

Core and Connector 11.2.0.0 Release and Upgrade Notes

April 19, 2021

For complete product documentation, see:
[Ivanti Documentation Home Page](#)

Contents

| | |
|--|-----------|
| About Core | 3 |
| Before you upgrade | 4 |
| Understand the impact of TLS protocol changes | 4 |
| New features and enhancements summary | 6 |
| General features and enhancements | 6 |
| Android and Android Enterprise features and enhancements | 6 |
| iOS and macOS features and enhancements | 6 |
| Windows features and enhancements | 7 |
| Mobile Threat Defense features | 7 |
| Support and compatibility | 8 |
| Supported components | 8 |
| Supported browsers | 14 |
| Supported browser resolutions | 14 |
| Supported languages | 15 |
| Supported languages for Core messages | 15 |
| Language support on Android and Android Enterprise devices | 16 |
| Language support on iOS and macOS devices | 16 |
| Language support on Windows devices | 16 |
| Resolved issues | 17 |
| Known issues | 19 |
| Limitations | 20 |
| Upgrade information | 21 |
| Core upgrade readiness checklists | 21 |
| Check disk space availability | 25 |
| Core upgrade paths | 26 |
| Core upgrade URL | 26 |
| Backing up Core | 26 |
| Enterprise Connector upgrade information | 27 |
| About Enterprise Connector upgrade | 27 |
| Enterprise Connector upgrade paths | 27 |
| Enterprise Connector upgrade URL | 27 |
| Enterprise Connector upgrade notes | 28 |
| Documentation resources | 29 |
| Core documentation | 29 |

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
- Integrated 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://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 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 and enhancements summary

This section provides summaries of new features and enhancements available in this release. References to documentation describing these features and enhancements are also provided, when available.

- [General features and enhancements](#)
- [Android and Android Enterprise features and enhancements](#)
- [iOS and macOS features and enhancements](#)
- [Windows features and enhancements](#)
- [Mobile Threat Defense features](#)

For new features and enhancements provided in previous releases, see the release notes for those releases.

General features and enhancements

This release includes the following new features and enhancements that are common to all platforms.

- **Maximum password length now enforced throughout Core:** Core now verifies that every password falls within the configured maximum allowed length, set in the Settings > Security > Password Policy > Maximum Password Length value. This provides better protection against Denial of Service (DOS) attacks. Password minimum length can be between 6-16 characters, and password maximum length between 21-32 characters. For information about configuring passwords, see [Local user password complexity enforcement details](#) in *Getting Started with Core*.
- **Content changes for rebranding and distribution:** Product documentation has been rebranded to align with Ivanti standards and is now available on the [Ivanti documentation website](#).

Android and Android Enterprise features and enhancements

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

iOS and macOS features and enhancements

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

- **New restrictions added for iOS 14.5 devices:** Three new iOS restrictions have been added:
 - Join only WiFi networks installed by a WiFi payload
 - Allow auto unlock
 - Allow putting into recovery mode from an unpaired device

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

- **New policy added - eSIM Refresh Cellular Plan:** Embedded SIMs ("eSIM") make it easier to switch from one cellular carrier to another. This new feature allows administrators to configure an eSIM Refresh Cellular Plan policy using the carrier's URL. Applicable only to iPads with iPadOS 13.0+ and iOS 14.0+ that have a cellular plan.

For more information, see [Configuring an eSIM refresh cellular plan policy](#) in the *Core Device Management Guide for iOS and macOS Devices*.

- **Configure Encrypted DNS settings:** Encrypted DNS allows administrators to enhance security without needing to configure a VPN. These settings can be managed via MDM. This feature is supported on iOS 14.0+ and macOS 11.0+ devices. For more information, see [Configuring encrypted DNS settings](#) in the *Core Device Management Guide for iOS and macOS Devices*.

Windows features and enhancements

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

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

This section includes the components that are supported with this release of Core.



This information is current at the time of this release. For product versions released after this release, see that product version's release notes for the most current support and compatibility information.

TABLE 1. 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 components

This version of Core is supported and compatible with the following product versions:

- [SAML / Identity Provider](#)
- [LDAP](#)
- [Hardware appliances](#)
- [Reporting database](#)
- [Monitor](#)
- [Sentry](#)
- [Access](#)
- [Android](#)
- [iOS](#)
- [macOS](#)
- [tvOS](#)
- [Windows](#)

SAML / Identity Provider

TABLE 2. SAML / IDENTITY PROVIDER SUPPORTED AND COMPATIBLE PRODUCTS AND COMPONENTS

| Product / Component | Supported | Compatible |
|--------------------------|---|--|
| SAML / Identity Provider | <ul style="list-style-type: none"> • OpenSAML 3.3.0 • ADFS 3.0 • Okta - Developer Account 3.6.0 • Ping Identity – Trial version 1.3.0 • OneLogin – Developer Account | <ul style="list-style-type: none"> • Shibboleth |

LDAP

TABLE 3. LDAP SUPPORTED AND COMPATIBLE PRODUCTS AND COMPONENTS

| Product / Component | Supported | Compatible |
|---------------------|--|----------------|
| LDAP | <p>Windows Active Directory</p> <ul style="list-style-type: none"> • Server OS: Windows Server 2003, Version: 5.2 • Server OS: Windows Server 2008, Version: 6.1 • Server OS: Windows Server 2012R2, Version: 6.3 <p>IBM Domino Server</p> <ul style="list-style-type: none"> • Server OS: Windows Server 2008, Version: 8.5.2 | Not applicable |

Hardware appliances

TABLE 4. HARDWARE APPLIANCES SUPPORTED AND COMPATIBLE PRODUCTS AND COMPONENTS

| Product / Component | Supported | Compatible |
|---------------------|---|----------------|
| Hardware appliances | <ul style="list-style-type: none"> • M2200 (Core and Enterprise Connector) • M2250 (Core) • M2600 (Core) | Not applicable |

Reporting database

TABLE 5. REPORTING DATABASE SUPPORTED AND COMPATIBLE PRODUCTS AND COMPONENTS

| Product / Component | Supported | Compatible |
|---------------------|-----------|------------------------------------|
| Reporting Database | 2.1.0.0 | 1.9.1.0, 2.0.0.0, 2.0.0.1, 2.0.0.2 |

Monitor

TABLE 6. MONITOR SUPPORTED AND COMPATIBLE PRODUCTS AND COMPONENTS

| Product / Component | Supported | Compatible |
|---------------------|-----------|------------------------------------|
| Monitor | 2.1.0.0 | 1.2.1.0, 2.0.0.0, 2.0.0.1, 2.0.0.2 |

Sentry

TABLE 7. SENTRY SUPPORTED AND COMPATIBLE PRODUCTS AND COMPONENTS

| Product / Component | Supported | Compatible |
|---------------------|-----------|--------------|
| Standalone Sentry | 9.12.0 | 9.8.1, 9.9.0 |
| Integrated Sentry | 6.4.0 | 6.2.0–6.3.0 |

Access

TABLE 8. ACCESS SUPPORTED AND COMPATIBLE PRODUCTS AND COMPONENTS

| Product / Component | Supported | Compatible |
|---------------------|-----------|--|
| Access | R46 | Not applicable, because only the latest version is available to all customers. |


Android

TABLE 9. ANDROID SUPPORTED AND COMPATIBLE PRODUCTS AND COMPONENTS

| Product / Component | Supported | Compatible |
|---|---|---------------------------------|
| Android | 8.0, 8.1, 9.0, 10.0, 11.0 | 5.0–7.1 |
| Mobile@Work | 11.1.0.0, 11.2.0.0* * Mobile@Work 11.2.0.0 is targeted to release on April 12, 2021 | 9.3.0.0–11.0.0.0 |
| Tunnel (Android native, Android Enterprise, and Samsung Knox Workspace) | 4.6.0 | 4.3.0, 4.3.2, 4.4.0, 4.5.0 |
| Secure Apps Manager | 9.1.0.0, 9.2.0.0 | 8.3.0.0–9.0.0.0 |
| Email+ (Android AppConnect and Android Enterprise) | <ul style="list-style-type: none"> 2.19.0.0 3.9.0, 3.10.0* * Email+ 3.10.0 is targeted to release on April 12, 2021 | 2.2.0.0–2.18.3.0 3.0.0–3.8.0 |
| Docs@Work (Android AppConnect and Android Enterprise) | 2.14.0, 2.15.0 | 2.0.0–2.13.0 |
| Web@Work (Android AppConnect) | 2.5.1 | 2.1.0–2.4.2 |

iOS

TABLE 10. iOS SUPPORTED AND COMPATIBLE PRODUCTS AND COMPONENTS

| Product / Component | Supported | Compatible |
|----------------------------|---|---|
| iOS | 12.0.0–14.0.0 | 11.0.0 |
| Mobile@Work | 12.11.1, 12.11.10 | 12.0.0–12.4.0 |
| Tunnel | 4.1.0 | 2.4.1–4.0.0 |
| Email+ | 3.17.1 | 2.6.0–3.16.0 |
| Docs@Work | 2.16.1 | 2.2.0–2.15.1 |
| Web@Work | 2.13.0 | 2.0.0–2.12.1 |
| Apps@Work Container app | Not supported | <ul style="list-style-type: none"> • 1.1.2–1.2.0 when using Mobile@Work 8.6.0, 9.0.1, or 9.1.0 • 1.3.0 when using Mobile@Work 9.5.0 |
| Help@Work |  Help@Work does not work on iOS 10 and newer supported releases. Use TeamViewer App instead for Help@Work support. | 2.0.2–2.1.1 |

macOS

TABLE 11. macOS SUPPORTED AND COMPATIBLE PRODUCTS AND COMPONENTS

| Product / Component | Supported | Compatible |
|---------------------|--------------|--------------|
| macOS/OS X | 11.2 | 10.1–10.15 |
| Tunnel | 4.1.0, 4.1.1 | 3.0.0, 4.0.0 |

tvOS

TABLE 12. TVOS SUPPORTED AND COMPATIBLE PRODUCTS AND COMPONENTS

| Product / Component | Supported | Compatible |
|---------------------|------------|------------|
| tvOS | 13.4, 14.0 | 12.4–13.4 |

Windows

TABLE 13. WINDOWS SUPPORTED AND COMPATIBLE PRODUCTS AND COMPONENTS

| Product / Component | Supported | Compatible |
|---------------------|--|---|
| Windows | Windows 10 Pro, Windows 10 Enterprise (version 20H2) | <ul style="list-style-type: none"> Windows 10 Pro, Windows 10 Enterprise (versions 1703, 1709, 1809, 1903, 1909, 2004) Windows HoloLens (versions 1701, 1803) <p>Note The Following:</p> <ul style="list-style-type: none"> With 1803, Apps@Work cannot be pushed to the device because of a known Microsoft issue. We recommend 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. <p>For more information, see https://support.microsoft.com/en-us/help/13853/windows-lifecycle-fact-sheet.</p> |
| 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

TABLE 14. SUPPORTED BROWSERS

| Browser | Supported | Compatible |
|-------------------|---------------|----------------|
| Internet Explorer | 11 | 9*, 10* |
| Chrome | 89 | 88, 87, 86 |
| Firefox | 87 | 86, 85, 84 |
| 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 15. 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.

Supported languages

Core supports the following languages on devices for messages and apps:

- [Supported languages for Core messages](#)
- [Language support on Android and Android Enterprise devices](#)
- [Language support on iOS and macOS devices](#)
- [Language support on Windows devices](#)

Supported languages for Core messages

Core supports the following languages and locales 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

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

For resolved issues fixed in previous releases, see the "Resolved issues" section in the release notes for those releases.

This release includes the following resolved issues.

- **VSP-64953:** There was an issue where an LDAP user with a password that was more than 32 characters long was unable to complete device registration or log into the Core Admin and User portals. This issue has been fixed. LDAP users can now register and log successfully into Core with passwords of up to 128 characters.
- **VSP-64748:** Syslog data export jobs have been changed in how they inject data into the syslog stream. This change will not automatically take effect after an upgrade to Core 11.2.0.0. To make this change take effect, syslog exports will have to be disabled and then reenabled. The easiest way to do this is to set the administrative state of all enabled syslog target servers to "disabled" and then back to "enabled."
- **VSP-64737:** There was an issue with earlier releases defaulting to "Device Enrollment" for "User Enrollment" users who were trying to register an iPad. This issue has been fixed. User enrollment now allows iPadOS registrations.
- **VSP-64632:** There was an issue whereby VMware-based macOS devices registered using International Roaming Expert Group (iREG) or Apple Automated Device Enrollment (DEP) could not subsequently register to Mobile@Work, because the Wi-Fi MAC address was not reported properly to Core. This issue has been fixed. VMware-based macOS devices using iREG or DEP can register to Mobile@Work as expected, for 11.2.0.0 and supported newer versions.
- **VSP-64583:** Core now supports up to 15,000 LDAP groups for 11.2.0.0 and newer versions. Previously, Core supported a maximum of 10,000 LDAP groups.
- **VSP-64558:** There was an issue with displaying large numbers of Lightweight Directory Access Protocol (LDAP) groups in Core. Because they were displaying in the order they were retrieved from the database, finding a particular group was difficult. This issue has been fixed. LDAP groups now display in alphabetical order in the Admin portal.
- **VSP-64520:** Local Certificates of Authority (CA) are now exported with encrypted passwords. Due to this security upgrade, configuration files with local CAs from earlier releases cannot be imported into Core 11.2.0.0. The local CA will need to be recreated within Core 11.2.0.0 or newer supported versions to bring the configuration into security compliance.
- **VSP-64517:** There was an issue with a TeamViewer launch URL not working as expected when the "Launch TeamViewer session" was displayed for copying. This issue has been fixed. You can now click to select and copy the TeamViewer URL.

- **VSP-64459:** Android Open Source Project (AOSP) mode registration now supports Simple Certificate Enrollment Protocol (SCEP) configurations. Use the following workaround for devices registered prior to Core 11.2.0.0:
 1. Create a static test label and apply this to all the impacted devices.
 2. Apply the test label to the required SCEP configurations.
 3. Remove the test label from the SCEP configuration and devices.
- **VSP-64390:** There was an issue where, when an LDAP configuration was associated with 10,000 or more groups, sometimes there was a slow response or timeout of the user interface while rendering the list. This issue has been fixed.
- **VSP-63780:** There was an issue within the Self-Service Portal, where some English text strings were not being translated into Korean and Japanese. This issue has been fixed. Korean and Japanese text now render as expected.
- **VSP-63479:** There was an issue where a menu item was alphabetized incorrectly in the **Connection Type** drop-down menu on the **Policies & Configs > Configs > Add New > VPN** dialog box. This issue has been fixed, and the list now displays alphabetically.
- **VSP-62503:** There was an issue with Core-managed Android devices not honoring the custom selection defined in the "Mutual Authentication Certificate Enrollment" configuration. This issue has been fixed. Core 11.2.0.0 and later supported releases support custom subjects in the "Mutual Authentication Certificate Enrollment" configuration.



The SCEP subject field is case-sensitive, and must be configured with capital letters.

Known issues

For known issues found in previous releases, see the "Known issues" section in the release notes for those releases.

This release includes the following known issues.

- **VSP-65009:** There is an issue when Federal Information Processing Standards (FIPS) is enabled or disabled in Core, which prevents the Apache Tomcat web container from starting.
Workaround: Contact Ivanti support for information about this workaround.
- **VSP-64962:** There is an issue with macOS devices during iReg or DEP enrollment, in which the FileVault policy is not successfully pushed to the devices. Enrollment succeeds, but device encryption cannot be enabled.
Workaround: A database trigger is available from Ivanti Customer Support for those users who need device encryption.
- **VSP-64912:** There is an issue when the Core Admin portal is configured to access port 8443, the self-service user portal text is misaligned due to a stylesheet issue.
Workaround: Use port 443 to access the Core Admin portal. For more information, see the chapter "Pre-deployment tasks" in the *On-Premise Installation Guide for Core and Enterprise Connector*.
- **VSP-64868:** There is an issue where an iPad image displays on the Self-service portal instead of an iPhone, when the phone number is not present.
- **VSP-64835:** There is an issue where Core continues to hold the Integrated Circuit Card Identification Number (ICCID) of a device in memory, even after the SIM card is removed.
- **VSP-64820:** There is an issue with iPad devices failing iReg registration when the Apple Safari browser is in Mobile mode.
- **VSP-64796:** There is an issue where the host "pcs.mobileiron.com" must be whitelisted for Core outbound connections when the Azure device compliance feature is enabled.
- **VSP-64669:** There is an issue where, when a managed configuration is added to a device and a label is applied, if the app configuration is saved as the lowest priority configuration, the label does not display in the Admin portal > App Configuration table as having been correctly applied, and instead the field is blank.
- **VSP-64191:** The Lightweight Directory Access Protocol (LDAP) Sync function cannot import more than 1000 organizational unit (OU) objects. The LDAP server allows only 1000 entries per search request. This value is controlled by the LDAP server attribute MaxPageSize. As a result, sometimes not all OU objects will display on the LDAP management page.
Workaround: Configure the LDAP server attribute MaxPageSize to a value higher than 1000 OUs.

Limitations

For limitations found in previous releases, see the "Limitations" section in the release notes for those releases.

This release does not include any new third-party limitations.

Upgrade information

Use the information in this section for upgrade information specific to this release. 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.

- [Upgrade information](#)
- [Check disk space availability](#)
- [Core upgrade paths](#)
- [Core upgrade URL](#)
- [Backing up Core](#)
- [Upgrade information](#)

Before you begin

Read [Before you upgrade](#) .

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 1. PRE-UPGRADE CHECKLIST


| Check | Tasks | References |
|-------|-----------------------------------|--|
| | Prepare and plan for downtime | <ul style="list-style-type: none"> • Core (1 - 3 hours) • Sentry (5 - 20 minutes) |
| | Review relevant documentation | See Core product documentation. |
| | Check certificates | <ul style="list-style-type: none"> • iOS Enrollment, Portal HTTPS, Client TLS certificates <hr/> <p> 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 <i>Core Device Management Guide for iOS and macOS Devices</i>.</p> <hr/> <ul style="list-style-type: none"> • MDM Certificate (check a month before expires) • Local CA <p>Knowledge Base article: Renewing an expired local CA certificate.</p> |
| | Check Boot partition | <p>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.</p> <p>Knowledge Base article: Core Upgrade: Increase Boot Partition to 1GM if Avail Space is less than 35MB.</p> |
| | Ensure there is enough disk space | <ul style="list-style-type: none"> • Old File System (2 GB /mi and 5 GB /mi/files) • New File System (10 GB /mi) <p>Knowledge Base article: Resizing Disk Partition of a Core Virtual Machine.</p> |
| | Check for new system requirements | <ul style="list-style-type: none"> • Minimum 80 GB hard drive • If there is insufficient storage, increase the available disk space using the procedure outlined in Resizing Disk Partition of a Core Virtual Machine • Call Ivanti support if issues persist when physical appliances and VMs have the minimum required disk space configured • Port 8443 for Summary MICS - Configuration Service (that is, the service that supports System Manager.) |

TABLE 1. PRE-UPGRADE CHECKLIST (CONT.)

| Check | Tasks | References |
|-------|--|--|
| | Review your backup and high availability options | <ul style="list-style-type: none"> Physical backup: built in backup, showtech all VMware backup: VDMK backup, snapshot High Availability: confirm HA version 2.0 <p>Knowledge Base article: How to tell if your Core has HA 2.0 If using HA 1.0, contact Ivanti Professional Services to upgrade to 2.0.</p> |
| | Set up your proxy configuration (if required) | Manually set the upgrade URL and use HTTP instead of HTTPS. |
| | Prepare test devices | <ul style="list-style-type: none"> 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 2. 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 | <ul style="list-style-type: none"> Download vs. Stage for install Reboot when the system displays: Reboot to install <code>https://<serverFQDN>:8443/upgrade/status</code> |
| | Leverage CLI upgrade commands (as appropriate) | See <i>Core Command Line Interface (CLI) Reference</i> |
| | Understand scenario options | <ul style="list-style-type: none"> Single server High availability: <ul style="list-style-type: none"> 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 |

TABLE 2. UPGRADE CONSIDERATIONS (CONT.)

| Check | Considerations | References |
|-------|-----------------------------------|--|
| | | <p>Download guide: <i>Core High Availability Management Guide</i></p> <p>Review section: HA Core Software Upgrade Procedures</p> |
| | Monitor the upgrade | <ul style="list-style-type: none"> Log into the Admin Portal Select Logs > MDM Logs > States > Waiting XML generation pending Monitor upgrade status using: <code>https://<serverFQDN>:8443/upgrade/status</code> |
| | 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 | <p>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.</p> <p>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</p> |
| | 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 3. POST-UPGRADE CHECKLIST

| Check | Tasks | References |
|-------|-----------------------------|--|
| | Testing and troubleshooting | <ul style="list-style-type: none"> • 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 Ivanti Support for further investigation |
| | Verify services | <ul style="list-style-type: none"> • Log into the Admin Portal • Select Services > Overview • Click Verify All |
| | Verify devices | <ul style="list-style-type: none"> • Register a new device • Re-enroll/check-in existing devices |
| | HA system cleanup | <ul style="list-style-type: none"> • 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 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.

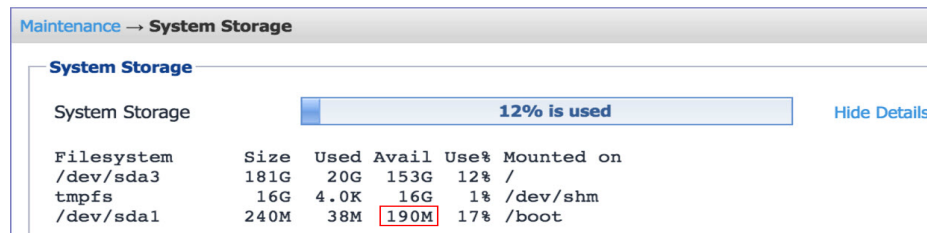
```
CORE(8.5.0.1a-6)@host.company.com#show system disk
Filesystem Size Used Avail Use% Mounted on
/dev/sda3 181G 20G 153G 12% /
tmpfs 16G 4.0K 16G 1% /dev/shm
/dev/sda1 95M 76M 15M 84% /boot
```

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.



Maintenance → System Storage

System Storage

System Storage 12% is used [Hide Details](#)

| 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.

Supported upgrade paths to Core 11.2.0.0

- 11.1.0.0 → 11.2.0.0
- 11.0.0.1 → 11.2.0.0
- 11.0.0.0 → 11.2.0.0
- 11.2.0.0 (GMRC) → 11.2.0.0

Core upgrade URL

To upgrade Core:

Use the following URL if you specify an alternate URL:

<https://support.mobileiron.com/mi/vsp/11.2.0.0-31/mobileiron-111.2.0.0-31>

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

Use the information in this section for upgrade information specific to this release.

- [About Enterprise Connector upgrade](#)
- [Enterprise Connector upgrade paths](#)
- [Enterprise Connector upgrade URL](#)
- [Enterprise Connector upgrade notes](#)

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 detailed in the *On-Premise Installation Guide*.

Enterprise Connector upgrade paths

Direct upgrade from only the following Enterprise Connector versions to version 11.2.0.0 is supported:

Supported upgrade paths to 11.2.0.0

- 11.1.0.0 → 11.2.0.0
- 11.0.0.1 → 11.2.0.0
- 11.0.0.0 → 11.2.0.0
- 11.2.0.0 (GMRC) → 11.2.0.0

If you are upgrading from a version not listed here, then you need to complete one or more previous upgrades first. See the upgrade guide for that version.

Enterprise Connector upgrade URL

Use the following URL if you specify an alternate URL:

Upgrades from supported Connector releases:

<https://support.mobileiron.com/mi/connector/11.2.0.0-31/mobileiron-11.2.0.0-31>

Enterprise Connector upgrade notes

There are no Enterprise Connector upgrade notes for this release.

Documentation resources

Product documentation is available on the [Ivanti documentation website](#).

To access documentation, navigate to a specific product and click the > symbol next to the name to view all documents in that product category.

Current release documentation is available in the main section. For prior versions, navigate to the **ARCHIVED DOCUMENTATION** section at the bottom of the page.

Core documentation

The following is a list of the documentation:

- *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*

Everything you need know about setting up and managing devices on Core. The guide is available in the following flavors, one for each of these device platforms:

- Android, including Android Enterprise and Samsung Knox
- iOS, including macOS
- Windows, including Windows 10

Information about Sentry and AppTunnel and ActiveSync, AppConnect, and 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.

- *Event Notification Service and Common Platform Services API Guide*

Describes how to use the Event Notification Service and Common Platform Services (CPS) API with Cloud 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.