were no associated known issues.

- Core 11.6.0.1 - Known issues
- Core 11.6.0.0 - Known issues
- Core 11.5.0.0 - Known issues
- Core 11.4.0.0 - Known issues

# Limitations

These are cumulative release notes. If a release does not appear in this section, then there are no associated third-party limitations.

## Related information from previous releases

If a release does not appear in this section, then there were no associated limitations.

- Core 11.6.0.0 - Limitations
- Core 11.5.0.0 - Limitations
- Core 11.4.0.0 - Limitations

# Core upgrade information

For detailed instructions on how to upgrade Core using this upgrade information, refer to the *Core System Manager Guide*.

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

- Core upgrade readiness checklists
- Check disk space availability
- Core upgrade paths
- Core upgrade URL
- Backing up Core

**Before you begin**

Read "Before you upgrade" on page 4.

## 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

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

**TABLE 16.** PRE-UPGRADE CHECKLIST

| Check | Tasks | References |
|---|---|---|
| | Prepare and plan for downtime | • Core (1 - 3 hours)<br>• Sentry (5 - 20 minutes) |
| | Review relevant documentation | See Core product documentation. |

TABLE 16. PRE-UPGRADE CHECKLIST (CONT.)

| Check | Tasks | References |
|---|---|---|
| | Check certificates | • iOS Enrollment, Portal HTTPS, Client TLS certificates<br>ⓘ 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 Core in the Core Device Management Guide for iOS and macOS Devices.<br>• MDM Certificate (check a month before expires)<br>• Local CA<br>**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" on page 35 in this document for details on how to perform this check.<br>**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)<br>• New File System (10 GB /mi)<br>• If there is insufficient storage, increase the available disk space. See this VMware knowledge base (KB) article and this VMware KB article for information. Note that these are third-party articles hosted by VMware, whose locations are subject to change. Contact Ivanti Support if you need shell access to the Core VM. |
| | Check for new system requirements | • Minimum 80 GB hard drive<br>• If there is insufficient storage, increase the available disk space. See this VMware knowledge base (KB) article and this VMware KB article for information. Note that these are third-party articles hosted by VMware, whose locations are subject to change. Contact Ivanti Support if you need shell access to the Core VM.<br>• Call Ivanti support if issues persist when physical appliances and VMs have the minimum required disk space configured |

TABLE 16. PRE-UPGRADE CHECKLIST (CONT.)

| Check | Tasks | References |
|---|---|---|
| | | - Port 8443 for Summary MICS - Configuration Service (that is, the service that supports System Manager.) |
| | Review your backup and high availability options | - Physical backup: built in backup, showtech all<br>- VMware backup: VDMK backup, snapshot<br>- High Availability: confirm HA version 2.0<br>**Knowledge Base article**: How to tell if your Core has HA 2.0<br>If using HA 1.0, contact Ivanti 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.<br>- **Core**: Note the watchlist and label numbers. |

## Upgrade considerations

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

TABLE 17. 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 Ivanti Support. |
| | Understand the stages | - Download vs. Stage for install<br>- Reboot when the system displays:<br>Reboot to install https://<serverFQDN>:8443/upgrade/status |
| | Leverage CLI upgrade commands (as appropriate) | See Core Command Line Interface (CLI) Reference. |
| | Understand scenario options | **Single server**<br>**High availability—Option 1**: little downtime:<br>- Upgrade secondary |

TABLE 17. UPGRADE CONSIDERATIONS (CONT.)

| Check | Considerations | References |
|---|---|---|
| | | • Upgrade primary<br>**High availability—Option 2**: zero downtime:<br>• Upgrade secondary<br>• Failover to secondary<br>• Upgrade primary<br>• Re-establish sync<br>**Download guide**: *Core High Availability Management Guide*<br>**Review section**: HA Core Software Upgrade Procedures |
| | Monitor the upgrade | • Log into the Admin Portal<br>• Select **Logs** > **MDM Logs** > **States** > **Waiting XML generation pending**<br>• 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 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.<br>For more information, see the following knowledge base article: Core Product Bulletin: Reset Pin command Fails to return a New Pin for Windows Phones 10 Devices |
| | 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

After completing the upgrade, we recommend the following verification checklist.

**TABLE 18.** POST-UPGRADE CHECKLIST

| Check | Tasks | References |
|---|---|---|
|  | Testing and troubleshooting | 1. Log into the System Manager<br>2. Select **Maintenance > Software Updates > Software Version**<br>3. Verify that the new version is listed<br>4. DO NOT re-boot the system once the upgrade process has begun<br>5. Call Ivanti Support for further investigation |
|  | Verify services | • Log into the Admin Portal<br>• Select **Services > Overview**<br>• Click **Verify All** |
|  | Verify devices | • Register a new device<br>• Re-enroll/check-in existing devices |
|  | HA system cleanup | • Set secondary back to secondary<br>• 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 Ivanti Technical Support before proceeding with the upgrade.

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

## The CLI command: show system disk

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

```
CORE(8.5.0.1a-6)@host.company.com#show system disk

Filesystem Size Used Avail Use% Mounted on

/dev/sda3 181G 20G 153G 12% /
```

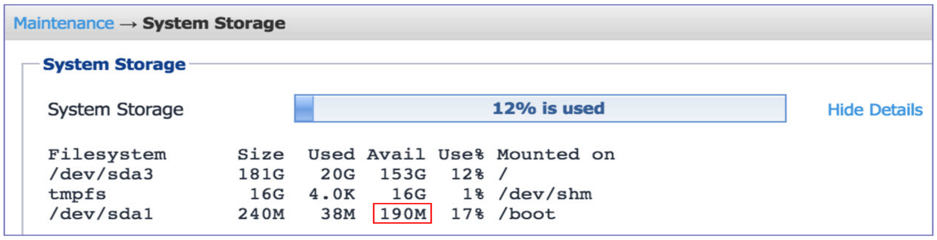
```
tmpfs 16G 4.0K 16G 1% /dev/shm

/dev/sda1 95M 76M 15M 84% /boot
```

## The System Manager

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

### Procedure

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



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

## Core upgrade paths

We recommend the following upgrade paths, which are fully tested and supported.

- 11.5.0.0 → 11.7.0.0
- 11.6.0.1 → 11.7.0.0
- 11.7.0.0 (GMRC) → 11.70.0

## Related information from previous releases

- Core 11.6.0.1 - Upgrade paths
- Core 11.6.0.0 - Upgrade paths
- Core 11.5.0.0 - Upgrade paths
- Core 11.4.1.0 - Upgrade paths
- Core 11.4.0.0 - Upgrade paths

# Core upgrade URL

To upgrade Core, use the following URL if you specify an alternate URL:

**https://support.mobileiron.com/mi/vsp/11.7.0.0-45/mobileiron-11.7.0.0-45**

## Related information from previous releases

- Core 11.6.0.1 - Upgrade URL
- Core 11.6.0.0 - Upgrade URL
- Core 11.5.0.0 - Upgrade URL
- Core 11.4.1.0 - Upgrade URL
- Core 11.4.0.0 - Upgrade URL

# Backing up Core

We recommend that you make a local backup of Core before starting an upgrade. For more information on backing up Core, see the Core System Manager Guide.

# Enterprise Connector upgrade information

For detailed instructions on how to upgrade Enterprise Connector using this upgrade information, refer to the *Core System Manager Guide*.

- "About Enterprise Connector upgrade" below
- "Enterprise Connector upgrade paths" below
- "Enterprise Connector upgrade URL " on the next page

## About Enterprise Connector upgrade

In most cases, Enterprise Connector is upgraded automatically after a 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 explained in the *On-Premise Installation Guide for Core and Enterprise Connector*.

## Enterprise Connector upgrade paths

Enterprise Connector releases can be directly upgraded only from the following listed releases:

11.5.0.0 → 11.7.0.0

11.6.0.1 → 11.7.0.0

11.7.0.0 (GMRC) → 11.70.0

### Related information from previous releases

- Core 11.6.0.1 - Connector upgrade paths
- Core 11.6.0.0 - Connector upgrade paths

- Core 11.5.0.0 - Connector upgrade paths
- Core 11.4.1.0 - Connector upgrade paths
- Core 11.4.0.0 - Connector upgrade paths

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

To upgrade Enterprise Connector, use the following URL if you specify an alternate URL:

**https://support.mobileiron.com/mi/connector/11.7.0.0-45/mobileiron-11.7.0.0-45**

## Related information from previous releases

- Core 11.6.0.1 - Connector upgrade URL
- Core 11.6.0.0 - Connector upgrade URL
- Core 11.5.0.0 - Connector upgrade URL
- Core 11.4.1.0 - Connector upgrade URL
- Core 11.4.0.0 - Connector upgrade URL

# Documentation resources

Product documentation is available on the Ivanti documentation website, help.ivanti.com. You can access Core documentation directly at this link.

To select a product document:

1. Navigate to the Ivanti documentation website.

2. Optionally, select a product category and language.

3. Enter a search term, or scroll down the product list.

4. Click the documentation link to open the document in a new window.

## Core documentation

The following is a complete list of documentation for this product. However, the list of documents updated for specific versions will vary, depending on release requirements. Therefore, you might encounter documents from previous releases that still apply to the current release.

- *Core Release Notes and Upgrade Guide* — Contains the following release-specific information: new feature summary, support and compatibility, upgrade notes, known and resolved issues, and limitations.

- *On-Premise Installation Guide for Core and Enterprise Connector* — Contains information needed to install Core on a VM or on an appliance. You will find pre-deployment tasks, steps to install and configure Core and Enterprise Connector, and set up the VMware tool.

- *Getting Started with Core* — Contains information you need to get started with Core. Contains an introduction to the Admin Portal, information about setting up users, devices, and basic policies, managing the dashboard, labels, and custom attributes, registering devices using the Mobile@Work. Mobile@Work does not have a separate product guide.

- *Core System Manager Guide* — Everything you need to know about configuring Core system settings, managing network settings, performing maintenance tasks including upgrading Core, and troubleshooting issues using the Core System Manager.

- *Core Apps@Work Guide* — The complete guide to installing, setting up, and managing apps for devices. Information about the Email+, Web@Work, and Docs@Work are covered in the guides for the apps.

- *Core Delegated Administration Guide* — The complete guide to configuring and maintaining delegated administration with Core.

- *Core Device Management Guide for Android and Android Enterprise Devices*
  *Core Device Management Guide for iOS and macOS Devices*
  *Core Device Management Guide for Windows, including Windows 10 Devices* — Everything you need to know about setting up and managing devices on Core. Each volume is specific to a general device platform. Information about Sentry, AppTunnel, ActiveSync, AppConnect, Access, and Zero Sign-on are covered in the related product guides.

- *Core High Availability Management Guide* — This document includes steps for setting up Core High Availability as well as a description of common HA scenarios and troubleshooting tips.

- *Core Command Line Interface (CLI) Reference* — The Core command line interface (CLI) enables you to access certain Core capabilities from the command line. The reference describes how to access the CLI, use the help, the various command modes, and the available commands.

- *Core V2 API Guide* — API reference guide for the version 2 public APIs.

- *V1 API Reference Guide for Core WebService* — This reference guide provides development information for customers and partners intending to use WebService APIs.

- *Common Platform Services API Guide* — Describes how to use the Event Notification Service and Common Platform Services (CPS) API with Ivanti Neurons for MDM and Core.

- *ServiceNow Integrator Update Set Guide* — Describes how to set up and use the ServiceNow Integrator Update Set.

- *Mobile@Work for Android Release Notes* — Contains the following release-specific information: new feature summary, support and compatibility, known and resolved issues, and limitations.

- *Mobile@Work for iOS Release Notes* — Contains the following release-specific information: new feature summary, support and compatibility, known and resolved issues, and limitations.

- *Mobile@Work for macOS Release Notes* — Contains the following release-specific information: new feature summary, support and compatibility, known and resolved issues, and limitations.