



Getting Started with Core 11.4.0.0 - 11.7.0.0

July 2022

Revised: August 2022

For complete product documentation, see:

[Ivanti Documentation Home Page](#)

Contents

Revision history	4
New features summary	5
Related information from previous releases	6
Introduction to Core	7
Core overview	7
What can you do with Core?	8
Core components	8
Documentation resources	10
Prerequisites for using this guide	12
Getting Started Using Core	13
Logging in to the Admin Portal with user name and password	13
Logging in to the Admin Portal with a smart card	14
Setup tasks	15
Admin Portal workspace	33
Ivanti Community - Submitting Ideas	38
Managing Users	40
User management overview	40
Accessing the user management page	43
Configuring LDAP servers	43
Managing LDAP users	49
Managing local users in the Admin Portal	64
Managing Devices	79
Devices & Users pages	80
Understanding the Registration page	81
Displaying device assets	84
Single device registration	93
Bulk device registration	97
Tracking registration status	105
Restricting the number of devices a user registers	105
Restricting device registration by enrollment type	106
Using bulk enrollment for Android devices	106
Registration considerations	109
Using Policies	116
Policy overview	117
Working with policies	118
Using default policies	124
Managing Labels	190
Apply to Label	191
Device label search	192
Using search for device labels	192
Remove from label	193
Applying a device to a label	193

Removing a device from label	194
Using labels to establish groups	194
Using search for device labels	195
Notifying all device users using labels	196
Default labels	197
Filter and manual type labels	199
Editing Labels	201
Copying a label to a new label	203
Viewing devices currently associated with a label	203
Associating a filter with a label	204
Searching for device labels	205
Calculating devices impacted by changing or removing labels	207
Creating a label based on custom LDAP user attributes	210
Using the Dashboard	211
Dashboard overview	211
Dashboard charts	211
Arranging the devices dashboard charts	214
Changing the charts included in the dashboard	214
Devices associated with chart sections in the devices dashboard	214
Displaying device lists from devices dashboard charts	215
Adding an app chart to the apps dashboard	217

Revision history

For the complete revision history, see the [online version](#) of this document.



New features summary

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

- **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" on page 81](#).
- **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 admin user - you first need to remove the admin 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" on page 68](#).

- **Support for Private DNS:** On fully-managed devices running Android 10 or later, the admin 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" on page 163](#).
- **macOS and Windows registration configurations enabled upon upgrade:** For new Core deployments, Ivanti's support for macOS and Windows device management is available in Core, Ivanti EPM, and Ivanti Neurons for MDM.

- **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, when the Mobile@Work auto-grant location permission check box is selected, admins 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. End user consent is required for Mobile@Work to have phone permission.

For more information, see ["Privacy policies" on page 144](#) and ["Understanding the Registration page" on page 81](#).

Related information from previous releases

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

- [Core 11.6.0.0 New features summary](#)
- [Core 11.5.0.0 New features summary](#)
- [Core 11.4.0.0 New features summary](#)



Introduction to Core

The topics in this chapter include:

- [Core overview](#)
- [What can you do with Core?](#)
- [Core components](#)
- ["Documentation resources" on page 10](#)
- [Prerequisites for using this guide](#)

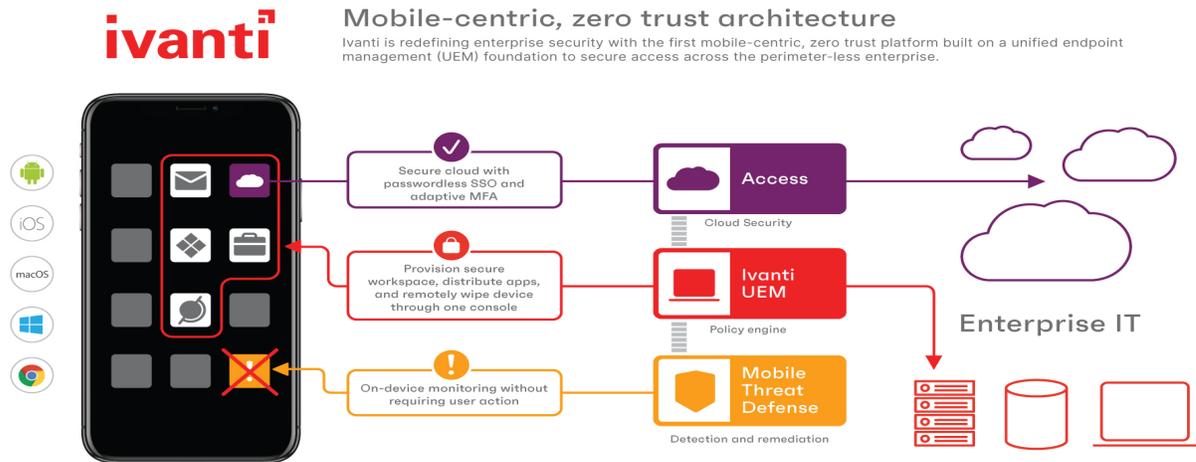
Core overview

Core brings together comprehensive security and Unified Endpoint Management (UEM) tools including:

- Mobile Device Management (MDM)
- Mobile Application Management (MAM)
- Mobile Content Management (MCM)

With Core, you can securely manage the lifecycle of mobile devices and mobile applications, from registering a device with Core, to retiring the device from Core management. When using a Core managed device, device users can securely access corporate data, email, and mobile apps that you control and distribute using Core.

FIGURE 1. CORE PRODUCT OVERVIEW



What can you do with Core?

Core allows you to:

- Connect to backend services such as LDAP and leverage LDAP users for use in Core.
- Register both company- and employee-owned devices to be managed by Core.
- Configure and push to devices policies and settings such as VPN settings and security policies.
- Securely synchronize data from backend systems such as corporate email.
- Distribute, install, and manage both publicly available and in-house mobile apps.
- Leverage existing platform-specific mobile device management protocols, such as iOS MDM.
- Configure and push certificates to devices.
- Configure and enforce compliance rules to handle compromised or stolen devices.

Core components

The main components of Core include:

- ["Admin Portal" on the next page](#)
- ["System Manager" on the next page](#)
- ["Enterprise Connector" on the next page](#)
- ["CLI" on the next page](#)
- ["APIs" on the next page](#)

Admin Portal

The Admin Portal is a web-based administrator portal you use to configure, manage, maintain, and troubleshoot users, devices, apps, policies, settings, and labels. The Admin Portal is where you register devices, distribute apps, configure and push policies to devices, and view the status of your fleet of managed devices at a glance. This getting started guide focuses on the Admin Portal, as this is where the majority of setup occurs.

After you have used this guide to get started, refer to the *Core Device Management Guide* for each operating system (Android, iOS, Windows) for more advanced device management topics.

System Manager

The System Manager is used to configure Core, manage network settings, manage Core within your infrastructure, upgrade Core, troubleshoot and maintain Core itself. For more information about the System Manager, refer to the *Core System Manager Guide*.

Enterprise Connector

The Enterprise Connector is a component that connects Core to corporate directories, such as Microsoft Active Directory or LDAP, by means of secure HTTPS connections. Multiple connectors can be used for scaling and redundancy purposes. For more information about the Enterprise Connector, refer to the *On-Premise Installation Guide for MobileIron Core and Enterprise Connector*.

CLI

The CLI, or Command Line Interface, allows you to access certain Core and System Manager functions from the command line in a terminal window. For more information about using the CLI, refer to the *Core Command Line Interface (CLI) Reference*.

APIs

Core supports a number of application program interfaces (APIs) described in the following guides:

- *V1 API Reference Guide for Core Webservice*
- *Core V2 API Guide*
- *Common Platform Services (CPS) Guide*

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](#), and [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 Ivanti Sentry, Ivanti Tunnel, ActiveSync, Ivanti AppConnect, Ivanti 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.

Prerequisites for using this guide

All steps and procedures in this document assume you have successfully installed Core. If not, go to the *On-Premise Installation Guide for Core and Enterprise Connector* and complete the installation process before using this guide.



Make sure you have configured networks and ports, as described in the *On-Premise Installation Guide for MobileIron Core and Enterprise Connector*. If you did not configure networks and ports during installation, you must do so in the System Manager. For more information, see “Access Control Lists: Networks and Hosts” in the *Core System Manager Guide*.



Getting Started Using Core

The topics in this chapter include:

- [Core administrator tools overview](#)
- [Logging in to the Admin Portal with user name and password](#)
- [Logging in to the Admin Portal with a smart card](#)
- [Admin Portal workspace](#)
- [Ivanti Community - Submitting Ideas](#)
- [Setup tasks](#)

Logging in to the Admin Portal with user name and password

The Admin Portal is installed as part of the system setup. Log in to the Admin Portal to manage users, devices, apps, and configurations, settings, and policies.

Refer to the *On-Premise Installation Guide for Core and Enterprise Connector* for installation details.

If supported by your system administrator, you can login to the Admin Portal with a user name and password. Refer to the *Core System Manager Guide* for information on setting up this authentication method.

About authentication settings

- If you enter the wrong password five consecutive times, the user ID you entered will be locked out temporarily. Wait 30 seconds and try again.
- You can configure the time period before auto-lock by selecting **Settings > Security > Password policy > Auto-Lock Time**. The default period is 5 minutes.
- You can configure the number of incorrect consecutive passwords entered before Core lock the user name by selecting **Settings > Security > Password policy > Number of failed attempts**. The default number is 5.

Procedure

1. Open a supported browser.

Refer to the latest release notes for information on supported and compatible browsers.

2. Enter the URL for the Admin Portal, for example:

```
https://<fully_qualified_hostname>/mifs
```

3. Enter the user ID and password.

The user associated with the credentials you enter must have one or more roles that provide access to Admin Portal actions. The ID and password are case sensitive.



The Super Administrator created during installation is automatically assigned several roles that enable Admin Portal actions.

4. Click **SIGN IN**.

Related topics

[Logging in to the Admin Portal with a smart card](#)

Logging in to the Admin Portal with a smart card

The Admin Portal is installed as part of the system setup. Log in to the Admin Portal to manage users, devices, apps, and configurations, settings, and policies.

Refer to the *On-Premise Installation Guide for Core and Enterprise Connector* for installation details.

If supported by your system administrator, you can login to the Admin Portal on a desktop computer using an identity certificate on a smart card. Refer to the *Core System Manager Guide* for information on setting up this authentication method.



This authentication method is supported only on desktop computers. It is not supported on mobile devices. Also, it is not supported with Firefox.

Procedure

1. Attach your smart card reader with your smart card to a USB port on the desktop computer.

If your computer has a built-in smart card reader, insert your smart card.

2. Go to the URL of the Admin Portal at https://<fully_qualified_hostname>/mifs.
3. If you are not logged in, select **Sign In With Certificate**.

A prompt appears to select your certificate.
4. Select the certificate from the smart card.
5. If prompted, enter the password of the private key of the identity certificate on your smart card. The Admin Portal displays.

Related topics

[Logging in to the Admin Portal with user name and password](#)

Setup tasks

This section includes the following setup tasks:

- [Setting the enterprise name](#)
- [Setting the external hostname](#)
- [Setting the idle timeout for the Admin Portal and user portal](#)
- [Setting the EULA or other login text](#)
- [Enabling last login information display](#)
- [Enabling Notes for Audit Logs](#)
- [Trusted certificates management](#)
- [Uploading your MDM certificate](#)
- [Enabling iOS MDM support](#)
- [Requesting an MDM certificate](#)
- [Confirming MDM for a macOS or iOS device](#)
- [Denying check-Ins for devices having expired MDM certificates](#)
- [Displaying a report of devices having expired MDM certificates](#)
- ["Setting a System Event to be notified about certificate expiration " on page 31](#)
- ["Renewing your MDM certificate " on page 31](#)

Setting the enterprise name

The company name entered during Core installation is used as the default enterprise name identifying your organization in email, SMSes, alerts, and certificates. If the company name you entered is not the one you want to use in these contexts, you can change the name.



Be sure to set the enterprise name before you upload certificates, or you may impact all registered devices.

Procedure

1. Log into the Admin Portal.
2. Go to **Settings > System Settings > General > Enterprise**.
3. In the **Enterprise Name** field, enter the text to use when referring to the enterprise.
4. Click **Save**.

Setting the external hostname

The external hostname is set during installation. It is used in the registration URL sent to users for completing the registration process. It is also used in self-signed certificates.

Impact: Changing this field requires the following:

- Regeneration of any self-signed certificates or uploading matching portal-HTTPS and client-TLS certificates
- Rebooting the appliance

Procedure

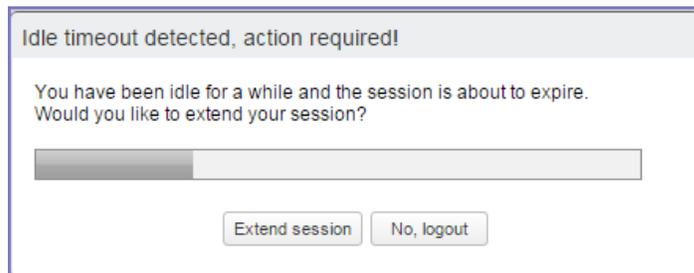
1. Log into the Admin Portal.
2. Go to **Settings > System Settings > General > Enterprise**.
3. In the **External Host** field, enter the fully-qualified domain name to be used for accessing MobileIron.
4. Click **Save**.

Setting the idle timeout for the Admin Portal and user portal

Based on your security requirements, you can decide how much idle time is allowed before an administrator or user is automatically logged out of the Admin Portal or self-service user portal. You configure the idle session timeout in the Admin Portal at **Settings > System Settings > General > Timeout**. You can choose an idle timeout between 5 and 90 minutes.

A pop-up warns the administrator or user about the impending timeout a few minutes before the configured idle time elapses.

FIGURE 1. IDLE TIME OUT WINDOW



When the time elapses, the administrator or user is logged out. If the administrator or user clicks **Extend session**, the timer is reset.



Changing the idle timeout impacts all future logins. It does not impact your current session.

Setting the idle timeout for CLI and SSH sessions

You can set the idle timeout for command line interface (CLI) and secure shell (SSH) sessions in Core System Manager.

For details, refer to “System Settings” in the *Core System Manager Guide*.

Warning period details

The pop-up that warns that the administrator or user will be logged out precedes the timeout as follows:

TABLE 1. ADD VLAN FIELDS

Configured idle timeout	Pop-up warning appearance
5 to 35 minutes	3 minutes before timeout
40 or 45 minutes	4 minutes before timeout
50 or 55 minutes	5 minutes before timeout
60 or 65 minutes	6 minutes before timeout
70 or 75 minutes	7 minutes before timeout
80 or 85 minutes	8 minutes before timeout
90 minutes	9 minutes before timeout

Setting the EULA or other login text

You can configure Core to display an End User License Agreement (EULA) or any other text on the following user interfaces:

- Admin Portal login screen
- System Manager login screen
- A CLI session
- The Self-service user portal login screen

Procedure

1. In the Admin Portal, go to **Settings > System Settings > General > Login**.
2. Select **Enable Login Text Box**.
3. In **Text To Display**, enter the text.



Core treats the text as plain characters. It does not recognize, for example, HTML tags. The text must be ASCII only; no multi-byte characters are allowed.

4. Click **Save**.

The Admin Portal and the System Manager display this text the next time a user logs in.



The Core CLI command banner, available in CLI CONFIG mode, also sets this text.

To disable this setting:

1. In the Admin Portal, go to **Settings > System Settings > General > Login**.
2. Uncheck **Enable Login Text Box**.

The text you had entered in **Text To Display** is grayed out.

3. Click **Save**.

The login screens and CLI session do not show the text the next time a user logs in.

Enabling last login information display

You can enable a setting to show the current Admin Portal user some login information about the last login to the Admin Portal. This information provides you security insight about Admin Portal use. The information displays when you click on the user icon at the top right of the screen. An example of the information is:

```
Last login was 3/11/2014 1:28:52 PM from 171.15.10.221
```

The information includes:

- the date of the last login
- the time of the last login
- the IP address of the computer that was used for the last login

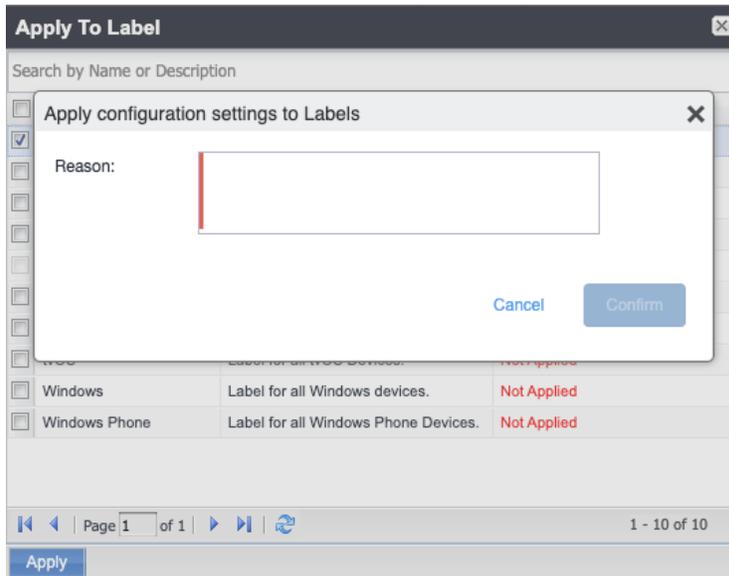
To configure this setting:

1. In the Admin Portal, go to **Settings > System Settings > General > Login**.
2. Select **Always Show Last Login**.
3. Click **Save**.

The Admin Portal displays the last login information the next time a user logs in.

Enabling Notes for Audit Logs

As a best practice, we recommend enabling Notes for Audit Logs. This is used for tracking changes to labels made by administrators. By default, this feature is disabled. When enabled, administrators will be prompted with a text box similar to the one below.



For example, an administrator can enter a change ticket order number, thus allowing for automated monitoring of the Core environment. This information is then displayed in the Audit logs, in the Details column as "Reason."

Dashboard Devices & Users Admin Apps Policies & Configs Services Settings Logs							
Audit Logs MDM Activity Certificate Management Event Settings Events							
Export to CSV							
	ACTION	STATE	PERFORMED BY	ACTION DATE	COMPLETED AT	PERFORMED ON	DETAILS
	Apply Label To Configu...	Success	miadmin	2020-01-20 03:52:39...	2020-01-20 03:52:39...	Restrictions - iOSRestriction : V...	Label All-Smartphones applied to configuration iO...
	Preference Config Cha...	Success	misystem	2020-01-20 03:49:04...	2020-01-20 03:49:04...	System	Label All-Smartphones applied to configuration iOSRestriction. Reason: AddLabel
	Modify Configuration	Success	miadmin	2020-01-20 03:48:22...	2020-01-20 03:48:22...	Restrictions - iOSRestriction : V...	Configuration iOSRestriction modified
	Admin Portal Sign In	Success	miadmin	2020-01-20 03:46:26...	2020-01-20 03:46:26...	Admin Portal - 管理端	Successfully Signed In

Notes for Audit Logs is applicable for the following label-related activities:

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

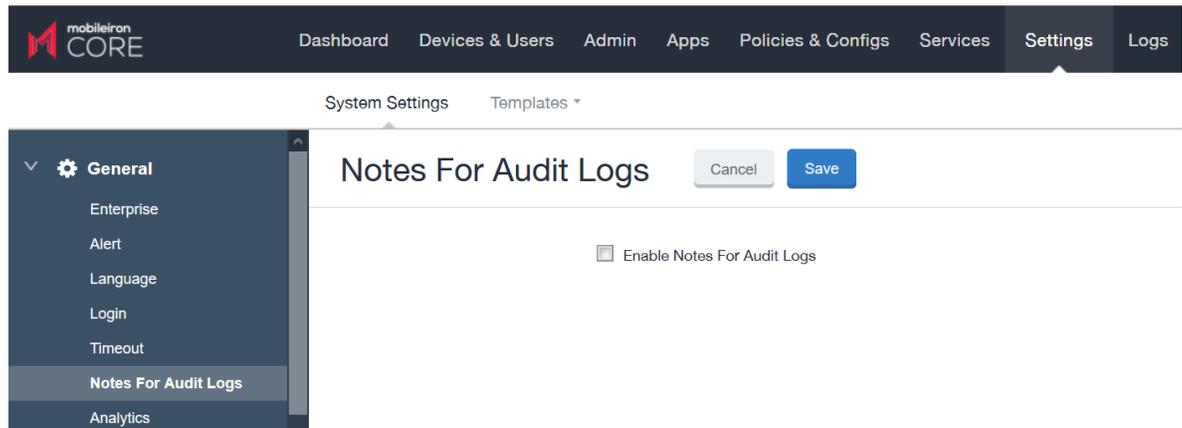
- Add/Edit/Remove Label to policies
- Add/Edit/Remove Label to apps
- Add/Edit/Remove Label to iBooks

Using this feature, you can also track administrator-made changes to iOS and macOS restrictions. Whenever an administrator adds, edits or deletes iOS and macOS restriction(s), a text dialog box displays for the administrator to enter a reason for the change. For more information about restrictions, see the *Core Device Management Guide for iOS and macOS Devices*.

Procedure

To set the tracking of changes made by administrators:

1. Go to **Settings > System Settings**.
2. In the left pane, click **General > Notes for Audit Logs**. The Notes for Audit Logs page displays.



3. Select **Enable Notes for Audit Logs** and then click **Save**.

Trusted certificates management

Core uses TLS/SSL to secure incoming and outgoing connections to outside entities, such as servers, clients, and Sentry. Clients connecting to a server over TLS/SSL are required to verify the server certificate chain obtained during the TLS/SSL handshake. To ensure these connections are secure, Core verifies the certificate chain and server hostname, and checks the certificate against the Certification Revocation List (CRL).

The Trusted Certificates feature provides administrators with the ability to:

- **Check the CRL:** This ensures that verification information is current by checking certificates (trusted and new) against obtained CRLs. Certificate validity periods are checked against the current time provided by the verifier's system clock.
- **Verify signatures:** These are verified using the public key in the issuer's certificates.
- **Verify the certificate chain:** This ensures the certificate chain is well-formed, valid, properly signed, and trustworthy. Certificate chain verification stops at trusted anchor certificate stored by MobileIron.
- **Verify server hostname:** This verifies the server's hostname against names included in server certificate.

The trusted certificate feature has the following settings:

- **Allow only TLS/SSL connections certified by trusted CAs:** This setting provides the highest level of security using the TLS/SSL protocol. Administrators manually enable the configuration of trusted certificates with additional preferences for server hostname verification and revocation status validation based on the Certification Revocation List (CRL).
- **Allow all TLS/SSL connections and register certifying CAs as trusted:** This setting adds all connections to the **Show Trusted Certs** table. This action creates a migration path where administrators can review details of each certificate and manually turn on TLS/SSL over time.
- **Allow all TLS/SSL connections:** This is the default setting and allows all outgoing connections after verifying the Issuer, Subject, Signature, and Validity status.

Configuring trusted certificate settings

Core allows you to configure any of the following trusted certificate settings:

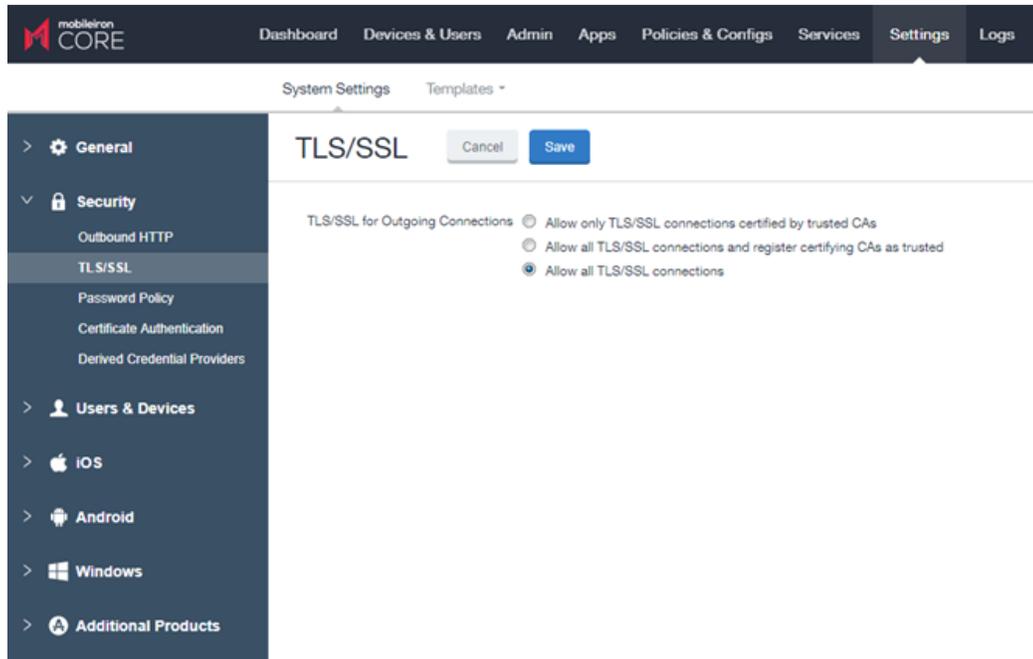
- **Allow only TLS/SSL connections certified by trusted CAs.** This setting allows administrators to manually configure trusted certificates and allows them to disable the server hostname and revocation status verification. Revocation status validation is based on Certification Revocation List (CRL) that are automatically downloaded and verified. The CRL grace period is configurable with a default value of 30 minutes.
- **Allow all TLS/SSL connections and register certifying CAs as trusted.** This setting automatically adds all required certificates to the trusted certificate table available for review in the Admin Portal. This allows administrators to turn on TLS/SSL instantly.
- **Allow all TLS/SSL connections.** This setting allows all outgoing connections, providing basic certificate chain verification including certificate names, signatures, and validity.



Switching among these TLS/SSL settings requires you to restart Core for your changes to take effect.

Procedure

1. From the Admin Portal, go to **Settings > System Settings > Security > TLS/SSL** to open the trusted certificate settings window.



2. Select one of the following settings.
 - a. **Allow only TLS/SSL connections certified by trusted CAs.** This setting allows administrators to manually configure trusted certificates and allows them to disable the server hostname and revocation status verification. Revocation status validation is based on Certification Revocation List (CRL) that are automatically downloaded and verified. The CRL grace period is configurable with a default value of 30 minutes.
 - b. **Allow all TLS/SSL connections and register certifying CAs as trusted.** This setting automatically adds all required certificates to the trusted certificate table available for review in the Admin Portal. This allows administrators to turn on TLS/SSL instantly.
 - c. **Allow all TLS/SSL connections.** This setting allows all outgoing connections, providing basic certificate chain verification including certificate names, signatures, and validity.
3. Click **Save**.

Managing trusted certificates

Depending on how trusted certificates are configured, Core adds trusted and untrusted root certificates to the Admin Portal. The procedures in this section describe how to manage the information in these tables.

This section contains the following procedures:

- Delete a certificate.
- Trust an untrusted certificate.
- Add a trusted certificate.
- View certificate details.

To delete a certificate:

1. From the Admin Portal, go to **Services > Trusted Root Certificates**.
2. Click the drop down box to the right and select one of the following options:
 - a. Show Trusted Certs
 - b. Show Untrusted Certs
3. Select one or more certificates.

4. Select **Actions > Delete**.
5. Click **Yes** in the confirmation box.

IMPORTANT: You must restart the server to complete the process of deleting the selected trusted certificates.

To trust an untrusted certificate:

- Log into the Admin Portal and select **Services > Trusted Root Certificates**.
- Click the drop down box and select **Show Untrusted Certs**.
- Click the **View Certificate** link for the certificate you want to trust.

You can select only one certificate at a time to allow you to review each certificate individually.

- Review the certificate information and click **Close** when you have completed the review.
- Select **Actions > Trust**.
- Review the trust certificate.
- Click **Trust** if you want to continue or **Cancel**.

To add a trusted certificate:

- Log into the Admin Portal and select **Services > Trusted Root Certificates**.
- Click the drop down box and select **Show Trusted Certs**.
- Click the **Add+** button to open the **Upload Trust Root Certificate** dialog.
- Add the certificate to the **File** box using the **Browse** button.
- Click **Upload Certificate** to add it to the list of trusted certificates.
- Click **OK**.

To view certificate details:

1. Log into the Admin Portal and select **Services > Trusted Root Certificates**.
2. Click the drop down box to the right and select one of the following options:
 - a. Show Trusted Certs
 - b. Show Untrusted Certs
3. Click the **View Certificate** link for a single certificate.
4. View the certificate details, then click **Close**.

Importing untrusted certificates

Core fails to connect to a service if both of the following are true:

- On **Settings > Security > TLS/SSL**, you have selected **Allow only TLS/SSL connections certified by trusted CAs**.
- Core does not trust at least one Certificate Authority (CA) in the certificate chain that the service presents to Core.

This failure can occur for:

- Services listed on **Services > Overview**.
- Additional services you use, such certificate providers configured in certificate enrollment settings.

On a new Core installation, to simplify the process to trust the services listed on **Services > Overview**, Ivanti recommends the following procedure:

Procedure

1. On **Settings > Security > TLS/SSL**, select **Allow all TLS/SSL connections and register certifying CAs as trusted**.
2. Verify your connections with the backend services by selecting **Verify All** in **Services > Overview**.
Core imports the certificate chains, which will now appear in **Services > Trusted Root Certificates**.
3. On **Settings > Security > TLS/SSL**, select **Allow only TLS/SSL connections certified by trusted CAs**.
4. To trust additional certificates, follow the procedure in [Managing trusted certificates](#).

Managing Mobile Device Management (MDM) certificates for iOS and macOS

This section includes the following topics:

- [" Requesting an MDM certificate " below](#)
- [" Uploading your MDM certificate " on the next page](#)
- ["Enabling iOS MDM support " on page 29](#)
- ["Confirming MDM for a macOS or iOS device" on page 30](#)
- ["Denying check-Ins for devices having expired MDM certificates " on page 30](#)
- ["Displaying a report of devices having expired MDM certificates " on page 30](#)

If you are using only MAM-only iOS devices, skip these MDM-related sections. For more information, see "Managing apps on MAM-only devices" in the *Core Apps@Work Guide*.

Requesting an MDM certificate

You can request an MDM certificate from Apple.

Before you begin

When using the option **Allow only TLS/SSL connections certified by trusted CAs** as selected in ["Configuring trusted certificate settings" on page 22](#), make sure that all certificates listed in **Services > Trusted Root Certificates** are trusted. To trust certificates, see ["Managing trusted certificates" on page 24](#).

Procedure

1. Log into the Admin Portal and select **Settings > System Settings**.
2. Select **iOS > MDM**.
3. Select the Enable MDM Profile option.
4. Click **Install MDM Certificate**.

The **MDM Certificate Generation** window displays.

5. Click **Download Certificate Signing Request**.

If an empty text file downloads, see the steps in **Before you begin**. Otherwise, this step generates the required property list in Apple's .PLIST XML format. This may take a few minutes.

6. Select a location for the plist when prompted.

The downloaded file is `req-plist.txt`.

7. Click the **Apple Push Certificates Portal** link to start the process of requesting the MDM certificate.
8. When you receive the MDM certificate from Apple, click **Upload MDM Certificate**. The Upload MDM Certificate dialog appears.
9. Click
10. Click **Upload Certificate**.

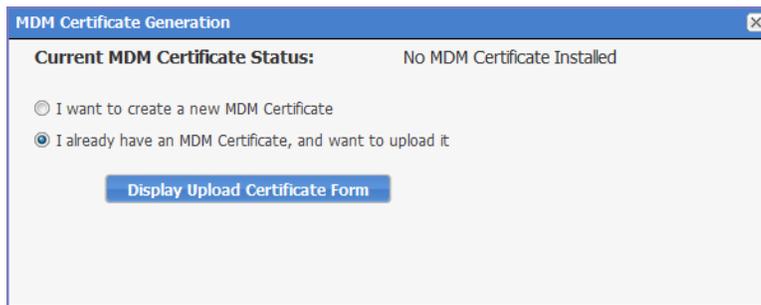
Uploading your MDM certificate

If you have already requested and received your MDM certificate from Apple, you can upload the certificate using the following steps:

Procedure

1. Log into the Admin Portal.
2. Go to **Settings > System Settings**.
3. Select **iOS > MDM**.
4. Select the **Enable MDM Profile** option.
5. Click **Install MDM Certificate** to open the **MDM Certificate Generation** dialog.

6. Select **I already have an MDM Certificate, and want to upload it**.



7. Click **Display Upload Certificate Form** to open the **Upload MDM Certificate** dialog.
8. Click **Choose File** to select the MDM certificate.
9. Click **Upload Certificate**.

Enabling iOS MDM support

Once you have completed all steps required by Apple, you can enable iOS MDM support in MobileIron. See the following source for information on Apple's current program:

<http://www.apple.com/ipad/business/integration/mdm/>

Core uses Apple's enhanced MDM certificate infrastructure to streamline the process of acquiring and uploading an MDM certificate. You can now complete the following tasks from a single screen within the Admin Portal:

- generate a Certificate Signing Request (CSR)
- upload the CSR
- access the Apple Push Certificates Portal to request a certificate
- upload the MDM certificate

If you already have an MDM certificate, but have not uploaded it, you can upload it from the same screen.

If you enabled iOS MDM support in a previous Core release, then you should not use the enhanced certificate infrastructure at this time unless otherwise instructed by Apple or MobileIron. Doing so will disable your current certificates for all registered Mac iOS devices.



If you intend to develop in-house apps for distribution, then you still need to participate in Apple Device Enrollment. For more information about participating in Apple Device Enrollment, see “Managing Devices Enrolled in the Apple Device Enrollment Program” in the *Core Device Management Guide for iOS and macOS Devices*

Confirming MDM for a macOS or iOS device

To confirm that MDM is operational for a macOS or an iOS device:

Procedure

1. Log into the Admin Portal and select **Device & Users > Devices**.
2. Select any iOS device and click the up arrow to expand the device details.
3. In the **Device Details** tab, confirm that the **MDM Operational** flag value is **Yes**.

Denying check-Ins for devices having expired MDM certificates

By default, Core allows macOS and iOS devices with expired MDM certificates to check in. You can, however, configure Core to deny check-ins to these devices.

Procedure

1. Log into the Admin Portal and select **Settings > System Settings**.
2. Select **iOS > MDM**.
3. In the **MDM Preferences** section, clear the **Permit expired client certificate** option.
4. Click **Save**.

Displaying a report of devices having expired MDM certificates

You can save to a CSV file a list of the iOS or macOS devices with expired MDM certificates.

Procedure

1. Log into the Admin Portal and select **Settings > System Settings**.
2. Select **iOS > MDM**.

3. Click **Download Expired MDM Certificate Devices Report** .
4. Open or save the resulting CSV file.

Setting a System Event to be notified about certificate expiration

You can be notified of the pending expiration of your iOS MDM certificate 30 days before its expiry.

Procedure

1. Log into the Admin Portal and select **Logs > Event Settings**.
2. Click **Add New > System Event**.
3. Enter a name for the System Event.
4. Make sure **Certificate Expired** is selected. Select other options according to your requirements.
5. In the **Send Alerts** section, under **Apply to Labels**, do **not** select a label.
6. In the **Search Users** field, enter the user ID of an administrator who has a device registered on Core.
7. Select the administrator in the **Apply to Users** list.
8. Click the right arrow to move the administrator to the **Selected** list.
9. Click **Save**.

Related topics

"System event settings" in the *Core Device Management Guide for iOS and macOS Devices*.

Renewing your MDM certificate

Renew your MDM certificate before it expires. This procedure uses the Core Admin Portal and the Apple Push Certificates Portal. You need the Apple ID that was originally used to create the MDM certificate. If you don't know what Apple ID to use, open a ticket with Apple Developer Program Support.

- Do not use Internet Explorer for this procedure.
- Apple might change the steps involving the Apple Push Certificates Portal.

Procedure

1. Log into the Core Admin Portal and select **Settings > System Settings**.
2. Select **iOS > MDM**.
3. Click **Install MDM Certificate**.
4. Click **Download Certificate Signing Request**.
5. Note to where the file is downloaded.
6. Click **Apple Push Certificates Portal**.
7. Log in to the Apple Push Certificates Portal using the same Apple ID that was used to create the certificate.
8. In the Apple Push Certificates Portal, you will see your MDM certificate.
9. Click **Renew**.
10. Click **Choose File** and find the txt file that you downloaded.
11. Click **Upload**.
12. When you see the confirmation screen, click **Download**.
The renewed certificate, a PEM file, downloads.
13. In the Core Admin Portal, in the **MDM Certificate Generation** screen, click **Upload MDM Certificate**.
14. Browse to the PEM file and click **Upload Certificate**.
A confirmation screen displays.
15. Click the **X** to close the confirmation screen.
16. Click **View Certificate** to note the new date and time on the certificate.

Related topics

[How To Identify a Matching MDM Cert in the Apple Push Certificate Portal](#)

Admin Portal workspace

The Admin Portal provides the following types of workspaces:

- **Dashboard:** the first page open each time you log into the Admin Portal gives you an at-a-glance view of the all managed devices.
- **Action menus:** includes all the top-level menus that help you manage devices.



Do not create bookmarks for Admin Portal pages. Session IDs are included in the bookmark and may cause connection problems. If you would like to create a bookmark for the Admin Portal, create one manually for the following URL: `https://<fully_qualified_hostname>/mifs`.

Dashboard workspace

Core opens the Dashboard each time you log into the Admin Portal. The Dashboard workspace has the following components (the numbers displayed in "Dashboard workspace" below correspond to the numbers listed in "Admin Portal menu items" on the next page).

FIGURE 1. DASHBOARD WORKSPACE

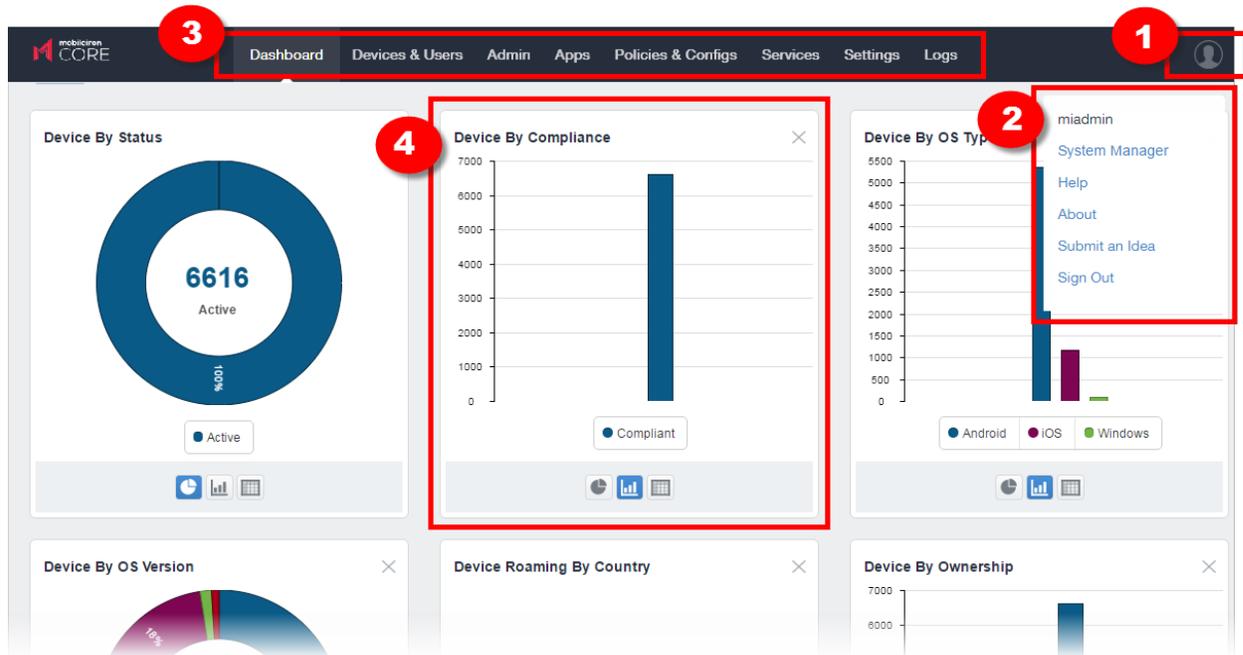


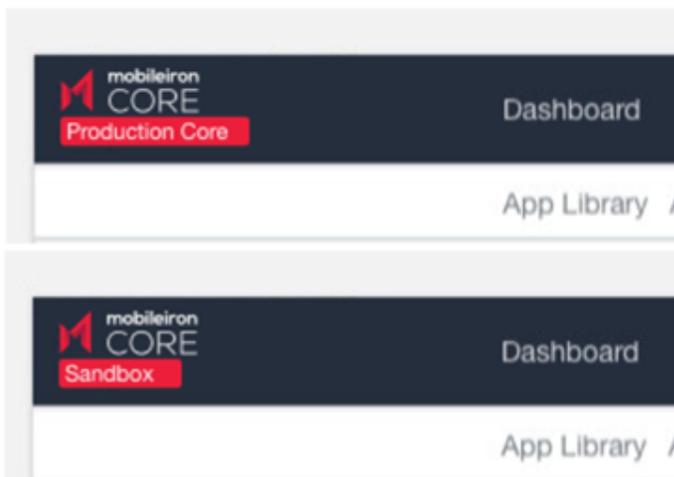
TABLE 2. ADMIN PORTAL MENU ITEMS

Number	Element	Description
1	User Icon	Opens the drop down Core information (2).
2	Core information	Displays: <ul style="list-style-type: none"> • Username logged into the Admin Portal (User1, for example). • System Manager links to System Manager. • Help links to the Core support website. • About provides Core version information. • Submit an Idea opens "Ivanti Community - Submitting Ideas" on page 38. • Sign Out logs you out of the Admin Portal.
3	Main menu	The main navigation menu options (Dashboard, Devices & Users, Admin, Apps, Policies & Configs, Services, Settings, Logs).
4	Dashboard widgets	One of the many device management widgets available on the Dashboard.

Creating a customizable banner

As a convenience, you can set your Core to indicate to IT administrators what environment they are in when logging to the Core user interface console, for example: Production, Sandbox or Dev. This is done with an editable field that takes up to 35 characters and displays in the top-left corner of the Admin portal, under the Core logo.

FIGURE 2. CUSTOMIZABLE BANNER



Administrators with "Manage settings and services" or "View settings and services" or "Manage custom attributes role" privileges have access to creating or editing this customized banner.

Procedure

1. Go to **Settings > System Settings**.
2. Under General, select Enterprise.
3. In the Deployment section, enter a name that will appear under the Core logo in the left corner of the Admin portal.
4. When finished, click **Save**.
5. Refresh your browser. The new name displays.

Action menu workspace

Click any of the top-level action menus (Devices & Users, Admin, Apps, Policies & Configs, Services, Settings, Logs) to expand the Admin Portal workspace to take action on managing Core. Action menu workspaces have the following components (the numbers displayed in the following image corresponds to the numbers listed in "[Action menu workspace items](#)" on the next page).

FIGURE 3. ACTION MENU WORKSPACE

N...	MODEL	MANUFACT...	PLATFORM ...	HOME COUNTRY...	STATUS	REGISTRATIO...	LAST CHEC...	OWNER	OPERATOR
	iPhone 4	Apple	iOS 8.0	United States	Active	2015-06-14 09:2...	52 m 22 s	Company	AT&T
	Lumia 920	NOKIA	Windows Ph...		Active	2015-06-14 09:2...	1 h 48 m	Company	
	DROIDX	motorola	Android 2.2	United States	Active	2015-06-14 09:2...	1 h 44 m	Company	T-Mobile
	Lumia 920	NOKIA	Windows Ph...		Active	2015-06-14 09:2...	1 h 48 m	Company	
	iPhone 4	Apple	iOS 8.0	United States	Active	2015-06-14 09:2...		Company	AT&T
	DROIDX	motorola	Android 2.2	United States	Active	2015-06-14 09:2...	1 h 45 m	Company	T-Mobile
	DROIDX	motorola	Android 2.2	United States	Active	2015-06-14 09:2...	1 h 43 m	Company	T-Mobile
	iPhone 4	Apple	iOS 8.0	United States	Active	2015-06-14 09:2...		Company	AT&T
	Lumia 920	NOKIA	Windows Ph...		Active	2015-06-14 09:2...	1 h 48 m	Company	

The following table describes the elements in the action menus of the Admin Portal.

TABLE 3. ACTION MENU WORKSPACE ITEMS

Number	Element	Description
1	Main menus	The top-level action menus (Devices & Users, Admin, Apps, Policies & Configs, Services, Settings, Logs).
2	Menu items	Displays the sub-level menu items for the main menu.
3	Page level task bar	Includes the set of actions you can take on each record displayed on the page.
4	User icon	The user icon logged into the Admin Portal.
5	Page	Displays all records for the menu.

Sub-level action menu items

The following table describes the secondary sub-level menu items for action menus in the Admin Portal.

TABLE 4. SUB-LEVEL MENU ITEMS

Action menu	Sub-level menu items	Actions
Devices & Users	Devices	Manage devices by adding, retiring, viewing details. You can also take actions such as lock, send messages, set custom attributes, add devices to labels.
	Users	Manage users by adding, deleting, viewing details. You can also take actions such as assign roles, set custom attributes, require password changes, delete
	Labels	Manage labels by adding, editing, viewing details.
	ActiveSync	Displays and registers devices accessing ActiveSync. This view is populated only if you have a Core Sentry configured.
	Apple DEP	Specifies an Apple Device Enrollment account for use with Core
Admin	Apple Education	Manage Apple School Manager devices using Core as the designated Mobile Device Management (MDM) server.
	Admins	Manage administrators by editing roles, assigning or removing from a space.
	Device Spaces	Create or manage device spaces.

TABLE 4. SUB-LEVEL MENU ITEMS (CONT.)

Action menu	Sub-level menu items	Actions
Apps*	App Catalog	Add apps from iTunes, Google Play, Windows Store, In-House apps, and Web Applications.
	iBooks	Manage Apple iBooks.
	Installed Apps	Manage installed apps.
	App Tunnels	Manage registered and unregistered app tunnels.
	App Control	App Control enables you to: <ul style="list-style-type: none"> Specify app control rules, including white list, black list, and required apps . Identify devices that are out of compliance with app control rules.
	Apps@Work Settings	Create store-front branding for Apps@Work.
	App Licenses	Manage the Apple licenses.
Policies & Configs	Configurations	Manage, import, and export configurations.
	Policies	Manage policies.
	ActiveSync Policies	Manage ActiveSync policies for devices that connect to the enterprise using ActiveSync.
	Compliance Policies	Customize compliance policy rules.
	Compliance Actions	Manage default and custom compliance actions for policies.
Services	Access	Add and manage Access as a service. Access is a cloud service that secures access to enterprise content in business cloud services such as Office 365, G Suite, Salesforce, Box, and Dropbox. For information about Access as a service and how to set up the service with Core, see the <i>Access Guide</i> .
	Sentry	Add and manage Sentry.

TABLE 4. SUB-LEVEL MENU ITEMS (CONT.)

Action menu	Sub-level menu items	Actions
		For information about Sentry and how to setup the service with Core, see the <i>Sentry Guide for Core</i>
	Connector	Add and manage Connector.
	LDAP	Add and manage LDAP.
	Google	Add and manage Google account.
	Operators	Add and manage Operators.
	LDAP	Add and manage LDAP.
	Local CA	Add and manage local CA.
	Trusted Root Certificate	Add and manage trusted root certificates.
	Samsung	Samsung Firmware E-FOTA License Management.
Settings	System Settings	Manage settings for General, Security, Users & Devices, iOS, Android, Windows, Licensed Products, and App Reputation. Actions you can take include, setting up alerts, outbound HTTP, registration, MDM for iOS devices, SMS & Call Log archives for Android devices, setting up the Business Store Portal for Windows devices.
	Templates	Manage templates such as registration and event center templates.
Logs	Audit Logs, MDM Activity, Certificate Management, Even Settings, Events	Use these options for troubleshooting.

*Refer to the *Core Apps@Work Guide* for more information on managing apps.

Ivanti Community - Submitting Ideas

The original Ideas Portal has moved to the [Ivanti Community](#) and is the place to add your enhancement and new feature suggestions for Core products.



To access the Ivanti Community, you must have an account with Core Support, and must also have the credentials to access that account. For more information, contact your Ivanti representative.

To submit an enhancement or new feature idea to Ivanti Community:

Procedure

1. Go to [Ivanti Community](#) and login.
2. From the **More** drop-down menu at the top, select **Product Ideas** from the alphabetical list.
3. Scroll down the page and select **MobileIron Ideas**.
 - Follow the instructions on the **Ideas** page for a search.
4. To submit an Idea, scroll to the **Post a new idea...** column on the right-hand side of a full screen or scroll down to find.
5. Choose the appropriate product from the list.
6. Fill in the form with the information for your enhancement or new feature idea. There is also a place to upload any files you would like to submit.
7. Click **Post Idea**.

Use the **Posting Guidelines** information if needed. There is a **Contact Us** link if you have issues getting your ideas uploaded.



Managing Users

The topics in this chapter include:

User management overview	40
Accessing the user management page	43
Configuring LDAP servers	43
Managing LDAP users	49
Managing local users in the Admin Portal	64

User management overview

This chapter explains how to manage local and LDAP users for Admin Portal. For information on managing local users in System Manager, refer to *Core System Manager Guide*.

The main topics in this overview include:

Types of users

Core supports local users and LDAP users.

- LDAP users are imported from your organization's LDAP server. In most cases, you will configure an LDAP server and import LDAP users.
- Local users are entities created in the local database. They are not known to the network or other corporate services.

Local users are best for the following scenarios:

- administration
- testing

Local users created in the Admin Portal can be used for registering devices and accessing the Admin Portal and the user portal. Local users created in the System Manager can be used in the System Manager and the CLI.

The misystem user

The **misystem user** is a default Core user used for the following tasks:

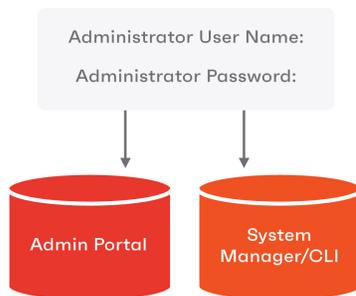
- creates the default rules and policies
- executes system maintenance tasks

This user is not listed in the Admin Portal, and it has no roles assigned to it.

Local users created during setup

The local user you define during setup actually results in two local users, one in the Admin Portal and one in the System Manager.

FIGURE 1. LOCAL USERS CREATED DURING SETUP



Though these two users start with the same name and password, they are separate users stored in separate databases. Changes made to one do not affect the other. For example, if you change the password for the Admin Portal user, the password for the System Manager user does not change.

Users and roles

Work with the following basic user and administrator types in the Admin Portal:

- **Device users:** end users who use the managed devices (owned by themselves or the enterprise).
- **Super Administrators:** manage devices and users throughout Core. These administrators are assigned to the global space. The role that these administrators have that set them apart is Manage administrators and device spaces. Only administrators with this role can create and manage device spaces and assign roles and device spaces to administrators. Core can have one or more Super Administrators.
- **Global Administrators:** manage devices throughout Core. These administrators are assigned to the global space and can be assigned any roles other than Manage administrators and device spaces.



In order for users with global space permissions to see the App tab in the Dashboard, they need to be granted View App Dashboard permissions. See ["Viewing the App Dashboard" on page 213](#).

- **Device Space Administrators:** manage only the devices and users assigned to the device spaces to which they are assigned. For example, an administrator assigned to the Dallas Help Desk device space can only manage devices assigned to that device space. The roles that can be assigned to Device Space Administrators are limited. For example, Device Space Administrators, if assigned the correct role, can view configurations or apply and remove configurations from a label. However, they cannot create or edit configurations.

User roles and LDAP groups

In a large organization, assigning roles to individual users can be cumbersome. Instead, you can assign roles to LDAP groups or organizational units. By assigning roles to an LDAP group or organizational unit, you apply a given role to all the members of the group or organization unit at once.



Core can support up to 15,000 LDAP groups, from Core 11.2.0.0 and higher releases. Earlier releases can support up to 10,000 LDAP groups.

Enforce Single Session role and concurrent session control

Concurrent session control is applied to administrators by assigning them the Enforce Single Session role. The concurrent session control feature automatically logs off a Core session if the administrator has logged in on another machine or browser.



An administrator can use multiple tabs of a single browser without being logged off. An administrator can also use multiple windows of the same browser on the same machine without being logged off.

To enable concurrent session control:

Procedure

1. From the Admin Portal, go to **Admin > Admins**.
2. Select an administrator.
3. Go to **Actions > Edit Roles**.
4. Select **Enforce Single Session**.
5. Click **Save**. The role appears as **Enforce single session (all spaces)** in the list of roles for the administrator.

Accessing the user management page

The Manage user role is required for access to the user management screen. See "[Assigning and removing device user roles](#)" on page 59 for more information.

By default, the user management screen displays the **Authorized Users** view. This view includes LDAP and local users. Select **LDAP Entities** from the **To** drop-down list to display only LDAP entities.

Procedure

1. Log into the Admin Portal.
2. Go to **Devices & Users**.
3. Click **Users** to display the user management screen.

Configuring LDAP servers

Core is designed to interact with LDAP servers. Beginning with the Core 11.7.0.0 release, Lightweight Directory Access Protocol over Secure Sockets Layer (LDAPS) (port 636) is recommended. Networks running Core 11.6.0.0 and earlier are allowed to use regular LDAP, but Ivanti recommends that you adopt LDAPS as soon as practical. See [LDAP Server window fields](#) for Directory URL information.

Before you begin

- You can configure multiple LDAP servers, but each server must contain a unique configuration.
- If you are using distributed LDAP Directory Connections (DC) in a round-robin configuration, you must use **Services > LDAP** to configure a primary DC and a failover (secondary) DC, or risk loss of group associations resulting in removal of apps and configurations. See the descriptions of the [Directory URL](#) and [Directory Failover URL](#) fields in this topic.

Alternatively, you could configure all DCs behind an F5 load balancer with persistent sessions, also known as sticky sessions, enabled. Ivanti has not fully tested this approach.

- The Core Enterprise Connector does not support certificate-based authentication. This means that once you enable Connector service, the **Upload X509 Certificate** option in **LDAP preferences** is not available.

Procedure

1. From the Admin Portal, go to **Services > LDAP**.
2. Click **Add New** to open the New LDAP Setting page.
3. Edit the fields as necessary. Refer to [LDAP Server window fields](#) for details.
4. Scroll to the **LDAP Groups** setting to specify the set of LDAP groups that Core gets from the LDAP server. Only these groups are available throughout the Admin Portal for viewing or selection.
 - a. Go to **Search By LDAP Groups**, enter the first characters of an LDAP Group that you want to select.
 - b. Click the search icon. The LDAP Groups in the LDAP server that match the search request appear in the **Available** section.
 - c. Click the right arrow to move one or more LDAP groups to the **Selected** section.
5. Repeat steps a through c for other LDAP Groups.
6. Click **Advance Options** to configure LDAP v3 properties.



Configurations in the **Advanced Options** pane apply only to LDAP v3 servers.

7. Select the authentication method between the client and server used in the SASL exchange.
 - **Bind** (default): This method uses the directory DN for authentication.
 - **Kerberos v5** (SASL): This method uses mutual authentication.

8. Select the user ID format from the **Authentication User ID Format** drop-down list.
 - User Principal
 - User UPN (user principal name)
 - User DN (distinguished name)
 - User DN with RFC2829 prefix
 - User Principal with RFC2829 prefix
9. Select the group member format from the **Group Member Format** drop-down list.
 - **DN** - Distinguished name
 - **UID** - Unique Identifier
10. Select the parameter for negotiating the authentication from the **Quality of Protection** drop-down list.



LDAP v3 supports the Quality of Protection feature, which is not an LDAP v2-supported feature.

- **Authentication only** is used for authenticating a user to a server.
 - **Authentication with integrity protection** is used to ensure that subsequent LDAP requests and responses are protected against tampering.
 - **Authentication with integrity and privacy protection** is used to ensure that subsequent LDAP requests and responses are encrypted and therefore protected against unintended monitoring. Privacy protection automatically entails integrity protection.
11. Select the LDAP authentication method.
 - **Use Client TLS Certificate**: Select this to use the X509 certificate for authentication.
 - Go to **Services > LDAP > Preferences** to upload the client X509 certificate that Core presents to the LDAP server
 - **Request Mutual Authentication**: Select this to verify both the identity of the user that is requesting authentication as well as server providing the requested authentication.
 12. Select **Enable Detailed Debug** to enable JNDI debugging for LDAP communication.
 13. Enter additional (and optional) properties in the **Additional JNDI Context Properties** field.

14. Most environment properties are predefined but some, such as **language**, **security.credentials**, **security.principle**, are implementation-specific. Properties defined here replace any values that are previously defined, and will take effect the next time the property is invoked. If a context does not have a particular environment property, it behaves as if it has that environment property with its default value. For example,
 - To set the language for Japanese, enter `Context.LANGUAGE, "ja-JP"`
 - To set the credentials to the string "secret", enter `Context.SECURITY_CREDENTIALS, "secret"`
 - To set the principal name to the distinguished name "cn=admin, o=MI, c=us," enter `Context.SECURITY_PRINCIPAL, "cn=admin, o=MI, c=us"`
15. Click **View LDAP Browser** to view the LDAP server directory tree structure.
16. Click **Test** to open the **LDAP Test** window
17. Enter user or group identifier in the appropriate field.
18. Click **Submit**. A result page displays if the user was configured on the LDAP server.
19. Return to the LDAP page and click **Save**. A dialog appears informing of traffic disruption and asks to proceed.
20. Click **Yes**. A dialog appears informing the status.
21. Click **OK**. The server you created appears on the LDAP page.

LDAP Server window fields

This field determines whether you use regular LDAP or LDAP over Secure Sockets Layer (LDAPS). LDAPS is recommended for Core 11.7.0.0 and later releases.

When using LDAPS

- You need an X509 certificate for LDAPS authentication.



If the certificate has a **SAN** field, Core ignores the **CN** value and seeks a match in the **SAN** list. Using the **CN** field is deprecated. Therefore, Core checks the **CN** only if the **SAN** is not present.

- These certificate fields presented by the LDAPS server to Core *must* match the URL:
 - Common Name (**CN**)
 - Subject Alternative Name (**SAN**)
 - Domain Name System (**DNS**) name
 If no match exists, the connection request fails.

- You do not need to specify the ports when you use these default ports:
 - **389** for LDAP - Not recommended. Available for Core releases 11.6.0.0 and earlier.
 - **636** for LDAPS - Recommended for Core releases 11.7.0.0 and later.

The following table summarizes fields and descriptions in the **LDAP Server** window:

TABLE 5. LDAP SERVER FIELDS

Fields	Description
Directory URL	Enter the URL to the LDAP server. Make sure to start with ldap:// or ldaps:// .
Directory Failover URL	Enter a secondary URL, if available.
Directory UserID	Enter the primary user ID, for example, userid@local.domain . Make sure to include the domain, for example, @local.domain , with the user ID.
Directory Password	Enter the password for the user ID set above.
Search Results Timeout	Do not change default of 30 seconds unless you get connection errors.
Chase Referrals	<p>Select Enable if you are using a multi-forested domain. This indicates you want to use alternate domain controllers when the targeted domain controller does not have a copy of the requested object.</p> <p>Select Disable if you do not use alternate domain controllers.</p> <hr/> <p> Enabling the Chase Referrals option delays LDAP authentication.</p>
Admin State	Select Enable to put the server to service. Make sure to enable the Admin state or the LDAP server will be invisible.
Directory Type	<p>Select Domino for the IBM Lotus Domino server platform. The default DN and other LDAP search filters are automatically changed to the Domino server.</p> <p>Select Active Directory for the Microsoft Windows server platform.</p>
Domain	Enter the domain name for the Active Directory. This information will automatically traverse all levels of the tree and use to populate Base DN , parent entry.

Changing the LDAP Server Sync Interval

The default interval for synchronization between Core and the LDAP server is 24 hours. You can change this interval for all configured LDAP servers. You might want to change the interval to ensure updated information when the LDAP server data is changing frequently.



For LDAP groups, each synchronization syncs only the LDAP groups that you specified in the LDAP Setting page for each LDAP server at **Services > LDAP**.

To change the LDAP sync interval:

Procedure

1. From the Admin Portal, go to **Services > LDAP > Preferences**.
2. Select the preferred interval from the drop-down. Intervals range from 15 minutes to 24 hours.
3. Click **Save**.

Managing LDAP users

Once you have configured one or more LDAP servers, the associated LDAP entities can be displayed in the **Devices & Users > Users** screen. LDAP entities are useful for assigning roles that are inherited by the members of an entity. LDAP users are immediately available for device registration.

For each LDAP server you configured, you specified the set of LDAP groups that Core gets from the LDAP server. Specifying this set improves Core performance when you use the Admin Portal to access LDAP groups. Because Core has already stored all necessary LDAP group information, no immediate communication with the LDAP server is necessary to complete a task involving LDAP groups.

If you want an LDAP user to have access to the user portal, then you must assign the User Portal role. Likewise, access to features in the Admin Portal requires the appropriate roles.

 Avoid creating user IDs that include `_Mlxx`, where `xx` is a number. This sequence is reserved for user IDs requiring special processing, which includes stripping the `_MI` sequence and all characters following it.

Core supports Apple User Enrollment for LDAP Users and LDAP Groups. See "User Enrollment" in the *Core Device Management Guide for iOS and macOS Devices*.

Configuring the set of LDAP groups

During Core installation, you configure the set of LDAP groups that you can reference in Core.

Procedure

1. From the Admin Portal, go to **Services > LDAP**.
2. Select an LDAP server and click the **Edit** icon.
3. In the **Modifying LDAP Setting** page, scroll down to the **LDAP Groups** setting.
4. In the **Search By LDAP Groups** field, enter the first characters of an LDAP Group you want to select.
5. Click the search icon.

The **LDAP Groups** in the LDAP server that match the search request appear in the Available section.

6. Click the right arrow to move one or more LDAP groups to the **Selected** section.

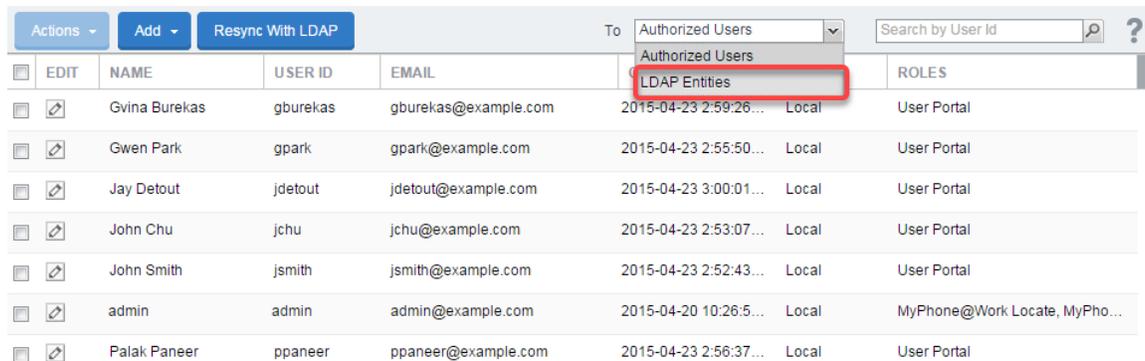
7. Repeat steps 4 through 6 for other LDAP Groups.
8. Click **Save**.

Displaying available LDAP users

Procedure

1. From the Admin Portal, go to **Devices & Users > Users**.
2. Select **LDAP Entities** from the **To** drop-down list.

FIGURE 1. SELECT LDAP ENTITIES FROM THE USERS PAGE



EDIT	NAME	USER ID	EMAIL	To	ROLES
<input type="checkbox"/>	Gvina Burekas	gburekas	gburekas@example.com	2015-04-23 2:59:26... Local	User Portal
<input type="checkbox"/>	Gwen Park	gpark	gpark@example.com	2015-04-23 2:55:50... Local	User Portal
<input type="checkbox"/>	Jay Detout	jdetout	jdetout@example.com	2015-04-23 3:00:01... Local	User Portal
<input type="checkbox"/>	John Chu	jchu	jchu@example.com	2015-04-23 2:53:07... Local	User Portal
<input type="checkbox"/>	John Smith	jsmith	jsmith@example.com	2015-04-23 2:52:43... Local	User Portal
<input type="checkbox"/>	admin	admin	admin@example.com	2015-04-20 10:26:5... Local	MyPhone@Work Locate, MyPho...
<input type="checkbox"/>	Palak Paneer	ppaneer	ppaneer@example.com	2015-04-23 2:56:37... Local	User Portal

3. Select **LDAP Users** from the **Category** drop-down list.
4. In the **Search by Name** field, enter text that will match an LDAP user entry in the selected category, based on first name, last name, or account name.

You may use % as a wildcard. For example, to search for all users having "smith" at the end of the user ID, you would enter %smith.

5. Click the search icon. The matching user records display.

LDAP does not report members for a group that is also the Primary Group for those members. If you do not see the users you expect, examine your LDAP configuration. Consider using organizational units (OUs), instead.

Deleting LDAP entities without roles

Core displays all LDAP entities, by default, whether or not they have a role assigned or if the role has been revoked. However, you can group all LDAP entities together that do not have roles and delete them at one time.

Procedure

1. From the Admin Portal, go to **Devices & Users > Users**.
2. Select **LDAP Entities** from the **To** drop-down list.
3. Select **LDAP Entities without Roles** from the **Category** drop-down list.
4. Select or search for one, some, or all of the LDAP entities without roles.
5. Click **Actions > Delete > Yes**.

Viewing LDAP user and group associations

The Users screen includes links for displaying associations between users and groups. For example, if you have assigned a role to the Engineering group, you can display the users associated with that group.

FIGURE 2. VIEWING LDAP ASSOCIATIONS

TYPE	NAME	DN	ROLES	USERS/...
Group	group100_1...	cn=group100_102,ou=labeltest,dc=auto2,dc=...	User Portal	View Users
Group	group2000_1	cn=group2000_1,ou=labeltest,dc=auto2,dc=m...	User Portal	View Users
Group	biggroup1	cn=biggroup1,ou=labeltest,dc=auto2,dc=mobi...	User Portal	View Users
Group	group100_1...	cn=group100_101,ou=labeltest,dc=auto2,dc=...	User Portal	View Users
Group	group100_1...	cn=group100_100,ou=labeltest,dc=auto2,dc=...	User Portal	View Users
Group	group100_10	cn=group100_10,ou=labeltest,dc=auto2,dc=m...	User Portal	View Users
Group	group100_1	cn=group100_1,ou=labeltest,dc=auto2,dc=mo...	User Portal	View Users
OU	N/A	ou=contacts,dc=auto2,dc=mobileiron,dc=com	MyPhone@Work Registration, User Portal	N/A

Synchronizing with the LDAP server

LDAP Sync returns all Lightweight Directory Access Protocol (LDAP) Organizational Unit (OU) information. This information is used to correlate users in the Core to their OUs. It syncs only the OU information itself, not all the OU user information, which would affect performance. Core synchronizes user data from the LDAP server every 24 hours, by default. For LDAP groups, each synchronization syncs only the LDAP groups you specified in the **Services > LDAP > LDAP Setting** page.

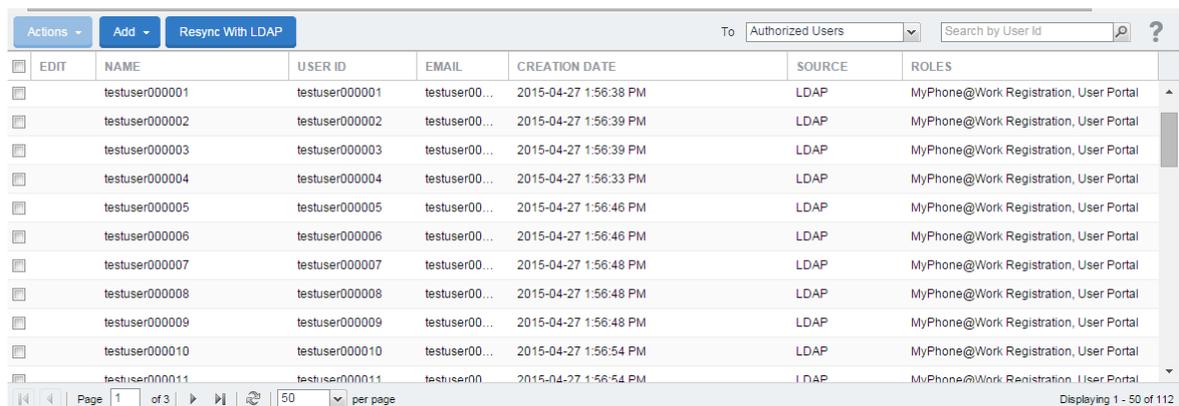
 When syncing LDAP records with Core, if any data integrity errors occur within the batch, only the failed record is discarded.

Procedure

To synchronize with the LDAP server:

1. From Core Devices & Users > Users page, select **LDAP Entities** from the **To** drop-down menu.
2. Click **Resync With LDAP**. A confirmation message displays.

FIGURE 3. SYNCHRONIZING WITH THE LDAP SERVER



The screenshot shows a user management interface with a table of users. At the top, there are buttons for 'Actions', 'Add', and 'Resync With LDAP'. A dropdown menu is set to 'Authorized Users' and there is a search box for 'Search by User Id'. The table has columns for 'EDIT', 'NAME', 'USER ID', 'EMAIL', 'CREATION DATE', 'SOURCE', and 'ROLES'. The table contains 11 rows of test users. At the bottom, there is a pagination control showing 'Page 1 of 3' and '50 per page', and a status indicator 'Displaying 1 - 50 of 112'.

EDIT	NAME	USER ID	EMAIL	CREATION DATE	SOURCE	ROLES
<input type="checkbox"/>	testuser000001	testuser000001	testuser00...	2015-04-27 1:56:38 PM	LDAP	MyPhone@Work Registration, User Portal
<input type="checkbox"/>	testuser000002	testuser000002	testuser00...	2015-04-27 1:56:39 PM	LDAP	MyPhone@Work Registration, User Portal
<input type="checkbox"/>	testuser000003	testuser000003	testuser00...	2015-04-27 1:56:39 PM	LDAP	MyPhone@Work Registration, User Portal
<input type="checkbox"/>	testuser000004	testuser000004	testuser00...	2015-04-27 1:56:33 PM	LDAP	MyPhone@Work Registration, User Portal
<input type="checkbox"/>	testuser000005	testuser000005	testuser00...	2015-04-27 1:56:46 PM	LDAP	MyPhone@Work Registration, User Portal
<input type="checkbox"/>	testuser000006	testuser000006	testuser00...	2015-04-27 1:56:46 PM	LDAP	MyPhone@Work Registration, User Portal
<input type="checkbox"/>	testuser000007	testuser000007	testuser00...	2015-04-27 1:56:48 PM	LDAP	MyPhone@Work Registration, User Portal
<input type="checkbox"/>	testuser000008	testuser000008	testuser00...	2015-04-27 1:56:48 PM	LDAP	MyPhone@Work Registration, User Portal
<input type="checkbox"/>	testuser000009	testuser000009	testuser00...	2015-04-27 1:56:48 PM	LDAP	MyPhone@Work Registration, User Portal
<input type="checkbox"/>	testuser000010	testuser000010	testuser00...	2015-04-27 1:56:54 PM	LDAP	MyPhone@Work Registration, User Portal
<input type="checkbox"/>	testuser000011	testuser000011	testuser00...	2015-04-27 1:56:54 PM	LDAP	MyPhone@Work Registration, User Portal

 If no LDAP servers are configured, the **Resync with LDAP** button does not appear. VSP-61682

Changing the LDAP Sync Interval

You can configure the amount of time you want between each synchronization with LDAP servers.

Procedure

1. From the Admin Portal, go to **Services > LDAP > Preferences**.
2. Select the preferred interval from the drop-down.
3. Click **Save**.

Suspending scheduled LDAP synchronization globally

You can stop scheduled LDAP synchronization globally in your Core instance. Suspending LDAP synchronization helps prevent losing label associations with devices during maintenance actions such as:

- Core maintenance
- AD or LDAP server maintenance



Any users added to your Core deployment during the time LDAP synchronization is suspended are not added to Core until scheduled LDAP synchronization is resumed.

Procedure

1. From the Admin Portal, go to **Services > LDAP**.
2. In **Preferences**, uncheck **Enable LDAP Sync with Core**.

A screenshot of the LDAP Sync configuration panel. It features a title 'LDAP Sync' in blue. Below the title, there is a label 'LDAP Sync Interval:' followed by a dropdown menu currently showing '24 hours'. Underneath, there is a checkbox labeled 'Enable LDAP Sync with Core' which is currently unchecked.

LDAP Sync

LDAP Sync Interval: 24 hours

Enable LDAP Sync with Core

3. Click **Save**.
4. Click **OK** when the confirmation message displays.



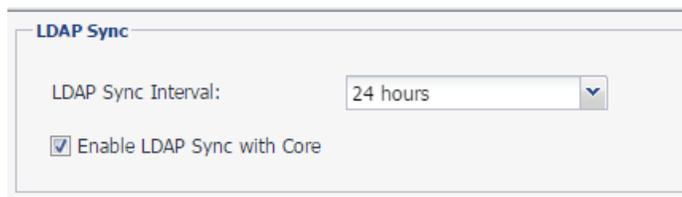
Core enables you to manually synchronize LDAP servers while LDAP synchronization is suspended (see [Synchronizing with the LDAP server](#))

Resuming scheduled LDAP synchronization

Use the LDAP option on the Services menu to resume scheduled LDAP synchronization.

Procedure

1. From the Admin Portal, go to **Services > LDAP**.
2. In **Preferences**, check **Enable LDAP Sync with Core**.



3. Click **Save**.
4. Click **OK** when the confirmation message displays.

Synchronizing your LDAP server manually

You can synchronize your LDAP server manually.

Procedure

1. From the Admin Portal, go to **Devices & Users > Users**.
2. Click **Resync With LDAP**.

Setting the LDAP sync discard option

The LDAP sync discard option under LDAP preferences provides control over:

- Whether to apply the discard policy to individual LDAP Groups as well as global, or global only.
- Whether to discard the LDAP sync data if the reloaded data set declines significantly. Discarding the sync data means that no LDAP data additions, changes, or deletions are made on Core.
- At what point the decline is considered significant. You can specify the decline of users as a percentage or a number. The percentage or number is compared against the following:
 - The total number of LDAP users in Core.
 - The number of users in each top-level LDAP group. A top-level LDAP group is one of the LDAP groups that you selected in the LDAP setting at **Services > LDAP** in the Admin Portal.

The LDAP sync discard option is enabled by default and set to 25%.

Using this option ensures that removing a number of users on the LDAP system in excess of the configured percentage or number does not result in the deletion of users in the Core database. Consider changing or disabling this setting if you are going to make major changes to your LDAP system.

Additional considerations

- Core discards the sync data only if the **net** decrease of users is greater than the specified percentage or number.
- For example, if 999 users had been removed from a group, and 1000 different users had been added to the same group, Core does **not** discard the LDAP sync data. The sync data is not discarded because the net change was 1 user. Therefore, Core will remove the 999 users.
- Changes on the LDAP server of information associated with a user (such as LDAP attributes, distinguished name, email, or country of origin) do not impact whether Core discards the LDAP sync data. However, changes in group membership can impact whether Core discards LDAP sync data.
- For example, if 1000 users were moved from one LDAP group to another, and the threshold number is 500, Core will discard the LDAP sync data, and no changes are made on Core.
- However, if only 400 users were moved from one LDAP group to another, and the threshold number is 500, Core does **not** discard the LDAP sync data. Therefore, if you had assigned a different set of roles or labels to each of the LDAP groups, users that were moved from one group to another would be associated with a different set of roles or labels. Depending on the change, users could no longer have the configurations, profiles, or policies that they require to access email, apps, or content critical to their job.



Important. Be sure to confirm that the changes are acceptable before disabling this feature.

Leaving it disabled can allow an LDAP server configuration change to remove every LDAP user from the Core database. That removal can cause catastrophic changes affecting a user's labels which impacts capabilities such as access to email and apps.

Procedure

1. From the Admin Portal, go to **Services > LDAP**.
2. In preferences, go to **Enable sync Discard**.

FIGURE 4. SERVICES > LDAP > PREFERENCES > ENABLE SYNC DISCARD

Enable Sync Discard ⓘ

Options: Group and Global Global Only

Discard if reloaded LDAP data decreases by more than: 25 %

Discard if reloaded LDAP data decreases by more than: [] users

3. The default choice is **Group and Global**, which allows you to enable sync discard for individual LDAP Groups, as well as global (top-level group).
4. If you select **Discard if reloaded LDAP data decreases by more than <25>%**, LDAP sync data will be discarded if reloaded LDAP data decreases by more than the threshold percentage.
5. If you select **Discard if reloaded LDAP data decreases by more than <value> users**, LDAP sync data will be discarded if reloaded LDAP data decreases by more than the threshold number of users.
6. Click **Save**.

Related topics

See also [Impacts of Making LDAP Changes, "Configuring LDAP servers" on page 43](#)

When the LDAP sync declines

Typical reasons for a significant decline in the LDAP sync include:

- Changes in the LDAP environment.
- Slow response from the LDAP server.

- Network congestion.

Procedure

1. In the System Manager, navigate to **Troubleshooting > Service Diagnosis**.
2. Click **LDAP>LDAP Sync History**.

Consider the following steps when the sync fails because of discarding the LDAP sync data:

- Did the issue first start at about the same time as a major change to the LDAP environment?

This would suggest that a valid change in the LDAP environment triggered the discard.

- Has the sync failed once or multiple times?

If sync has failed once, try a manual sync. If the LDAP sync continues to fail, check with the LDAP administrator for changes in the LDAP environment that could cause:

- Groups being removed.
- Users being removed from referenced groups or groups within those groups (child groups).
- Determine whether these LDAP changes were expected. Assuming the changes were expected, do the following:
 - Modify the LDAP sync discard percentage to allow Core to apply (not discard) the LDAP sync.
 - Run a manual LDAP sync. Make sure it succeeds.
 - Modify the LDAP sync discard percentage or number back to your previously determined safe level.

Impacts of Making LDAP Changes

Making changes in your LDAP implementation can result in removal of devices from Core labels, which also removes Core policies, configurations, and apps applied using those labels. This results when the information stored in the database on Core differs from the information returned by Core's LDAP sync process. For example, if your Core implementation uses labels based on LDAP group membership, then removing all configurations in your LDAP implementation would cause the LDAP sync process to determine that those associations no longer exist. Because the Enable Sync Discard option is based on a percentage or specified number change of the total number of users or the users in each top-level group, if this option is also unchecked, then the magnitude of the change does not prevent Core from making sweeping changes to your managed devices.

If you intend to make major changes to your LDAP implementation, consider the following precautions:

- Temporarily turn off the Enable LDAP Sync with Core option.
- Temporarily turn on the Enable Sync Discard option.

Deleting LDAP data from the Core database

i CAUTION: Typically, you delete all LDAP data from the Core database *only* on a test environment.

Because deleting all LDAP data leads to the following results:

- All labels populated by LDAP group membership will be removed from users and devices, because the users will no longer be associated with any groups.
- All policies, configurations, and apps dependent on those labels to be applied to a device will be removed.
- LDAP group and user role assignments will still be present on Core, even though, with the LDAP setting disabled, the user will not be able to login.

Therefore, use the following process to delete LDAP data from the Core database *only if you understand the above impact*.

Procedure

1. Disable or delete all existing LDAP settings.

These can be disabled by editing an LDAP setting under **Services > LDAP** and changing the **Admin State** from **Enabled** to **Disabled**.

2. Uncheck **Enable Sync Discard** under **Services > LDAP > Preferences**.
3. Either trigger a manual LDAP sync or wait for a regular LDAP sync.
4. After the LDAP sync has completed successfully, confirm device label association changes have completed.

Deleting LDAP users

You can delete an LDAP user if that user is not associated with a registered device.

Procedure

1. Log into the Admin Portal.
2. Go to **Devices & Users > Users**.
3. Click the check box for the user you want to delete.
4. Select **Actions > Delete User**.

Moving between the LDAP entity display and the local user view

To see the list of local users and LDAP users on the **Devices & Users > Users** page, select **Authorized Users** from the **To:** drop-down list. To see the LDAP entities, select **LDAP Entities**.

Assigning and removing device user roles

The Manage administrators and device spaces role is required for this task. Assign roles to enable access to product features available through the user portal.



When modifying permissions or roles for local or LDAP users, you must log out and log back in to the Admin Portal for your changes to take effect.

Procedure

1. From the Admin Portal, go to **Devices & Users > Users**.
2. Select one or more local users or LDAP groups.

Use the **To:** field to change between displaying local users and LDAP entities.
3. Click **Actions** and select **Assign Roles**.
4. Select roles for the users.
5. Click **Save**.

Core recognizes the following roles for device users:

TABLE 6. USER ROLES

Roles	Description
User Portal	<p>Allows access to the user portal.</p> <p>For Windows Phone (8.0) this role is required for registration.</p> <p>With User Portal selected, you can choose to enable or disable the following roles:</p> <ul style="list-style-type: none"> • Wipe Device • Lock Device • Unlock Device • Locate Device • Retire Device • Register Device • Change Device Ownership • Reset PIN • Reset Secure Apps Passcode <hr/> <p> Local administrative users must be assigned the User Portal role to allow them to reset their password.</p> <hr/> <p>Local users receive User Portal access by default, but LDAP users do not.</p>
Wipe Device	<p>Enables device users to wipe their phones through the user portal.</p> <hr/> <p> Warning: Wipe is destructive and cannot be reversed. Do not select this option unless you want to enable end users to wipe their devices.</p> <hr/>
Lock Device	<p>Enables device users to lock their phones from the user portal.</p>
Unlock Device	<p>Enables device users to unlock their phones through the user portal.</p>
Locate Device	<p>Enables device users to locate their phones from the user portal.</p>
Retire Device	<p>Enables device users to unregister their phones through the user portal.</p>
Register Device	<p>Enables device users to register phones from the user portal.</p>
Change Device Ownership	<p>Enables device users to change ownership from Employee Owned to Company Owned or vice-versa.</p>

TABLE 6. USER ROLES (CONT.)

Roles	Description
	<p>Changing device ownership from company-owned to employee-owned or vice-versa may impact:</p> <ul style="list-style-type: none"> • The policies and configurations that are applied to the device. • The apps that are available through Apps@Work. • iBooks that are available on the device. <p>Devices are impacted when they check-in with Core depending on the labels to which company-owned or employee-owned devices are applied.</p>
Reset PIN	Enables device users to reset the device PIN on Windows devices.
Reset Secure Apps Passcode	Enables device users to reset the secure apps passcode on Android and iOS devices.
Use Google Device Account (for Android Enterprise device only)	This selection is for configuring the Android shared-kiosk mode. See "Configuring a staging user" in <i>Getting Started with Core</i> .
Allow Account Driven Apple User Enrollment	Allows Apple device users to self-enroll from the Settings page on their device, thus making their device managed. For more information, see "Account-driven Apple User Enrollment" in the <i>Core Device Management Guide for iOS and macOS Devices</i> .
Force User Enrollment for non-supervised iOS device registrations.	This selection is for User Enrollment with Apple Business Manager. For more information, see "User Enrollment with Apple Business Manager" in the <i>Core Device Management Guide for iOS and macOS Devices</i> .
Enable Authenticator Only Role	<p>Select to enable users to register their unmanaged mobile device in Authenticator Only mode. This user role designates 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 SaaS applications and other business services.</p> <hr/> <p> If the role is removed, the devices registered by user are also retired.</p>

TABLE 6. USER ROLES (CONT.)

Roles	Description
	<p>When you assign the Enable Authenticator Only Role to a user, the Retire Device and Register DeviceUser Portal roles are selected by default. The Retire Device and Register Device roles are the only User Portal roles available for Authenticator Only users. All other User Portal roles are grayed out.</p> <p>For information about registering devices in Authenticator Only mode, see "Authenticator Only with Access" in the <i>Access Guide</i>.</p>

The new roles take effect the next time an affected user logs in. A user who is logged in when the change is made must log out and log back in to see the effects of the change.

Core administrator tools overview

After installing Core, administrators can access the following administrator tools:

- Admin Portal
- System Manager

Admin Portal

Use the Admin Portal to manage:

- Users, both local and LDAP .
- Devices, both employee- and company-owned.
- Configurations, settings, and policies, such as security, privacy, and synchronization policies, Wi-Fi and VPN settings, cellular connectivity and single-app mode policies.
- App distribution, including publicly available apps and apps developed in-house.

The Admin Portal is installed as part of the system setup. Refer to the *On-Premise Installation Guide for Core and Enterprise Connector* for installation details.

System Manager

Use the System Manager for performing configuration tasks, such as:

- Managing network settings .
- Configuring security settings.
- Managing Core within your network infrastructure.
- Upgrading Core.
- Troubleshooting and maintenance.

Refer to the *Core System Manager Guide* for information on using the System Manager.

Admin Portal and System Manager credentials

During setup, two local users having the same credentials are created, one for the Admin Portal and one for the System Manager. If you make changes to the roles or password for the Admin Portal user, the changes do not affect the System Manager user.

Managing local users in the Admin Portal

This section explains how to manage local users in the Admin Portal. For information on managing local users in System Manager, refer to *Core System Manager Guide*. Local users that you create in the Admin Portal are separate from the local users that you create in the System Manager.

 High-security environments using Core 11.5.0.0 and higher can apply the **CLISH *limitUser*** command during post-installation configuration to limit the creation of Local Users to one. Once enabled, you will need Ivanti Customer Support to modify the configuration. This feature has no effect on the number of LDAP users. In these cases, the following tasks do not apply.

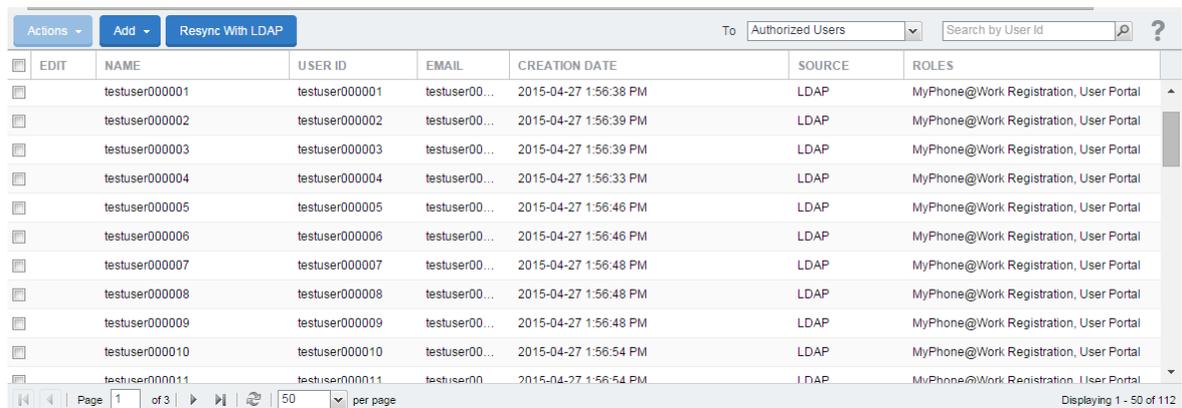
Adding local users in the Admin Portal

Required role: The **Manage** user role is required for completing this task. See [Assigning and removing device user roles](#) for more information.

 Avoid creating user IDs that include `_Mlxx`, where `xx` is a number. This sequence is reserved for user IDs requiring special processing, which includes stripping the `_MI` sequence and all characters following it.

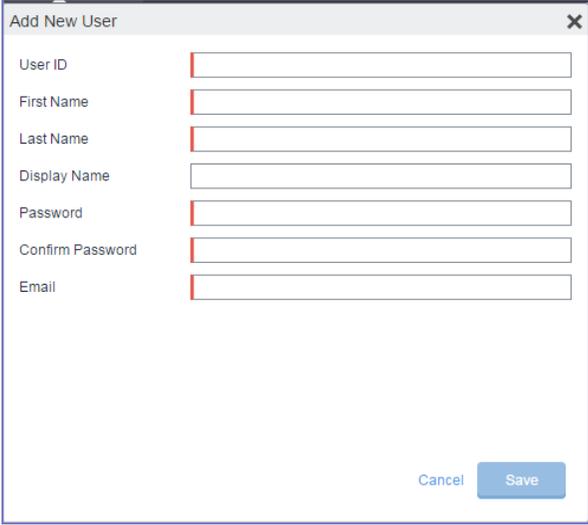
Procedure

1. From the Admin Portal, go to **Devices & Users > Users** to open the Users window.



EDIT	NAME	USER ID	EMAIL	CREATION DATE	SOURCE	ROLES
<input type="checkbox"/>	testuser000001	testuser000001	testuser00...	2015-04-27 1:56:38 PM	LDAP	MyPhone@Work Registration, User Portal
<input type="checkbox"/>	testuser000002	testuser000002	testuser00...	2015-04-27 1:56:39 PM	LDAP	MyPhone@Work Registration, User Portal
<input type="checkbox"/>	testuser000003	testuser000003	testuser00...	2015-04-27 1:56:39 PM	LDAP	MyPhone@Work Registration, User Portal
<input type="checkbox"/>	testuser000004	testuser000004	testuser00...	2015-04-27 1:56:33 PM	LDAP	MyPhone@Work Registration, User Portal
<input type="checkbox"/>	testuser000005	testuser000005	testuser00...	2015-04-27 1:56:46 PM	LDAP	MyPhone@Work Registration, User Portal
<input type="checkbox"/>	testuser000006	testuser000006	testuser00...	2015-04-27 1:56:46 PM	LDAP	MyPhone@Work Registration, User Portal
<input type="checkbox"/>	testuser000007	testuser000007	testuser00...	2015-04-27 1:56:48 PM	LDAP	MyPhone@Work Registration, User Portal
<input type="checkbox"/>	testuser000008	testuser000008	testuser00...	2015-04-27 1:56:48 PM	LDAP	MyPhone@Work Registration, User Portal
<input type="checkbox"/>	testuser000009	testuser000009	testuser00...	2015-04-27 1:56:48 PM	LDAP	MyPhone@Work Registration, User Portal
<input type="checkbox"/>	testuser000010	testuser000010	testuser00...	2015-04-27 1:56:54 PM	LDAP	MyPhone@Work Registration, User Portal
<input type="checkbox"/>	testuser000011	testuser000011	testuser00...	2015-04-27 1:56:54 PM	LDAP	MyPhone@Work Registration, User Portal

2. Select **Add > Add Local User**. The Add New user window displays.



The screenshot shows a dialog box titled "Add New User" with a close button (X) in the top right corner. The dialog contains the following fields:

- User ID
- First Name
- Last Name
- Display Name
- Password
- Confirm Password
- Email

At the bottom right of the dialog, there are two buttons: "Cancel" and "Save".

3. Refer to the following guidelines to complete the information:
4. Add the new user. Refer to the [Add New User window](#) for details.
5. Click **Save**.
6. Assign the necessary roles to users. See "[Assigning and removing device user roles](#)" on page 59.

Add New User window

Use the following guidelines to complete the information:

TABLE 7. ADD NEW USER TABLE

Field	Description
User ID	<p>Enter the unique identifier to assign to this user. The following characters are allowed when entering a UserID. All other characters, including spaces, are prohibited.</p> <ul style="list-style-type: none"> • Letters (uppercase and lowercase) • Numbers (0-9) • Dashes (-) • Underscores (_) • Periods (.) • At sign (@) • Dollar sign (\$) • Hash tag (#) • Extended ASCII/UTF-8 <hr/> <p> If you are using local users and LDAP users, the user ID cannot match that of an LDAP user.</p> <hr/>
First Name	Enter the user's first name.
Last Name	Enter the user's last name.
Display Name	<p>Optional name used to identify the device user. If you leave this field blank, then the display name will have the following format:</p> <p>Firstname Lastname</p>
Password	<p>Enter a password for the user. Valid passwords are determined by the password policy for local users. For details, see:</p> <ul style="list-style-type: none"> • Local user password policy overview • Setting the password policy for local users
Confirm Password	Confirm the password for the user.
Email	Enter the user's email address.

Editing local users in the Admin Portal

Required role: The Manage user role is required for completing this task. See [Assigning and removing device user roles](#) for more information.

You can edit account information for local users. For example, you can:

- Change the user's Core password.
- Edit the first name, last name, or display name.
- Update the email address.

You cannot change the User ID.

To edit local user account information:

Procedure

1. From the Admin Portal, go to **Devices & Users > Users**.
2. Click the **Edit** icon for the user entry to display the **Edit User** dialog.
3. Make the changes to the displayed information. See [Adding local users in the Admin Portal](#) for information on completing each field.
4. To change the user password, click the **Change Password** link, and then enter the old password, the new password, and the new password again in the space provided.
5. Click **Save**.

Linking local users to LDAP users

A local user can be matched with its corresponding LDAP user. For example, suppose you created a local user for preliminary system rollout and testing, but for the production rollout, you want that user matched with their LDAP equivalent.

To match a local user to their corresponding LDAP entry:

Procedure

1. From the Admin Portal, go to **Devices & Users > Users**.
2. Click the check box for the local user you want to match.

3. Select **Actions > Link to LDAP**.



Existing roles for the local user are removed. The next time the user authenticates, roles will be applied based on the LDAP group of the corresponding LDAP user.

Unlocking locked-out local users

Administrators can unlock users who have locked themselves out of the user portal. Users who fail to correctly log in to the user portal within the configured number of tries is blocked from logging in again for a configured period of time, for example, 30 minutes. This function allows a Core Admin to unlock the user account before the required waiting period completes.

Procedure

1. From the Admin Portal, go to **Devices & Users > Users**.
2. Click the check box for the user you want to admit.
3. Select **Actions > Unlock User**.

Deleting local users in the Admin Portal

You can delete a local user if that user is not associated with a registered device.

Procedure

1. From the Admin Portal, go to **Devices & Users > Users**.
2. Click the check box for the user you want to delete.
3. Select **Actions > Delete User**.

Deleting multiple local users in the Admin Portal

You can delete multiple local 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 user's administrator role
- there is a non-retired device associated to the user

Procedure

1. From the Admin Portal, go to **Devices & Users > Users**.
2. Select the check boxes of the users you want to delete.
3. Select **Actions > Delete User**.
4. Click **Yes** to confirm deletion of user.

A dialog box displays confirming successful deletion of user.

5. Click **OK** to close the dialog box.

Forcing a password change for local users

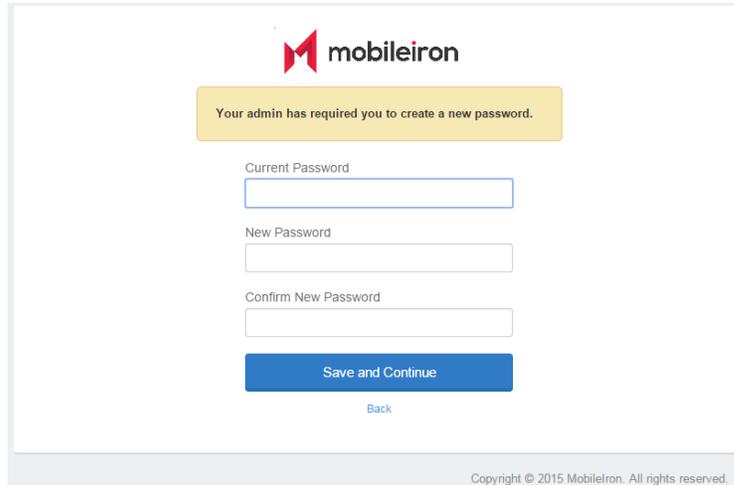
If there is a possibility that a local user's credentials have been exposed or compromised, you can force that user to change the password during the next login. For example, if you have emailed credentials, you should consider forcing the user to set a new password.

Procedure

1. From the Admin Portal, go to **Devices & Users > Users**.
2. Select the user whose password you want to change.
3. Select **Actions > Require Password Change** button.
4. Click **Yes** to confirm the action.

5. The next time the user completes a successful login, the Core login window displays, prompting the user to set a new password.

FIGURE 1. SET A NEW PASSWORD IN THE LOGIN WINDOW



The screenshot shows the MobileIron login interface. At the top center is the MobileIron logo. Below it is a yellow notification box with the text: "Your admin has required you to create a new password." Underneath the notification are three input fields: "Current Password", "New Password", and "Confirm New Password". Below these fields is a blue "Save and Continue" button and a smaller "Back" link. At the bottom right of the page, there is a small copyright notice: "Copyright © 2015 MobileIron. All rights reserved."

Local user password policy overview

You can specify the password policy for local users.

The password policy includes the following:

- Enforcement type, which is one of the following:
 - [Local user password complexity enforcement](#)
 - [Local user password strength enforcement](#)
- Core enforces the password complexity or strength when:
 - You add a new local user in the Admin Portal in **Devices & Users > Users**.
 - Local users change their password.
- Number of failed attempts

After the local user fails to enter the correct password after the specified number of attempts, Core does not allow the user to login until the specified auto-lock time has expired.

- Password history enforcement

When you enforce password history, the local user **cannot** use the previous 4 passwords when changing his password.

Related topics

- [Setting the password policy for local users](#)
- [Local user password complexity enforcement details](#)

Local user password complexity enforcement

You can enforce password complexity requirements on local user passwords. Complex requirements prevent local users from using passwords that are weak and therefore easy to guess. However, requirements that are too complex make using the user ID and password inconvenient for the user because they have to enter a more complicated or longer password. Therefore, when you choose the complexity requirements, consider both your security needs and you local user convenience.

You specify the following password complexity requirements:

- Minimum and maximum password length
- Minimum number of character classes in a password
- Character classes are:
 - Lower case alphabetic characters
 - Upper case alphabetic characters
 - Numeric characters 0 through 9
 - Special characters, which are `! = ({ [_ : - ; ~ ,) }] @ # ^ | $`

In addition to the requirements that you specify, Core enforces the following requirements:

- The password cannot have 4 or more repeating characters.
- The password cannot be the same as the user ID.

Related topics

- [Setting the password policy for local users](#)
- [Local user password complexity enforcement details](#)

Local user password strength enforcement

You can specify the local user password strength to enforce how strong a password must be. Setting the password strength prevents local users from using passwords that are weak and therefore easy to guess. However, setting the password strength too high makes using the user ID and password inconvenient for the user because they have to enter a more complicated or longer password. Therefore, when you choose the password strength requirement, consider both your security needs and your local user convenience.

In addition to your specified password strength, Core enforces the following requirements:

- The password length must be 128 or less.
- The password cannot be the same as the user ID.

Related topics

- [Setting the password policy for local users](#)
- [Local user password strength enforcement details](#)

Setting the password policy for local users

On the password policy for local users, you specify their password requirements.

Procedure

1. Log into the Admin Portal.
2. Go to **Settings > Security > Password Policy**.
3. Select one of these options, and modify one or more of the default fields, as necessary:
 - **Enable Password Complexity Enforcement.** See [Local user password complexity enforcement details](#).
 - **Enable Password Strength Enforcement.** See [Local user password strength enforcement details](#).
4. Click **Save**.



Click **Reset to Default** followed by **Save** to reset the password policy to the default values.

Related topics

- [Local user password policy overview](#)

Local user password complexity enforcement details

The following table summarizes the fields of the local user password policy when using password complexity enforcement:

TABLE 8. FIELDS FOR LOCAL USER PASSWORD COMPLEXITY ENFORCEMENT

Field	Description	Default value
Enable Password Complexity Enforcement	Select this field when you want to apply password complexity requirements to local user passwords.	Selected
Number of Failed attempts	Specify the number of failed attempts that a local user can make when entering his password. After this number of attempts, Core does not allow the user to login until the specified auto-lock time has expired. After the auto-lock time expires, each failed login attempt results in Core not allowing the user to login until the auto-lock time expires again. Valid values are 1 through 16.	5
Auto-Lock Time	Specify how much time in seconds, minutes, hours, or days the local user must wait before he can log in after exceeding the number of failed attempts. Valid values are 0 seconds through 21 days in seconds, minutes, hours, or days. The default value is 5 minutes .	5 minutes
Enforce Passcode History (Last 4 passwords)	Select Enable if you do not want to allow a local user to use the previous 4 passwords when changing his password. To allow a local user to use the previous 4 passwords, select Disable .	Enable
Minimum number of character classes in password	This field is only available when you selected Enable Password Complexity Enforcement . Select the minimum number of different character classes (lower case, upper case, numeric, and special character) that you require in a password.	3

TABLE 8. FIELDS FOR LOCAL USER PASSWORD COMPLEXITY ENFORCEMENT (CONT.)

Field	Description	Default value
	<p>For each character class, you select whether it counts towards the minimum number. The minimum number must be less than or equal to the number of character classes you select.</p> <p>For example, if the minimum number of character classes is 2, you can select 2 or more of the character classes. In this case, if you select Lower Case, Upper Case, and Numeric, the password must contain at least 2 of those character classes.</p>	
Lower Case	<p>Select this option if the lower case character class counts towards the minimum number of character classes that you require in a password.</p> <p>The lower case character class includes the lower case alphabetic characters 'a' through 'z'.</p>	Selected
Upper Case	<p>Select this option if the upper case character class counts towards the minimum number of character classes that you require in a password.</p> <p>The lower case character class includes the upper case alphabetic characters 'A' through 'Z'.</p>	Selected
Numeric	<p>Select this option if the numeric character class counts towards the minimum number of character classes that you require in a password.</p> <p>The numeric character class includes the characters '0' through '9'.</p>	Selected
Special Character	<p>Select this option if the special character class counts towards the minimum number of character classes that you require in a password.</p> <p>The special character class includes these characters:</p> <p>!= ({ [_ : - ; ~ ,) } } @ # ^ \$</p>	Not selected

TABLE 8. FIELDS FOR LOCAL USER PASSWORD COMPLEXITY ENFORCEMENT (CONT.)

Field	Description	Default value
Min Password Length	Select the minimum number of characters in a password. Valid values are 6 through 16. For Android devices: When the Don't Care option is set for the Password Type field, the Password Length field does not apply.	8
Max Password Length	Select the maximum number of characters in a password. Valid values are 21 through 32.	32

Related topics

- [Local user password policy overview](#)
- [Setting the password policy for local users](#)

Local user password strength enforcement details

The following table summarizes the fields of the local user password policy when using password strength enforcement:

TABLE 9. FIELDS FOR LOCAL USER PASSWORD STRENGTH ENFORCEMENT

Field	Description	Default value
Enable Password Strength Enforcement	Select this field when you want to apply password strength requirements to local user passwords.	Not selected
Number of Failed attempts	Specify the number of failed attempts that a local user can make when entering his password. After this number of attempts, Core does not allow the user to login until the specified auto-lock time has expired. After the auto-lock time expires, each failed login attempt results in Core not allowing the user to login until the auto-lock time expires again. Valid values are 1 through 16.	5

TABLE 9. FIELDS FOR LOCAL USER PASSWORD STRENGTH ENFORCEMENT (CONT.)

Field	Description	Default value
Auto-Lock Time	Specify how much time in seconds, minutes, hours, or days the local user must wait before he can log in after exceeding the number of failed attempts. Valid values are 0 through 3600 seconds (60 minutes).	30 seconds
Enforce Passcode History (Last 4 passwords)	Select Enable if you do not want to allow a local user to use the previous 4 passwords when changing his password. To allow a local user to use the previous 4 passwords, select Disable .	Enable
Password Strength	Select a value between 0 and 100, where 0 is the weakest requirement, and 100 is the strongest requirement. You can enter a value or move the slider. For details, see Local user password strength value descriptions .	35

Related topics

- ["Local user password policy overview" on page 70](#)
- [Setting the password policy for local users](#)

Local user password strength value descriptions

The following table describes the local user password strength values:

TABLE 10. LOCAL USER PASSWORD STRENGTH VALUE DESCRIPTIONS

Strength value	Description	Examples
0 - 20	<p>Weak: risky password</p>	<ul style="list-style-type: none"> • Few characters: ;">zxcvbn • Sequences: ;">abcdefghijk987654321 • Names: ;">briansmith4mayor • Words: ;">viking • Words with number substitutions: ;">ScoRpi0ns
21 - 40	<p>Fair: protection from throttled online attacks</p> <p>Throttled online attacks are attacks to guess the passcode which are:</p> <ul style="list-style-type: none"> • on the device • rate-limited <p>Rate-limited attacks are limited to some number of attempts per time period.</p>	<ul style="list-style-type: none"> • Few characters but with special characters: ;">qwER43@! • Words plus numbers: ;">temppass22 • Names plus numbers: ;">ryanhunter2000 • Words with special character and number substitutions: ;">R0\$38uD99 • Names with capitalization: ;">verlineVANDERMARK
41 - 60	<p>Good: protection from unthrottled online attacks</p> <p>Unthrottled online attacks are attacks to guess the passcode which are:</p> <ul style="list-style-type: none"> • on the device • not rate-limited 	<ul style="list-style-type: none"> • Longer words with special character and number substitutions: ;">Tr0ub4dour&3 • Longer phrases with numbers and special characters: neverforget13/3/1997 • Longer letter, number, and special character combinations: ;">asdfghju7654rewq, AOEUIDHG&*()LS
61 - 80	<p>Strong: moderate protection from offline slow-hash scenario</p>	<ul style="list-style-type: none"> • Longer random letters and numbers: <ul style="list-style-type: none"> ◦ zevusqr3 ◦ resqu3Wil ◦ tgbvdnjuk

TABLE 10. LOCAL USER PASSWORD STRENGTH VALUE DESCRIPTIONS (CONT.)

Strength value	Description	Examples
	An offline slow-hash scenario is a sophisticated algorithm for guessing a passcode. The algorithm runs offline from the device after copying passcode-related files from the device.	<ul style="list-style-type: none"> Longer phrases with numbers and special characters: Compl3xChar\$
81 - 100	Very strong: strong protection from offline slow-hash scenario	<ul style="list-style-type: none"> Very long random characters: <ul style="list-style-type: none"> eheuczkqyq rWibMFACxAUGZmxhVncy Ba9ZyWABu99 [BK#6MBgbH88Tofv)vs\$w Long phrases: <ul style="list-style-type: none"> ;">correcthorsebatterystaple Long phrases with substitutions: <ul style="list-style-type: none"> coRrecth0rseba++ery9.23.2007staple\$

Related topics

- [Local user password policy overview](#)
- [Setting the password policy for local users](#)



Managing Devices

A device is available for management by Core after it has been registered by a device user or administrator. This chapter covers the following topics:

Devices & Users pages	80
Understanding the Registration page	81
Displaying device assets	84
Single device registration	93
Bulk device registration	97
Tracking registration status	105
Restricting the number of devices a user registers	105
Restricting device registration by enrollment type	106
Using bulk enrollment for Android devices	106
Registration considerations	109

Refer to the *Core Device Management Guide* for other device-related topics. The following table lists advanced topics related to device registration.

TABLE 11. DEVICE REGISTRATION ADVANCED TOPICS

Registration topic	OS
<ul style="list-style-type: none"> • Specifying eligible platforms for registration • Configuring user authentication requirements for registration • Customizing registration messages • Configuring the default ownership for newly registered devices 	All
Web-based registration for Android devices	Android
<ul style="list-style-type: none"> • Web-based registration iOS and macOS device. • Removing an MDM profile. 	iOS, macOS
Registration by invitation	Windows
<ul style="list-style-type: none"> • In-app registration for iOS and Android • Visual privacy 	Android, iOS
<ul style="list-style-type: none"> • ActiveSync device registration • Managing operators and countries 	Android, iOS, Windows



Some features are not applicable if you use MAM-only iOS or Android devices. For more information, see “Managing apps on MAM-only devices” in the Core Apps@Work Guide.

Devices & Users pages

The **Device & Users** pages enable you to manage enterprise devices. Use these pages to:

- Set device registrations defaults
- Register/enroll a new device and associate it with a user.
- Register/enroll devices in bulk mode.
- Display a list of registered devices.
- View and manage devices connected through ActiveSync.
- Apply labels in order to group devices.
- Create, edit, and delete labels.

- Locate, Lock, Wipe or perform other administrative actions on a device.
- Manage Apple Device Enrollment Program and Apple School Manager devices.

Access to Devices & Users pages

To view the Users page, you must have the Manage user role. To view the Devices page, you must have the View device role or a role that includes that permission.

Understanding the Registration page

The Users and Devices Registration page defines a variety of key defaults that will help define the device registration defaults for your device users.

The page consists of the following sections:

- ["Setting passcode and registration code defaults" below](#)
- ["Setting the per-user device limit" on the next page](#)
- ["Ownership settings" on the next page](#)
- ["Using the end user Terms of Service" on page 84](#)
- ["Countries for registration" on page 84](#)
- ["Platforms for registration" on page 84](#)
- ["Setting the default PIN registration settings" on page 84](#)

Setting passcode and registration code defaults

The first options on the Registration page set the defaults for Registration passcodes and PIN codes.

Passcode Expiry (hours): After the configured number of hours, the registration passcode expires. The default is 4 hours. The maximum value is 4320 hours (6 months).

Registration PIN Code Length (6-12): By default, device users must enter a password to register a device. You have the option to require a Core-generated Registration PIN in place of or in addition to the password.

Procedure

1. In the Admin Portal, go to **Settings > System Settings > Users & Devices > Registration**.
2. Select the number of hours after which your registration passcode expires.

3. Select a Registration PIN code Length between 6-12 characters, which sets the minimum length for the PIN.
4. Click **Save**.

Setting the per-user device limit

This task is described (with images) in the section "[Configuring the Per-User Device limit](#)" in the Self-service User Portal chapter of the *Core Device Management Guide* for your operating system.

Setting LDAP group-specific device limits

This task is described (with images) in the section "[Limiting devices per user by LDAP group membership](#)" in the Self-service User Portal chapter of the *Core Device Management Guide* for your operating system.

Ownership settings

Ownership settings allow the administrator to decide whether:

- A newly-registered device is **Company** or **Employee** owned by default
- A newly-registered device from the self-service user portal is **Company** or **Employee** owned by default
- A newly-registered Android device using Google Zero Touch (ZT) or Samsung Knox Mobile Enrollment (KME) or non-GMS (Android Open Source Project (AOSP) mode is **Company** or **Employee** owned by default

Procedure

1. In Core, go to **Settings > System Settings > Users & Devices > Registration**.
2. For the **Default ownership for a newly registered device** setting, select the relevant radio button:
 - Company owned
 - Employee owned

- For the **Default ownership for a device newly registered at the user Self-Service Portal**, select the relevant radio button:
 - Company owned
 - Employee owned
-



This only impacts the default selection in the self-service portal at the time of new device registration. Device users can still change the device ownership.

- For the **Default Ownership of Android devices using Google ZT or Samsung KME or non-GMS (AOSP) mode** setting, select the relevant radio button:
 - Company owned
 - Employee owned

Select **Show Terms of Service** to have them displayed in the client. If de-selected (default), the Terms of Service will not display. (To create a Terms of Service, see [Configuring an end user Terms of Service agreement](#) in the *Core Device Management Guide for Android and Android Enterprise Devices*.)

- Enable **Save User Password** if you plan to save device user passwords.
-



Important Prior to Core 11.6.0.0, if the "Save User Password" check box was enabled and then disabled, Core did not delete all the Lightweight Directory Access Protocol (LDAP) user passwords already in its database. For Core 11.6.0.0 and later releases, if "Save User Password" is enabled and then disabled, a pop-up message appears, warning that all stored passwords will be deleted.

- To allow device users to learn more about the privacy of their data, click **Enable Privacy Settings in Mobile@Work**. For more details about this feature, see the section [Visual privacy](#) in the Managing Devices chapter of the *Core System Manager Guide* for your operating system.
 - Select **Require device identifiers for enrollment (Android 6.0 or later only)** to require permissions to phone details (phone number and IEMI) for Android device administrator and profile owner.
-



For Core 11.6.0.0 and earlier, this setting applies only to devices with Device Admin (DA) mode. In Core 11.7.0.0+, it includes Android Enterprise modes.

- Click **Save**.

Using the end user Terms of Service

This task is described (with images) in the section [Configuring an end user Terms of Service agreement](#) in the Self-service User Portal chapter of the *Device Management Guide* for your operating system.

Countries for registration

A subset of countries are enabled for device registration by default. You should check this list and determine if any of your users have home countries not represented in the default list. You can move countries back and forth between the Enabled Countries and the Disabled Countries list. For a full task description, see [Enabling additional countries for registration](#) in the Managing Devices chapter of the *Device Management Guide* for your operating system.

Platforms for registration

This task is described in the section [Specifying eligible platforms for registration](#) in the Managing Devices chapter of the *Device Management Guide* for your operating system.

Setting the default PIN registration settings

Enable the **My device has no phone number** check box to allow device users to register without a phone number during PIN Registration.

Displaying device assets

Go to the **Device & Users > Devices** page to display the devices being managed by Core. The following information displays for each device, by default. The columns are configurable.

TABLE 12. DEVICE ASSETS FIELDS

Name	Description
Display Name	Displays the full name of the user registered with this phone.
Current Phone Number	Displays the phone number.
Model	Displays the make and model of the device.

TABLE 12. DEVICE ASSETS FIELDS (CONT.)

Name	Description
	For iOS: If you have MDM for iOS enabled and the View MDM Alerts option selected under Settings > System Settings > iOS > MDM , then entries for iOS devices that need attention will include alert icons. See "Alerts displayed in the Devices page" for information on alerts and what they mean.
Manufacturer	Displays the name of the company that manufactures the device.
Platform Name	Displays the operating system running on the phone as reported by the Core client running on the phone.
Home Country Name	Displays the home country for the device.
Status	Displays the state for each device: <ul style="list-style-type: none"> • Pending means that the user's device has been registered on the Core Server, but the Core Client download has not yet been completed. • Verified means that the user has confirmed that the download of the Core Client should proceed. • Active means that the Core Client has been successfully downloaded and connected back to Core at least once. • Lost means that this phone has been manually marked as Lost. This status does not affect other functionality. • Wiped means that the phone has been restored to factory defaults.
Registration Date	Date the device registered.
Last Check-In	Displays the elapsed time since the device was able to update profiles and configurations from Core.
Owner	Displays whether the device is owned by the company or employee.
Operator	Displays the name of the service provider specified when the phone was registered with Core.

Configuring the Devices page display

You can determine what information displays in the Devices page, such as IP address and battery level.



The selected columns are only retained from session to session for the same user who is using the same browser. In all other situations, the columns displayed on the Devices page revert to the default columns.

Procedure

1. In the Admin Portal, go to **Devices & Users > Devices**.
2. Click the gear icon at the right of the Devices page.
3. Check and uncheck boxes to select the device information to display on the Devices page. The information types are listed in "[Device Page Fields](#)" below. For example, uncheck **Display Name** to remove that column, or check **Battery Level** to add that column. The columns are added and removed from the page as you check and remove checks from the list. The columns are displayed on the Devices page in the order listed beneath the gear icon.

Devices page information types

Use the information in the following table as you set up the **Devices** page.

TABLE 13. DEVICE PAGE FIELDS

Information Type	Description
Display Name	Optional device user name (displayed by default).
Current Phone Number	Current device phone number (displayed by default).
Model	Device model (displayed by default).
Manufacturer	Device manufacturer (displayed by default).
Platform Name	Device platform name (displayed by default).
Home Country Name	Device home country (displayed by default).
Status	Device status, for example, Active (displayed by default).
Registration Date	Date device registered with Core (displayed by default).
Last Check-in	Time of last device check-in (displayed by default).
Anti-Phishing native status	Indicates the status of the anti-phishing policy on the device.
Anti-Phishing VPN status	Indicates the status of the local phishing VPN.

TABLE 13. DEVICE PAGE FIELDS (CONT.)

Information Type	Description
Connected	Lists whether device is currently connected (applies to Android "always connected" devices only).
Owner	Device owner (displayed by default).
Operator	Carrier device uses (displayed by default).
Language	Language device uses.
Email Address	Device email address.
Battery Level	Device power level.
Client Name	The Core client the device uses.
Client Version	Version of the client the device uses.
Data Protection	Displays whether data protection is set or not for the device.
Data Roaming Enabled	Displays whether data roaming is enabled or not for the device.
Device Admin Enabled	List whether device administrator privilege is enabled.
Device is Compromised	Indicates whether the device has been compromised.
Device Locale	Lists the device locale.
Device UUID	The device UUID.
Ethernet	Lists the Ethernet MAC.
IMEI	Lists the IMEI value.
IMSI	Lists the IMSI value.
IP Address	IP address of the device.
iPhone ICCID	Lists the integrated circuit card identifier (ICCID) for the iPhone or iPad device, which is an international identifier for the SIM.
iPhone MAC Address	Lists the MAC address for an iPhone device.
iPhone UDID	Lists the Unique Device Identifier for the Apple device.
iPhone Version	Lists the version of an iPhone.
Device Name	Name assigned the device.
OS Version	OS version the device uses.

TABLE 13. DEVICE PAGE FIELDS (CONT.)

Information Type	Description
Apple Education role	Indicates whether the device has an Apple School Manager role applied to it, specifically Teacher or Student.
Apple Education enabled	Indicates whether Apple Education is enabled on the device, meaning Apple School Manager.

Alerts displayed in the Devices page

The Devices page alert icons table describes the alerts that may be displayed in the **Device & Users > Devices** page (**Device** column) for devices. These alert icons apply to Android and iOS devices only.

TABLE 14. DEVICES PAGE ALERT ICONS

Alert Icon	Alert Name	Description	Action
	Data Protection Disabled (iOS only) iOS Multitasking is Disabled	Data Protection: One of the following MDM-mandated security requirements is not being met: <ul style="list-style-type: none"> • Passcode is not set • Encryption is not fully enabled Multitasking: The multitasking feature for iOS is not enabled, most likely because Location Services has not been enabled on the device.	Display the tooltip for the alert icon. For tooltip Passcode Required , inform the user that MDM mandates setting a passcode on the device. For tooltip Restore Required , inform the user that the device must undergo a complete restore after upgrade to fully enable encryption features. For tooltip iOS Multitasking is Disabled , confirm that Location Services is enabled on the device. On the device, enable location services for Mobile@Work by selecting Settings > Privacy > Location Services > MobileIron .
	Unlocked Device	The OS has been compromised.	If the device connects to email via ActiveSync, then block it using the Block feature in the ActiveSync Association page.

TABLE 14. DEVICES PAGE ALERT ICONS (CONT.)

Alert Icon	Alert Name	Description	Action
			Inform the user that the device must be restored.
	App Control Violation	An app control rule has been violated.	Expand the device's Device Details panel to see specific information on the violation. See the <i>Core Apps@Work Guide</i> .
	Quarantined (iOS only)	Configurations have been removed from the device due to a security violation.	For more information, see "Viewing quarantine information" in the <i>Core Device Management Guide for iOS and macOS Devices</i>
	Device Administrator Not Activated (Android) MDM Profile Removed (iOS)	Device Administrator Not Activated: The device administrator privilege is not activated for the Core app or the Samsung DM Agent. The device administrator privilege is required for most of the device management features that Core provides. For more information on the Samsung DM Agent, see "Uninstalling the Samsung DM Agent" in the <i>Core Device Management Guide for Android and Android Enterprise Devices</i> MDM Profile Removed: The MDM profile has been removed from the device. An MDM profile is required for the Core app on iOS to operate with full functionality.	If the device connects to email via ActiveSync, then block it using the Block feature in the ActiveSync Association page. Inform the user that the privilege must be restored.

Displaying more device and user information

Detailed information about each device is available on the **Device & Users > Devices** page. To expand the device details panel, find the device in the table, and click the caret next to the check box. The device details panel expands immediately below the row. You can have multiple device detail panels open at once.

To close device details, click the **X** in the top right of the panel, or click the caret next to the check box.

When you expand the device details panel, the following displays on the left-hand side:

- Health Attestation (Windows only)
- Location Data (Windows only)
- A link to View Logs for the Device
- A link to Push/Remove Profiles (if applicable)
- A link to Software Version Update
- User name
- User email
- Image of the device
- Phone number (if applicable)
- Device model
- OS version
- Device capacity
- Status
- Last check-in time
- Registration date
- Operator
- Country name
- Device Space

The categories and information available on the right side of the **Device Details** panel are shown in the following table:

TABLE 15. DEVICE DETAILS PANEL

Category	Information Available
Device Details	Device-specific details received from the device. For more information, see "Valid search fields" in the <i>Core V2 API Guide</i> .
Policies	Status of policy distribution.
Labels	Labels applied to this device.
Logs	Click the links to view the logs. For iOS devices, you can only view logs if MDM is enabled. <ul style="list-style-type: none"> • Certificate Inventory • Profile Inventory • Provisioning Profile Inventory

TABLE 15. DEVICE DETAILS PANEL (CONT.)

Category	Information Available
	<ul style="list-style-type: none"> • Managed Apps Inventory • MDM Log (Android and iOS)
Apps	List of apps that are installed on the device.
iBooks	List of iBooks that are present on the device (iOS only).
Configurations	Status of configurations distribution, e.g., Exchange, VPN, etc.
Compliance	App control rule violations or Compliance Policy violations, if any, appear here.
Custom Attributes	Names of custom attributes assigned to the device. You can assign custom attributes to users or devices to associate additional properties with these objects. These properties can then be used to build groups or distribute configurations.
Restrictions	List of restrictions applied to the device.
Comments	Added by a Core administrator to record information about this device

For Android devices:

- For information about details displayed relating to AppConnect for Android, see the *AppConnect for Core Guide*.

For Windows 8.1 Phone devices:

In addition, the following information is also displayed for dual SIM phones:

- IMEI2
- IMSI2
- Roaming2

Adding a comment to device details

The **Comments** tab in the device details panel enables you to add brief text to the device record.

Procedure

1. Click the **Comments** tab.
2. Enter the text.

3. Click **Submit** to save your changes, or **Cancel** to revert to the original comment.
4. The comment pane displays the date and time the comment was created or modified.

Displaying log data for a selected device

You can view log data for a particular device.

Procedure

1. From the Admin Portal, go to **Device & Users > Devices**.
2. Expand the device details panel by clicking the up arrow next to the check box.
3. Click the **View Logs for Device** link, found at the top left of the **Device Details** panel.

Single device registration

Administrators can register a single device from the Admin Portal. This method is best for the following scenarios:

- adding the first few devices to a new system
- adding a few new devices to an existing system

This section contains the following topics for single device registration:

- [Prerequisites for registering a single device](#)
- [Registering a single device](#)
- [Add Single Device window](#)



See [Registration considerations](#) for points to consider before using this registration method.

Prerequisites for registering a single device

Verify that the following conditions exist before registering a device:

- The user (local or LDAP) associated with the device must be available for selection at the time of registration.
- User Portal role must be assigned to the user.

- The following information must be available for the device:
 - Phone number (if any)
 - Country
 - Platform

Registering a single device

For most platforms, this registration method results in user notification by SMS and email. PDA users are notified by email. The SMS contains a live URL link. The email includes a URL, instructions, and the information the user will need to enter during registration. The user can click the live URL in the SMS or enter the URL directly into the device browser to complete the registration process.

If the user does not respond within 48 hours, Core sends a reminder. After 120 hours, the registration expires. This expiration interval is configurable in **Settings > System Settings > Users & Devices > Registration** in the field **Passcode Expiry**. The maximum value is 4320 hours (6 months).

You can register devices using temporary passwords.

Procedure

1. From the Admin Portal, go to **Devices & Users > Devices**.
2. Click **Add > Single Device**.
3. Modify one or more of the following fields, as necessary.
4. Refer to the [Add Single Device Fields](#) table for details.
5. Click **Register**.

After a brief pause, a pop-up window lists instructions for the next step. The content of this pop-up window varies based on the OS and type of the device. Consider leaving this message displayed until the registration has been completed. Note that the instructions also appear in the log.

Add Single Device window

The following table summarizes fields and descriptions in the **Add Single Device** window:

TABLE 16. ADD SINGLE DEVICE FIELDS

Fields	Description
User	<p>Enter user information to locate the user account. For example, you might enter the user ID, first name, last name, or email address. Select the user you want to work with from the drop-down list of matching accounts.</p> <hr/> <p> You can restrict single device registration queries to users within an LDAP OU. If there is an LDAP OU or group included in the Space criteria, the Devices & Users > Devices > Add Device > User field will be constrained to that OU.VSP-62199</p>
Device Platform	<p>Select the name of the operating system used on this phone.</p> <p>If you do not see the platform you want, it may be disabled. For details, see the section, "Specifying eligible platforms for registration" in the Core Device Management Guide.</p>
This device has no phone number	<p>If you do not have a cellular operator for the device or a data plan with your current operator, select This device has no number.</p>
Country	<p>Select one of the supported countries from the drop-down list. Selecting the correct country populates the Country Code field. If the country you need is not displayed, you may need to alter the default country list. Select Settings > System Settings > Users & Devices > Registration.</p>
Operator	<p>Select the name of the mobile service operator for this phone. If you selected a country having a country code other than 1, then this field is hidden.</p> <hr/> <p> You can determine whether an operator is displayed in the list by selecting Services > Operators.</p>
Mobile	<p>Enter the phone number for the device. Your selection from the Country list will populate the Country Code field. Enter the prefix and number without spaces, dashes, leading zeros, or parentheses.</p> <p>For example, you would enter a typical US phone number as 4085555555. You would enter a typical UK phone number as 7889524526.</p>

TABLE 16. ADD SINGLE DEVICE FIELDS (CONT.)

Fields	Description
Device Ownership	<p>Select Company if this phone is owned by the enterprise. Select Employee if this phone is owned by the user. Note that Core automatically assigns default labels based on ownership. For details, see the section Using labels to establish groups.</p>
Device Language	<p>To communicate with the device user in a language other than the default language, select a language from the drop-down list. Languages must first be enabled under Settings > System Settings > General > Language. If the device reports a locale associated with a different language, then the language associated with the locale will be used.</p> <p>Supported languages are:</p> <ul style="list-style-type: none"> • de - GERMAN • en - ENGLISH • es - SPANISH • fr - FRENCH • hu - HUNGARIAN • it - ITALIAN • ja - JAPANESE • ko - KOREAN • nl - DUTCH • pl - POLISH • pt - PORTUGUESE • ro - ROMANIAN • ru - RUSSIAN • sk - SLOVAK • sw - SWEDISH • zh - CHINESE (Default) • zh_tw - CHINESE (Taiwanese)

TABLE 16. ADD SINGLE DEVICE FIELDS (CONT.)

Fields	Description
Include Registration PIN only for Android Company-Owned Device Enrollment	<p>If you selected Android in the Device Platform field, the Include Registration PIN only for Android Company-Owned Device Enrollment field activates. Select this check box to enable PIN-based enrollment for Android Company-Owned Devices. Core will prompt the device user to enter the registration PIN sent by the administrator.</p> <p>For more information, see "Registering Android devices" in the <i>Core Device Management Guide for Android and Android Enterprise Devices</i>.</p>
User Notification	<ul style="list-style-type: none"> • Email: Clear this check box if you do not want the user to receive email concerning registration status. For example, if you are in possession of the phone, and notifying the user about registration activities is not necessary, then clear this option. Select this option if the device is in the owner's possession. • SMS: This option is disabled by default. Select the check box if you want to send SMS messages to devices upon registration. If set to true, the device must have a phone number registered with Core. • Include Registration PIN only for Apple Device Enrollment: This option is only available when selecting iOS or macOS as the device platform. Select to enable PIN-based Apple Device Enrollment for the device. Core will prompt the device user to enter their username and a PIN. <p>For more information about anonymous DEP enrollment, see "Creating Apple Device Enrollment profiles" and "Assigning Apple Device Enrollment devices to an enrollment profile en masse" in the <i>Core Device Management Guide for iOS and macOS Devices</i>.</p>

Related topics

["Bulk device registration" below](#)

Bulk device registration

Administrators can register a large group of devices using a CSV file that contains the information required for bulk registration. This method is best for the following scenarios:

- Adding a large number of devices
- Rolling out multiple devices into a production environment
- Using web-based registration (for details, see "Web-based registration for iOS and macOS devices" in the *Core Device Management Guide for iOS*.)

After the registration CSV file has been imported, Core completes the following tasks:

- Creates specified local user accounts, if they do not already exist.
- Finds specified LDAP user accounts.
- Initiates the registration process.

This section contains the following topics for bulk registration:

- ["Prerequisites for bulk device registration" below](#)
- ["Registering multiple devices" on the next page](#)
- ["Bulk device registration CSV file requirements" on page 100](#)



See ["Registration considerations" on page 109](#) for points to consider before using this registration method.

Prerequisites for bulk device registration

Verify that the following conditions exist before using bulk device registration:

- LDAP users specified in the CSV file must be available for selection. Local users that have not been created already will be created as part of the Bulk Registration process.
- The User Portal role must be assigned to the users.
- The following information must be available for the device:
 - Phone number (if any)
 - Country
 - Platform

You can register devices using temporary passwords.



Core does not support creating both a bulk enrollment record and a single device record for the same user. Only a bulk enrollment or a single add device enrollment should be used for a user, not both.

Refer to "[Bulk device registration](#)" on page 97 for details on how to create a CSV file to use for bulk registration.

Registering multiple devices

For most platforms, the bulk registration method results in user notification by SMS and email. PDA users are notified by email. The SMS contains a live URL link. The email includes a URL, instructions, and the information the user will need to enter during registration. The user can click the live URL in the SMS or enter the URL directly into the device browser to complete the registration process.

If the user does not respond within 48 hours, Core sends a reminder. After 120 hours, the registration expires. This expiration interval is configurable in **Settings > System Settings > Users & Devices > Registration** in the field **Passcode Expiry**. The maximum value is 4320 hours (6 months).

Procedure

1. From the Admin Portal, go to **Devices & Users > Devices**.
2. Click **Add > Multiple Devices** to open the **Adding Multiple Devices** window.
3. Use the **Browse** button to select the CSV file containing the bulk registration data.

You can also select the **Sample CSV File** button in the to start with a sample file and input the content. Refer to the fields in the "[Bulk device registration CSV file requirements](#)" on the next page for details.



If an LDAP OU or Group is part of the Space criteria, the users in the comma-separated values (CSV) file will be matched against it. From the **Devices & Users > Devices > Add Multiple Devices** menu, enter a CSV file and click **Apply** to see the restricted list of users. If the user isn't in the OU or group, "User not found" displays in the Message column for that user.VSP-62258

4. Click **Import File > Apply**.
5. Review the status columns to confirm that each entry was successfully imported.
6. If any items failed, scroll to the right and hover over the **Message** column to display more information.

Bulk device registration CSV file requirements

Note the following requirements when entering your bulk registration content into a CSV file:

- Local user IDs cannot contain spaces. Spaces are allowed for LDAP users.
- The **Platform** field is case sensitive. Enter only uppercase letters in this field.
- Phone numbers cannot contain spaces or non-numeric characters.
- Maximum recommended number of device entries per spreadsheet is 2000. Bulk device registration could fail when using a comma-separated values (CSV) file with more than 2000 device entries.

Each line in the file must contain the following fields, separated by tabs or commas, in the following order.

TABLE 17. FIELDS IN THE BULK DEVICE REGISTRATION CSV FILE

Fields	Description
User ID	<p>Specifies the user ID for either an existing local user, a local user to be created, or an LDAP user that can be looked up as an LDAP user on the configured LDAP server. Spaces are not supported for local users.</p> <p>Example: jdoe</p>
Country Code	<p>Specifies the country code corresponding to the phone number.</p> <p>For PDAs, such as the iPod touch, enter 0 in this field.</p> <p>Example: 1</p>
Number	<p>Specifies the phone number (without country code.)</p> <p>For PDAs, such as the iPod touch, enter PDA.</p> <p>Example: 4085551212</p>
Operator	<p>Specifies the service provider name. This field is not required for PDAs, such as the iPod touch, or for countries having a country code other than 1. See Services > Operators for a list. If the operator does not appear in this list, contact Ivanti Technical Support.</p> <p>Example: Sprint</p>
OS	<p>Specifies a character indicating the operating system. Use the following character:</p> <ul style="list-style-type: none"> • A: Android • I: iOS • L: macOS • E: Windows and Windows Phone <p>Entries are case sensitive.</p> <p>If the specified platform has been disabled for registration, then the registration will fail. For details, see the section "Specifying eligible platforms for registration" in the <i>Core Device Management Guide</i> for your operating system.</p> <p>Example: A</p>

TABLE 17. FIELDS IN THE BULK DEVICE REGISTRATION CSV FILE (CONT.)

Fields	Description
E/C	Specifies phone ownership. Use the following characters: <ul style="list-style-type: none"> • C: Company • E: Employee Example: C
Source	Specifies the identity source of the user name. Use the following characters: <ul style="list-style-type: none"> • D: Directory (LDAP) • L: Local Entries are case sensitive. Example: D
First Name	If the Source field contains "L", provide the user's first name. Example: John
Last Name	If the Source field contains "L", provide the user's last name. Example: Doe
Email	If the Source field contains "L", provide the user's email address. Example: jdoe@mycompany.com
Password	Specifies the password to set for a new local user account. If you do not intend to use this field or the user is an LDAP user, then you can leave it blank. Example: p@\$W0rd

TABLE 17. FIELDS IN THE BULK DEVICE REGISTRATION CSV FILE (CONT.)

Fields	Description
Device Language	<p>Optional. Specifies the language to use for communicating with the device user if the device has not reported its locale.</p> <ul style="list-style-type: none"> • de - GERMAN • en - ENGLISH • es - SPANISH • fr - FRENCH • it - ITALIAN • ja - JAPANESE • ko - KOREAN • nl - DUTCH • pl - POLISH • pt - PORTUGUESE • ro - ROMANIAN • ru - RUSSIAN • sk - SLOVAK • zh - CHINESE Simplified (Default) • zh_tw - CHINESE Traditional (Taiwanese) <p>Example: ja-JP</p>
User Display Name	<p>Optional. Specifies an alternate name used to identify the device user. If you leave this field blank, then the display name will have the following format: Firstname Lastname</p> <p>Example: Smith, Ken</p>
Notify User	<p>Specifies whether to send an email concerning registration status to device users. For example, if you are in possession of the phone, and notifying the user about registration activities is not necessary, then set this option to FALSE. Specify TRUE if the device is in the owner's possession.</p>
Serial Number	<p>Lists device serial numbers.</p>

TABLE 17. FIELDS IN THE BULK DEVICE REGISTRATION CSV FILE (CONT.)

Fields	Description
Notify User by SMS	<p>Optional. Specifies whether to send an SMS regarding registration status to devices. Set this option to FALSE if you are in possession of the device, or if sending bulk SMS messages would be too costly. Set to TRUE if you want to notify device users of their registration status via SMS. If set to true, the device must have a phone number registered with Core.</p> <p>This field is enabled by default.</p>
Include Apple Device Enrollment Only Registration Pin (TRUE or FALSE)	<p>For iOS and macOS devices only.</p> <p>Specifies whether to enable PIN-based, anonymous enrollment using Apple Device Enrollment.</p> <p>For more information about anonymous Apple Device Enrollment, see "Creating Apple Device Enrollment profiles" and "Assigning Apple Device Enrollment devices to an enrollment profile en masse" in the <i>Core Device Management Guide for iOS Devices</i>.</p>
Include Android Corporate Device Enrollment Only Registration Pin (TRUE or FALSE)	<p>For Android devices only.</p> <p>Specifies whether to enable PIN-based registration enrollments for Android Corporate devices.</p> <p>For more information, see "Registering Android devices" in the <i>Core Device Management Guide for Android and Android Enterprise Devices</i>.</p>

Tracking registration status

You can track the registration status of each device.

Procedure

1. From the Admin Portal, go to **Devices & Users > Devices** page to view the state of each device.
 - **Pending:** the device has been registered on the Core Server, but the Mobile@Work app (Apps@Work for Windows) download has not yet been completed.)
 - **Verified:** the user has confirmed that the download of Mobile@Work app (Apps@Work for Windows) should proceed.
 - **Active:** the Mobile@Work app (Apps@Work for Windows) has been successfully downloaded and connected back to Core at least once.
 - **Lost:** the device has been manually marked as Lost. This status does not affect other functionality.
 - **Wiped:** the device has been restored to factory defaults.



Mobile@Work cannot be installed on macOS devices.

Restricting the number of devices a user registers

You can set and enforce a device limit for your users. For example, if the limit is three devices, Core prevents a user from registering a fourth device. The benefits to setting a device limit in Core:

- ensure resources, such as licenses, are available for all users
- prevents misuse of resources
- enforces the corporate device limit automatically, without the need to check each user one-by-one.

Modifying the number of devices users can register

Use this procedure to restrict the number of devices users can register at a time or remove all restrictions.

Procedure

1. From the Admin Portal, go to **Settings > System Settings > Users & Devices > Registration**.
2. In **Per-User Device Limit**, enter the number of devices each user can register.
 - Specify a limit from 1 to 50 devices.
 - Leave the box blank, the default value, to indicate no limit.
3. Click **Save**.

Restricting device registration by enrollment type

You can restrict which devices register with Core based on how the devices were initially enrolled.

Procedure

1. On the Admin Portal, go to **Settings > System Settings > Users & Devices > Device Registration**.
2. Select the check box for **Restrict device registrations by enrollment type**.

Additional options are now available to select.

3. Select one or more of the following enrollment types:
 - **Apple devices that are part of the Automated Device Enrollment Program**
 - **Android devices that are part of the Google Zero Touch**
 - **Android devices that are part of Samsung Knox Mobile Enrollment**
4. Click **Save**.

Only devices enrolled using the selected enrollment method can register with Core.

Deselecting **Restrict device registrations by enrollment type** removes the restriction.

Using bulk enrollment for Android devices

You can use bulk enrollment to register multiple Android devices quickly.



See "[Registration considerations](#)" on page 109 for points to consider before using this registration method.

Before you begin:

- The Android SDK must be installed on the computer used to register the devices.
- Enable USB debugging. For more information on USB debugging see <http://developer.android.com/tools/help/adb.html>.
- Install Mobile@Work on each device.
- Use a USB cable to connect the devices to the provisioning computer.

Example adb shell:

```
$ adb shell am start
"mirp://www.example.com%26user=cc%26pin=316940%26quickStart=false"
```

Sample values include:

TABLE 18. SAMPLE VALUES FOR ADB SHELL

Key	Value
user	User name that would have been typed into the username field if using iReg. Required.
pin	Registration Pin Required.
quickStart	<ul style="list-style-type: none"> • Set to TRUE: Do not display the splash screen. The Privacy screen is not displayed. The Apps@Work shortcut is not created. On Zebra devices, Device Administration privileges are set automatically. • Set to FALSE: The user must tap Continue on the Welcome screen to proceed. When quickstart is set to false the user must choose whether to accept Apps@Work shortcut creation, must Acknowledge Privacy policy, and accept Device Admin privileges. Optional defaults set to FALSE.

Here is an example of a bulk enrollment script:

```
for i in `adb devices | grep -v devices | grep device | cut -f 1`
do
    echo "Registering $i"
    adb shell am start
    "mirp://app183.auto.mobileiron.com%26user=cc%26pin=316940%26quickStart=false"
done
```

You might receive these error messages when you use bulk enrollment.

TABLE 19. BULK ENROLLMENT ERROR MESSAGES

Error	Resolution
mirp scheme not found	Example mirp scheme: am start "mirp://app183.auto.mobileiron.com%26user=cc%26pin=316940%26quickStart=false"
URL is invalid	Occurs if no data string is sent at all. Verify that the URL is correct.
No server information found	Server information missing or improperly entered.
No user information found	Verify that user key was entered.

Registration considerations

This section describes features and dependencies to consider before registering devices, organized by operating system.

- [Registration considerations: Android](#)
- [Registration restrictions for Android](#)
- [Registration considerations: iOS and macOS](#)
- [Registration considerations: Windows](#)
- [Registration considerations: mutual authentication](#)

Registration considerations: Android

Following is a list of registration considerations for Android devices.

- Administrators should decide whether they are supporting password, registration PIN or both for device registration.
- Registration currently depends on acquiring the Core client app (Mobile@Work) from the Google Play store.
- For devices that cannot access Google Play, provide another way for the device users to get the Mobile@Work for Android app. For example, email the app to the device users. You can also place the app on a website and provide the URL to the device users.
- Enabling the Server Name Lookup (in the Admin Portal under **Settings > System Settings**, in the **Users & Devices > Device Registration** page) makes registration easier by automatically filling in the server address for the device user. Administrators will need to follow important, specific instructions for this feature. Please see "Enabling Server Name Lookup" in the *Core Device Management Guide* of your OS.
- If you have configured a Sentry to support Android devices connecting via ActiveSync, then you can initiate registration from the ActiveSync Devices screen.
- By default, the user is required to enter a password to register the device. If you prefer, you can change this behavior to require a MobileIron-generated Registration PIN instead, or to require both a password and a Registration PIN. See the section, "Configuring user authentication requirements for registration" in the **Device Management Guide** for information on specifying behavior for this feature.

- Enroll with Android enterprise. Android enterprise enables devices to have separate private and work profile deployments, and enables administrators to have more control over enterprise owned and provisioned devices. For details on enrolling in Android Enterprise see, *Core Device Management Guide for Android and Android Enterprise Devices*.
- When an app is hidden it can be used by other apps, but not available to launch in the kiosk. For example, a browser can be added to the kiosk but hidden so that it can be used to open URLs from an email app

Registration restrictions for Android

When performing bulk registration of Android devices, you can restrict the OS version as well as the minimum security patch level. Also, you can set a manufacturer's Whitelist or Blacklist and set a minimum SafetyNet certification to enforce SafetyNet attestation. For more information about SafetyNet Attestation, see "Enabling SafetyNet Attestation on Android Devices" in the *Core Device Management Guide for Android and Android Enterprise Devices*.



When placing registration restrictions on Android devices, use Mobile@Work for Android 10.3.0.0 and higher supported versions for the optimum user experience.

To access the registration restriction fields for Android, go to **Settings > System Settings > Users & Devices > Device Registration** and scroll down to the "Restrictions for Android" heading. The following fields restrict device registration on Android devices.

TABLE 20. REGISTRATION RESTRICTIONS FOR ANDROID DEVICES

Item	Description	Default Policy Setting
Minimum OS Version	Use the pull-down menu to set the minimum Android OS version that can run on a registered Android device.	No Setting
Minimum Security Patch Level	Specify the minimum number of days a security patch level is active by using the pull-down menu.	No Setting
Manufacturer Whitelist/Blacklist	<p>Restrict the Android manufacturers that can be configured as Android devices. Select from the following:</p> <p>None: This is the default value. It sets neither whitelist nor blacklist registration restrictions.</p> <hr/> <p> For both the Create a Whitelist and Create a Blacklist fields, the Manufacturer names are case sensitive.</p> <hr/> <p>Create a Whitelist: Allows only devices from specific manufacturers to register as Android devices. Select the check box and then the Manufacturer Name menu is displayed. Use the Add+ button to add the names of one or more manufacturer. Also, Manufacturers who are not specified by this field are block from registering as Android devices.</p> <p>Create a Blacklist: Prevents devices from specific manufacturers from registering as Android devices. Select the check box and then the Manufacturer Name menu is displayed. Use the Add+ button to add the names of one or more manufacturers.</p>	None

TABLE 20. REGISTRATION RESTRICTIONS FOR ANDROID DEVICES (CONT.)

Item	Description	Default Policy Setting
Minimum SafetyNet Certification	<p>Set a required minimum SafetyNet certification level for registering Android devices. If you enable this field, you must also enable SafetyNet Attestation in the default security policy for the devices.</p> <p>None: It sets no minimum SafetyNet certifications for registration. This is the default value.</p> <p>basic: Select to allow only devices with a basic SafetyNet certification from registering as Android devices.</p> <p>certified: Select to allow only devices with a certified SafetyNet certification from registering as Android devices.</p>	None

Registration considerations: iOS and macOS



Some features for macOS are documented but may not be available in your installation.

Following is a list of registration considerations for iOS or macOS devices.

- Administrators will need to decide on whether they are supporting password, registration PIN or both for device registration.
- If you are registering a device with the Core client app, Mobile@Work, you must use an iTunes account to download the app from the iTunes App Store. A credit card is not needed to establish an iTunes account. Simply download Mobile@Work, click Create New Account, and select None as your payment method.
- If you have configured a Sentry to support iOS devices connecting via ActiveSync, then you can initiate registration from the ActiveSync Devices screen.

- Enabling the Server Name Lookup (in the Admin Portal under **Settings > System Settings**, in the **Users & Devices > Device Registration** page) makes registration easier by automatically filling in the server address for the device user. Administrators will need to follow important, specific instructions for this feature. Please see "Enabling Server Name Lookup" in the *Core Device Management Guide* of your OS.
- By default, the user is required to enter a password to register the device. If you prefer, you can change this behavior to require a Core-generated registration PIN instead, or both a password and a registration PIN. See the section, "Configuring user authentication requirements for registration" in the *Core Device Management Guide for iOS*, to specify the behavior for this feature. Registration PINs are not supported for iOS managed apps.
- For MDM-enabled iOS devices, MDM features are not dependent on Mobile@Work after registration. Therefore, if a user uninstalls the Mobile@Work, features like app inventory will continue to function.
- If you need to register many macOS or iOS devices on behalf of users, such as when Macs or iPhones are purchased by the corporation and rolled out in bulk, depot-style registration may be preferable. See "Web-based registration for iOS and macOS devices" in the *Core Device Management Guide for iOS*.
- Consider an extra security option if you are including Mobile@Work for iOS in the Core App Catalog and sending an installation request to devices after device users complete registration, such as with web-based registration. In this case, users do not have to reenter their credentials when they launch Mobile@Work. However, you can limit this silent registration with Mobile@Work to one time only. In the Admin Portal, go to **Settings > System Settings > Users & Devices > Device Registration** and select **Allow silent in-app registration only once. (iOS only)**.
- In iOS 13, the option to "Allow Always" was removed from the iOS Settings app. Instead, a dialog box displays requesting device users to enable tracking when the Mobile@Work app is running. Mobile@Work opens iOS Settings where device users can choose "Ask Next Time" or "Never". We recommend that device users enable tracking. This change applies to all versions of iOS 13 and later supported versions. Mobile@Work for iOS does not track device users' location without consent.
- You can register an Apple TV to Core only through the Apple Configurator. See "Registering an AppleTV" in the *Core Device Management Guide for iOS and macOS Devices*.
- For registering users and devices for Apple Education Manager and Apple Business Manager, see the *Core Device Management Guide for iOS and macOS Devices*

- Device users who are synced to LDAP are to be assigned to a device management role and associated with a Managed Apple ID. Use single invite or bulk registration to verify that the managed Apple ID was generated correctly. After registration, check the logs for any managed Apple ID failures. See "Requirements for enabling User Enrollment" in the *Core Device Management Guide for iOS and macOS Devices*.

Registration considerations: Windows



Some features for Windows are documented but may not be available in your installation.

Following is a list of registration considerations for Windows devices.

- The Apps@Work app is installed for Windows Phone 8.1 as part of the registration process.
- To register Windows 10 devices, open **Settings > Accounts > Your Workplace > Connect to Workplace**.
- Sentry is required for the available device management features.



These devices do not have device management features. However, these devices can sync using Exchange ActiveSync and be managed using ActiveSync policies.

- Single device registration, bulk registration, and invitations to register are supported for all available Windows devices.
 - Registration of the all available Windows device is done through the Windows native client.
 - Device registration fails if the device user enters a password that contains UTF-8 characters. Only ASCII characters are supported in the password field.
 - Enabling the Server Name Lookup (in the Admin Portal under **Settings > System Settings**, in the **Users & Devices > Device Registration** page) makes registration easier by automatically filling in the server address for the device user. Administrators will need to follow important, specific instructions for this feature. Please see "Enabling Server Name Lookup" in the *Core Device Management Guide* of your OS.
 - If auto discovery is not set up, the registration process requires the device user to enter the Core server address (FQDN). The device user will also have to enter the Core server address when logging into Apps@Work for the first time.
 - A root or intermediate certificate from a trusted certificate authority (CA) is required.
-

- The User Portal role is required for the user to register with Core.
- Single device registration, bulk registration, invitations to register are supported.
- Registering your Windows Phone device 8.1 in the User Portal is supported.
- Select Windows as the device platform.
- Reprovisioning the device is not supported. To re-provision the device, first retire the device, then re-register.
- Device registration fails if the device user enters a password that contains special characters. Only ASCII characters are supported in the password field.
- **Force Device Check-In** may not be available for a few minutes after the Windows Phone 8.1 device registers. If you try to retire the device during this time, it may take up to 24 hours to retire the device.
- Core certificates pushed to Windows 8.1 Phone devices are now always stored on the device TPM chip. This provides additional security to the certificate key.
- Autodiscovery is not required. We recommend autodiscovery for a seamless registration experience.
- A Subject Alternative Name (SAN) SSL certificate from a trusted Certificate Authority (CA), such as Verisign or GoDaddy, is required.
- Device registration from the Admin Portal or User Portal is not supported. Users can register only from their device.
- Pin-based registration is supported in Windows Phone 8.1 devices.
- The following registration statuses are supported:
 - **Verified:** After the device registers and before the first check in.
 - **Active:** The device has successfully synced with Core.
 - **Retired:** The Retire action was successfully applied.
 - **Pending:** The user's device has been registered on the Core Server, but downloading Apps@Work has not yet been completed.

Registration considerations: mutual authentication

Do not revert to earlier versions of Core using a snapshot after enabling mutual authentication. Doing so may necessitate re-enrolling devices.



Using Policies

This chapter includes the following sections:

- [Policy overview](#)
- [Working with policies](#)
- [Using default policies](#)

Refer to the *Core Device Management Guide for Android and Android Enterprise Devices* for advanced policy topics, such as those shown in "[Policy topics per operating system](#)" below.

TABLE 21. POLICY TOPICS PER OPERATING SYSTEM

Policy topic	OS
Notifications of changes to the privacy policy	All
<ul style="list-style-type: none">• Working with Android Quick Setup policies• Working with Samsung general policies	Android
<ul style="list-style-type: none">• Single-app mode policies• Global HTTP proxy policies• Cellular policies• Wallpaper policies• Customizing a home screen layout• Customizing a lock screen message• Configuring notification settings	iOS
Working with Windows Update policies	Windows
Compliance policies	Android, iOS, tvOS
AppConnect and AppTunnel	Android, iOS

TABLE 21. POLICY TOPICS PER OPERATING SYSTEM (CONT.)

Policy topic	OS
	For information about AppConnect and AppTunnel, including related policies and configurations, refer to the <i>AppConnect for Core Guide</i> .

 Some features are not applicable if you use MAM-only iOS or Android devices. For more information, see “Managing apps on MAM-only devices” in the *Core Apps@Work Guide*.

Policy overview

Core uses policies to regulate the behavior of the devices it manages. Each policy consists of a set of rules. Core groups the policies in the following categories:

- [Security policies](#)
- [Privacy policies](#)
- [Lockdown policies](#)
- [Sync policies](#)

 For information about the AppConnect global policy, see the **AppConnect for Core Guide**.

Core provides a set of default policies that you can use with little or no configuration. You can modify default policies, but you cannot delete them. You can distribute a policy to devices by applying a policy to a label. Core then pushes the policy to the devices assigned to that label the next time the devices sync with Core.

You can also create your own customized policies to replace or enhance the default policies included with Core. You can edit custom policies, but, unlike default policies, you can delete custom policies from Core. You apply custom policies to a label to distribute them to devices. Default policies do not require label assignment.

Core allows you to apply a label to multiple policies of a given category. For example, you can assign two custom security policies to the same label. However, Core only uses one security policy per device. This means that you need to prioritize the use of custom policies if you distribute to devices more than one policy of a given category.

Policy prioritization allows you to specify which policy should be used first if you have more than one policy of a given type associated with a label. For example, if you create two custom security policies, and apply the iOS label to both custom policies, you can configure custom security policy A to take precedence over custom security policy B.

Working with policies

You can create multiple policies for each policy type, but only one active policy of each type can be applied to a specific device. Use the **Policies** page to specify and control aspects of enterprise device behavior. To distribute the policy to devices, apply your policy to the relevant labels.

This section includes the following topics:

Accessing the Policies page

You can create multiple policies for each policy type, but only one active policy of each type can be applied to a specific device. Use the **Policies** page to specify and control aspects of enterprise device behavior.

Users must have one of the following roles to access the **Policies** page:

- View policies
- Apply and remove policy label
- Manage policy

Procedure

1. From the Admin Portal, go to **Policies & Configs > Policies**.
2. Refer to the [Policy page table](#) table for details.

Policy page table

The following table summarizes fields and descriptions in the **Policies** window.

TABLE 22. POLICIES PAGE TABLE

Fields	Description
Policy Name	Identifier for this policy. The policy name must be unique for policies of the same type.
Priority	Priority set for this policy in relation to other policies of the same type.

TABLE 22. POLICIES PAGE TABLE (CONT.)

Fields	Description
Status	Current status of this policy. The status can be Active or Inactive.
Description	Additional information about the policy that you entered when you created the policy.
Type	Which policy category this policy belongs to.
Last Modified	The date and time of the last change made to this policy.
# Phones	The number of devices affected by this policy. Click the link to display a list of the devices.
Labels	The labels applied to this policy.
WatchList	Exception: Backup & Restore policies are not distributed to the Mobile@Work client app. In this case, the WatchList column indicates the devices that are awaiting backup. Displays the number of devices for which the policy is queued. Click the link to display a list of the devices.

Modifying an existing policy

You can edit an existing default or custom policy in the Admin Portal.



When changing a policy, devices with the changed policy applied may prompt users to restart their devices.

Procedure

1. From the Admin Portal, go to **Policies & Configs > Policies**.
2. Click a policy in the **Policy Name** column to open the Policy Details pane on the right of the window.
3. Click the **Edit** button to open the **Modify Policy** window for the policy type you selected.

4. Refer to following sections as a guide for each policy type.
 - [Security policies](#)
 - [Privacy policies](#)
 - [Lockdown policies](#)
 - [Using default policies](#)
- AppConnect global policy: see the AppConnect for Core Guide for more information.
5. Click **Save**.



Policies do not take effect on any device until they are applied to a label. See [Applying policies to labels](#) for details.

Creating a custom policy

While you can edit the default policies provided by Core, you can also create your own custom security, privacy, lockdown, or sync policy.

Procedure

1. From the Admin Portal, go to **Policies & Configs > Policies**.
2. Click **Add New** and select a policy type you want to create.
3. Refer to following sections as a guide for each policy type.
 - [Security policies](#)
 - [Privacy policies](#)
 - [Lockdown policies](#)
 - [Using default policies](#)



See the AppConnect for Core Guide for more information regarding the AppConnect global policy.

4. Click **Save**.



Policies do not take effect on any device until they are applied to a label. See [Applying policies to labels](#) for details.

Prioritizing policies

When you create a custom policy, you can assign a priority relative to the other custom policies of the same type. This priority determines which policy is applied if more than one policy is associated with a specific device. For example, if you create a security policy for executives and a security policy for Windows devices, then an executive with a Windows device would have two different possible policies applied. Because only one policy of a given type can be applied to a device, the priority defined for the policies determines which is applied.

You can manage priorities for individual policies, or you can use the **Modify Priority** screen to manage priorities for a policy type in a single screen.

To manage priorities in a single screen:

1. Go to **Policies & Configs > Policies**.
2. Select a type from the **Policy Type** drop-down.
3. Click **Modify Priority**. The **Modify Policy Priorities** dialog appears.
4. Drag and drop policies until they reflect the priorities you want to set, with highest priority of 1 appearing at the top of the list.
5. Click **Save**.

Displaying custom policies for a selected label

To display a list of the policies associated with a specific label:

1. Go to a policies page under **Policies & Configs**.
2. Select a label from the **Labels** drop-down list.



Default policies are not included.

Displaying custom policies for a selected user

To display a list of the policies associated with a specific user:

1. Go to a policies page under **Policies & Configs**.
2. In **Search by User**, enter any portion of the user's first name, last name, or user ID and click the search icon. Policies assigned to user records matching the entered criteria are displayed.



Default policies are included. See [Using default policies](#).

Deleting a policy

When you delete a policy, all devices to which that policy were applied are updated with the default version of that policy. You cannot delete a default policy.

Procedure

1. From the Admin Portal, go to **Policies & Configs > Policies**.
2. Click one of the filters under the **Policies & Configs** tab to display the policy you want to delete.
3. Select the check box for the policy you want to delete.
4. Click **Delete** in the upper left.

Applying policies to labels

Use labels to apply policies to devices.

Procedure

1. Log into the Admin Portal.
2. Select **Policies & Configs > Policies**.
3. Click a policy in the **Policy Name** column to display the policies you want to work with.
4. Select the check box next to the policy.

You can search by policy name or description to help find the policy or policies you want to apply.

5. Click **More Actions > Apply To Label**.

6. Select the label.

You can search by label name or description to help find the label.

7. Click **Apply**.

Removing policies from labels

You can remove a policy from a label when you no longer want changes to that policy to affect devices having a given label.

Procedure

1. From the Admin Portal, select **Policies & Configs > Policies**.
2. Click a policy in the **Policy Name** column to display the policies you want to work with.
3. Select the check box next to the policy.
4. Click **More Actions > Remove From Label**.
5. Select the label.
6. Click **Remove**.

Using default policies

Default policies are the policies applied to a device automatically when it is registered. Default policy values are also used as a starting point when you create a custom policy. Core provides the values for each default policy specification. It is recommended that you create your own policies. You can use the settings in the default policies as a starting point. If you do edit a default policy's values (not recommended), those new values become the starting point when you create a new custom policy.

A device can have only one policy of each type.

Core provides defaults for the following policy types:

- [Security policies](#)
- [Privacy policies](#)
- [Lockdown policies](#)
- [Sync policies](#)

You cannot delete default policies.

For information about AppConnect global policy, refer to the *AppConnect for Core Guide*.

Security policies

Security policies specify how Core addresses several areas of mobile security. Use the following guidelines to create or edit a Security policy. We recommend you create separate policies for each platform to avoid inconsistencies.



Access control for macOS devices does not control email.

The following table summarizes fields and descriptions in the **Security Policy** window.

TABLE 23. SECURITY POLICY FIELDS

Item	Description	Default Policy Setting
Name	<p>Required. Enter a descriptive name for this policy. This is the text that will be displayed to identify this policy throughout the Admin Portal. This name must be unique within this policy type.</p> <hr/> <p> Though using the same name for different policy types is allowed (e.g., Executive), consider keeping the names unique to ensure clearer log entries.</p> <hr/>	Default Security Policy
Status	<p>Select Active to turn on this policy. Select Inactive to turn off this policy.</p> <hr/> <p> Use the Status feature to turn a policy on or off across all phones affected by it. The policy definition is preserved in case you want to turn it on again.</p> <hr/>	Active
Priority	<p>Specifies the priority of this custom policy relative to the other custom policies of the same type. This priority determines which policy is applied if more than one policy is associated with a specific device. Select "Higher than" or "Lower than", then select an existing policy from the drop-down list. For example, to give Policy A a higher priority than Policy B, you would select "Higher than" and "Policy B." Because this priority applies only to custom policies, this field is not enabled when you create the first custom policy of a given type.</p>	
Description	Enter an explanation of the purpose of this policy.	Default Security Policy
Password fields		
Password	<p>Select Mandatory to specify that the user must enter a password before being able to access the device. Otherwise, select Optional, which allows the user to determine whether the password will be set.</p>	Optional

TABLE 23. SECURITY POLICY FIELDS (CONT.)

Item	Description	Default Policy Setting
	<p data-bbox="537 415 586 478"> If you intend to use the Lock feature in case the phone is lost or stolen, then a password must be set on the phone. Therefore, specifying a mandatory password is strongly advised.</p> <hr/> <p data-bbox="537 575 1235 730">For iOS, tvOS, and macOS devices: Select Mandatory to specify that the device user must comply with the password policy when resetting the password for the device. This does not force a user to change an existing password.</p> <p data-bbox="537 764 1230 995">For iOS devices: If a security policy is edited and the Password field is set to Optional, then the security policy will not be pushed to devices. This results in an inaccurate count in your WatchList on the Policies & Configurations > Policies page. Ivanti recommends you have the Password field set to Mandatory.</p>	
Password Type	<p data-bbox="537 1020 1057 1052">Specify general restrictions for the password:</p> <p data-bbox="537 1066 1219 1178">Simple: Determines whether a simple password is allowed. A simple password can contain repeated characters, or ascending/descending characters, for example 123 or CBA.</p> <p data-bbox="537 1192 1219 1262">Alphanumeric: Requires passwords to include at least one letter and one number.</p> <p data-bbox="537 1276 1214 1472">For iOS, tvOS, and macOS: If you select both Simple and Alphanumeric, then passwords can include repeating and/or ascending/descending characters. If you select Alphanumeric only, then passwords may not include repeating and/or ascending/descending characters.</p> <p data-bbox="537 1486 1214 1556">Don't Care: Applies the default requirements specified by the device OS. This option is not supported on iOS.</p> <hr/> <p data-bbox="537 1612 1170 1682"> If no check box is selected, the Password Type defaults to Don't Care.</p>	Don't Care

TABLE 23. SECURITY POLICY FIELDS (CONT.)

Item	Description	Default Policy Setting
	<p>For Android 12: Android 12 devices in Work Profile mode do not support password type and password length. As a result, they are reported in Core as "Unsupported."</p> <p>For Windows Phone 8.1 devices: The Don't Care option requires that the password is either simple or alphanumeric. To allow the use of a PIN, but not a simple password such as 1234 or 1111, select the Don't allow simple password option.</p> <p>For Windows 10 Mobile devices: This feature is not supported. Use Minimum Number of Complex Characters to make changes to these keyboards.</p>	
Complex PIN (Android only)	<p>For Android devices only:</p> <p>Select On to prohibit the device user from using ordered or repeating digits in a PIN.</p> <p>This option is enabled only if:</p> <ul style="list-style-type: none"> • the password is mandatory • the password type is simple only <p>Examples of ordered digits: 1234, 2468, 9876</p> <p>Example of repeating digits: 4444</p> <p>This feature requires Android 6.0 and supported newer versions. Devices running earlier versions behave as if this option is set to Off.</p>	Off
Minimum Password Length	<p>Enter a number between 1 and 16 to specify the minimum length for the password. Leave this setting blank to specify no minimum.</p> <p>Note the following:</p> <ul style="list-style-type: none"> • For Android devices: When the Don't Care option is set for the Password Type field, the Minimum Password Length field does not apply. 	6

TABLE 23. SECURITY POLICY FIELDS (CONT.)

Item	Description	Default Policy Setting
	<ul style="list-style-type: none"> For Android 12: Android 12 devices in Work Profile mode do not support password type and password length. As a result, they are reported in Core as "Unsupported." 	
Maximum Inactivity Timeout	<p>Select the maximum amount of time to allow as an inactivity timeout. To disable this feature, select Never. The user can then specify up to this value as the interval after which the screen locks.</p> <p>For macOS: Enter the maximum timeout interval that the device user can set for the device before the screen saver engages.</p> <p>For iOS and tvOS: The Grace Period for Device Lock option determines whether the user must enter a password to unlock the screen. Also consider the case when the maximum inactivity timeout that you specify is greater than the maximum inactivity timeout that the device supports. In this case, the inactivity timeout that the user can specify is limited by the device's maximum inactivity timeout.</p> <p>For Windows Phone 8.1 and Windows 10 Mobile devices: If the Maximum Inactivity Timeout is set to one minute, the device uses the timeout set on the device.</p>	30 minutes
Minimum Number of Complex Characters	<p>Specify the minimum number of special characters that must be included in a password.</p> <p>For Windows Phone 8.1 devices: Specify the minimum level of complexity, 1 to 4, required in a password. The values indicate the minimum number of character types required. The character types are lowercase, uppercase, numbers, and non-alphanumeric.</p> <p>For Windows 10 Mobile devices: The complexity will determine what type of password and keypad the user sees.</p> <p>1 - Digits only (the default) 2 - Digits and lowercase letters are required 3 - Digits, lowercase letters, and uppercase letters are required 4 - Digits, lowercase letters, uppercase letters, and special characters are required.</p>	0

TABLE 23. SECURITY POLICY FIELDS (CONT.)

Item	Description	Default Policy Setting
	For Windows 10 Desktop devices: This feature is not supported.	
Maximum Password Age	<p>For Windows Phone 8.1 devices: This feature is not supported.</p> <p>For Windows 10 devices: Specifies when the password expires (in days).</p> <hr/> <p> This policy must be wrapped in an Atomic command.</p> <hr/> <p>Supported values are listed below:</p> <ul style="list-style-type: none"> • An integer X where $0 \leq X \leq 730$. • 0 (default) - Passwords do not expire. <p>If all policy values = 0 then 0; otherwise, Min policy value is the most secure value.</p> <p>For iOS, macOS, tvOS, and Android: Specify the numbers of days after which the password will expire. 0 indicates no limit.</p> <hr/> <p> Mobile@Work 10.1.0.0 for Android and higher supported releases provides the device user a notification when the password is going to expire within the next 7 days.</p> <hr/> <p>For more information, see "Setting an alert that a device's PIN change request was skipped" in <i>Core Device Management Guide for Android and Android Enterprise Devices</i>.</p>	0
Maximum Number of Failed Attempts	<p>This feature does not apply to Windows devices.</p> <p>Specify the maximum number of times the user can enter an incorrect password before the device is wiped. 0 indicates no limit.</p>	0 (no limit)

TABLE 23. SECURITY POLICY FIELDS (CONT.)

Item	Description	Default Policy Setting																								
	<p>For Android and Android Enterprise devices: When set to zero, unlimited passcode failures are allowed. When set to anything greater than zero only the number of consecutive failures specified are allowed.</p> <p>For iOS and tvOS: When set to a maximum number of 3 or less, the device imposes a time delay before a passcode can be entered again. The time delay increases with each failed attempt, as shown in the following table.</p> <table border="1" data-bbox="597 705 1170 1123"> <thead> <tr> <th>Failed attempt</th> <th>Wait time (minutes)</th> <th>Total added wait time (minutes)</th> </tr> </thead> <tbody> <tr> <td>1-5</td> <td>None</td> <td>None</td> </tr> <tr> <td>6</td> <td>1</td> <td>1</td> </tr> <tr> <td>7</td> <td>5</td> <td>6</td> </tr> <tr> <td>8</td> <td>15</td> <td>21</td> </tr> <tr> <td>9</td> <td>60</td> <td>81</td> </tr> <tr> <td>10</td> <td>60</td> <td>141</td> </tr> <tr> <td>11</td> <td>Black screen</td> <td>Device initiates wipe</td> </tr> </tbody> </table> <p>For example, if the device user has failed to enter the correct password for the 7th time, a wait time of 5 minutes is imposed, for a total wait time of 6 minutes, even when the maximum number of failed attempts has been set to 3.</p> <p>When set to 4 or above, devices that can no longer be disabled by users are wiped when entering the fifth incorrect passcode. There is no wait time in this case.</p> <p>When set to 3 or less, and enabling the iOS or tvOS setting to erase the device after too many failed passcode attempts (under Settings > Touch ID & Passcode > Erase Data in iOS), the device is wiped when entering the 11th failed passcode.</p>	Failed attempt	Wait time (minutes)	Total added wait time (minutes)	1-5	None	None	6	1	1	7	5	6	8	15	21	9	60	81	10	60	141	11	Black screen	Device initiates wipe	
Failed attempt	Wait time (minutes)	Total added wait time (minutes)																								
1-5	None	None																								
6	1	1																								
7	5	6																								
8	15	21																								
9	60	81																								
10	60	141																								
11	Black screen	Device initiates wipe																								

TABLE 23. SECURITY POLICY FIELDS (CONT.)

Item	Description	Default Policy Setting
	<p> If there is no passcode set on the device, data protection is disabled by default. This is as per Apple design.</p>	
Password History	<p>For Android, iOS, tvOS, and macOS devices:</p> <p>Specify the number of passwords remembered to ensure that users define a different password.</p> <p>For example, if you want to prevent users from repeating a password for the next four password changes, enter 4.</p>	0
Maximum Number of Failed Attempts	<p>If this is set as 1, the user is not prompted to enter the device password.</p> <p>This feature specifies the number of authentication failures allowed before the device will be wiped. A value of 0 disables device wipe functionality.</p> <hr/> <p> This policy must be wrapped in an Atomic command.</p> <hr/> <p>Prior to reaching the failed attempts limit, the user is sent to the lock screen and warned that more failed attempts will lock their computer. When the user reaches the limit, the device automatically reboots and shows the BitLocker recovery page. This page prompts the user for the BitLocker recovery key.</p> <p>The following list shows the supported values:</p> <ul style="list-style-type: none"> • An integer X where $4 \leq X \leq 16$ for desktop and $0 \leq X \leq 999$ for mobile devices. • 0 (default) - The device is never wiped after an incorrect PIN or password is entered. <p>The most secure value is 0 if all policy values = 0; otherwise, Min policy value is the most secure value.</p>	

TABLE 23. SECURITY POLICY FIELDS (CONT.)

Item	Description	Default Policy Setting
Maximum Number of Failed Attempts	For Windows 10 Mobile devices: When a user reaches the value set by this policy, the device is wiped.	
Maximum Number of Failed Attempts	For Windows 10 Desktop devices: When a user reaches the value set by this policy, it is not wiped, but put on BitLocker recovery mode, which makes the data inaccessible but recoverable. If BitLocker is not enabled, then the policy cannot be enforced.	
Password History	<p>For Windows Phone 8.1 devices: This feature is not supported.</p> <p>For Windows 10 devices: This feature specifies how many passwords can be stored in the history that cannot be used.</p> <hr/> <p> This policy must be wrapped in an Atomic command.</p> <hr/> <p>Supported values are listed below:</p> <ul style="list-style-type: none"> • An integer X where $0 \leq X \leq 50$. • 0 (default) <p>The value includes the user's current password. A setting of 1 indicates users cannot reuse their current password when choosing a new password and a setting of 5 indicates users cannot set their new password to their current password or their previous four passwords.</p> <p>The Max policy value is the most restricted.</p>	
Grace Period for Device Lock	<p>For macOS only: Specify the maximum amount of time the device can be on the screen saver without prompting for a passcode on wake from the screen saver.</p> <p>For iOS and tvOS only: Specify the interval after the device locks during which the user can unlock the device without entering a passcode.</p>	None
<p>Data Encryption These features are not supported on iOS or macOS devices.</p>		

TABLE 23. SECURITY POLICY FIELDS (CONT.)

Item	Description	Default Policy Setting
Device Encryption	<p>For Android Samsung Knox: Select On to turn on encryption. Otherwise, select Off.</p> <hr/> <p> If Device Encryption is turned on, then the Password option is automatically set to Mandatory.</p> <hr/> <p>For Windows: Setting encryption is supported for Windows Phone 8.1 and Windows 10 Mobile devices. Setting encryption is not supported for Windows 10 Desktop devices, however, encryption can be enabled by setting it manually on the device.</p> <p>Once encryption has been set, looking up encryption is supported for all Windows devices.</p> <p>If Device Encryption is turned on, it cannot be turned off. You must reset the device to factory settings to turn off device encryption.</p>	Off
Data Type	For Android devices only: Indicates the data type.	none selected
File Types	For Android devices only: Indicates the file type.	none specified
SD Card Encryption	<p>Android Samsung Knox and LG devices only: Select On to enforce SD card encryption. Otherwise, select Off.</p> <p>Supported only with Android 7.0 through the most recently released version as supported by MobileIron.</p> <p>Supported on LG devices only with Mobile@Work 9.7 for Android through the most recently released version as supported by MobileIron.</p> <p>Apply to Samsung managed devices</p> <p>Select to apply SD card encryption to Samsung Work Managed Devices or Managed Device with Work Profile (COPE) mode on Android devices versions 8-10.</p>	Off
Device Log Encryption	<p>Select On to turn on device log encryption. Otherwise, select Off.</p> <p>See "Device log encryption" in the Device Management Guide for Android Devices.</p>	Off

TABLE 23. SECURITY POLICY FIELDS (CONT.)

Item	Description	Default Policy Setting
For details on all Windows 10 Desktop options, see the Bridge chapter in the <i>Core Device Management Guide for Windows Devices</i> .		
Android (For Android only)		
Require strict TLS for Apps@Work (Android only)	For Android devices only: Select this check box so that Mobile@Work will require strict TLS between Apps@Work and other services, for all devices with this Security policy applied. The device will no longer allow you to use http:// links for override URLs in Apps@Work.	Not selected
Common Criteria Mode (Samsung Knox and LG only)	For Android 7.0 devices and supported newer versions: This feature is not commonly used. For customers that require this mode, select this check box to put a Samsung Knox or LG device in Common Criteria mode. For Samsung Knox devices, selecting this option requires a Knox license and the Samsung General policy needs to be enabled. Apply to Samsung Managed devices This feature is not commonly used. For customers that require this mode, select this check box to put a Samsung managed device in Common Criteria mode. This option is supported only on Android 7.0 and supported newer versions.	Not selected
Block SmartLock (from Android 6.0 only)	For Android devices only: Select this option to prohibit the device user from using the Smart Lock feature on the device. Selecting this option causes the Block Smart Lock Options to display. You must select at least one of the Block Smart Lock Options . The impact of selecting this option depends on the Android version and Mobile@Work version on the device:	Not selected

TABLE 23. SECURITY POLICY FIELDS (CONT.)

Item	Description	Default Policy Setting
	<ul style="list-style-type: none"> With Android 6.0 and Mobile@Work 10.1.0.0 and supported newer versions: Your selections of the individual Block Smart Lock Options are applied. Selecting Block SmartLock blocks all types of Smart Locks, regardless of your selections of the individual Block Smart Lock Options. <hr/> <p> This security policy setting overrides the Lockscreen Widgets setting in the lockdown policy.</p> <hr/>	
Block Smart Lock Options (from Android 6.0)	<p>These fields appear only if you have selected Block Smart Lock (from Android 6.0 only). You must select at least one of these options.</p> <p>Support for each of these options vary across device models. Selecting an option has no impact on devices that do not support the option.</p>	
Block Bluetooth	<p>This field appears only if you have selected Block Smart Lock (from Android 6.0 only)</p> <p>Select to not allow unlocking a device because it is connected to a trusted device using Bluetooth.</p> <hr/> <p> Some device models combine Bluetooth and NFC into trusted devices.</p> <hr/>	Not selected
Block NFC	<p>This field appears only if you have selected Block Smart Lock (from Android 6.0 only)</p> <p>Select to not allow unlocking a device because it is connected to a trusted device using NFC (near-field communication).</p> <hr/> <p> Some device models combine Bluetooth and NFC into trusted devices.</p> <hr/>	Not selected

TABLE 23. SECURITY POLICY FIELDS (CONT.)

Item	Description	Default Policy Setting
Block Places (Location)	This field appears only if you have selected Block Smart Lock (from Android 6.0 only) Select to not allow unlocking a device because of its location, also known as a "trusted place".	Not selected
Block Face	This field appears only if you have selected Block Smart Lock (from Android 6.0 only) Select to not allow unlocking a device because it recognizes the user's face, also known as a "trusted face".	Not selected
Block On-body	This field appears only if you have selected Block Smart Lock (from Android 6.0 only) Select to not allow unlocking a device because the user is carrying it in their hand, pocket, or bag.	Not selected
Block Voice	This field appears only if you have selected Block Smart Lock (from Android 6.0 only) Select to not allow unlocking a device because it recognizes the user's voice.	Not selected
Block Fingerprint (from Android 6.0 or Samsung MDM 5.3)	<p>For Android devices only: Select this option to prohibit the device user from using a fingerprint to access the device. This feature requires the following on the device:</p> <ul style="list-style-type: none"> • Android 6.0 and supported newer versions • On Samsung devices, Samsung MDM 5.3 through the most recently released versions supported by MobileIron. • Fingerprint hardware <p>This setting has no impact on devices that do not meet the listed requirements; fingerprint is allowed, if available.</p> <hr/> <p> This security policy setting overrides the LockscreenWidgets setting in the lockdown policy.</p>	Not selected

TABLE 23. SECURITY POLICY FIELDS (CONT.)

Item	Description	Default Policy Setting
Block Iris Scan (Samsung and Android 9.0)	<p>For Android devices only:</p> <p>Select this option to prohibit the device user from using iris scanning to unlock the device. This option requires that the device is:</p> <ul style="list-style-type: none"> • A Samsung device with the iris scanning feature. • A Samsung device running Samsung OS 7.0 through the most recently released version as supported by MobileIron. • A non-Samsung device running Android 9.0 through the most recently released version as supported by MobileIron. • Running Mobile@Work 10.1 through the most recently released version as supported by MobileIron. <p>This setting has no impact on other devices.</p> <hr/> <p> This security policy setting overrides the Lockscreen Widgets setting in the lockdown policy.</p>	Not selected
Block Face Unlock (Samsung and Android 9.0)	<p>For Android devices only:</p> <p>Select this option to prohibit the device user from using face recognition to unlock the device. This option requires that the device is:</p> <ul style="list-style-type: none"> • A Samsung device with the face unlock feature • A Samsung device running Samsung OS 7.0 through the most recently released version as supported by MobileIron. • A non-Samsung device running Android 9.0 through the most recently released version as supported by MobileIron. • Running Mobile@Work 10.1 through the most recently released version as supported by MobileIron. 	Not selected

TABLE 23. SECURITY POLICY FIELDS (CONT.)

Item	Description	Default Policy Setting
	<p>This setting has no impact on other devices.</p> <hr/>  This security policy setting overrides the Lockscreen Widgets setting in the lockdown policy.	
Require Google SafetyNet Attestation	For Android devices only: Select this option to perform SafetyNet attestation on devices. See "Enabling SafetyNet attestation on Android devices" in the <i>Core Device Management Guide for Android and Android Enterprise Devices</i> .	Not selected
Block notifications on lock screen	Android Enterprise managed device profile only: Select this option to prevent notifications from being displayed on the device lock screen. Applies to Managed Device with Work Profile (COPE) mode on Android devices versions 8-10.	Not selected
Allow only redacted notifications on lock screen	Android Enterprise work profile only: This option will redact notifications shown on the lock screen hiding the notification contents. Block notifications on lock screen does not affect this. Applies to Managed Device with Work Profile (COPE) mode on Android devices versions 8-10.	Not selected
Windows Phone 8.1	(For Windows Phone 8.1 devices only.)	
Firewall	This is available on all Windows-supported devices.	On
Anti-Virus	This is available on all Windows-supported devices.	On
Auto-Update	This is available on all Windows-supported devices.	On
Windows 10	(For Windows 10 devices only.)	
Defender Real-time Protection	This setting is turned on by default. Once a user turns it off it can only be turned back on by an administrator.	On
DHA On-premises URL	Device Health Attestation (DHA) is used to increase device monitoring for those systems (such as government agencies) that need the information. DHA also takes a passive approach to the data, allowing administrators to decide how they want to handle compliance.	Off

TABLE 23. SECURITY POLICY FIELDS (CONT.)

Item	Description	Default Policy Setting
	<p>Turning on this feature begins the collection of data, which is sent to Microsoft Cloud DHA or on-prem servers. To use an on-premises server, go to the Admin Portal > Policies & Configs > Policies > select a security policy > Edit > Windows 10 > DHA On-premises URL.</p> <hr/> <p> Only Microsoft Server 2016 can be used as DHAs.</p> <hr/> <p>Once collected and reported back the MobileIron, the information displays on individual Device Details pages on a per-device basis.</p> <p>Administrators can use this information to determine if a device should be wiped or looked at for other security reasons.</p>	
Access Control		
<p>For the following options, select the compliance action you want to apply to devices that trigger access control. For detailed information on the impact that compliance actions have on devices, see "Compliance actions for security policy violations" in the <i>Core Device Management Guide</i> for your operating system.</p>		
For All Platforms		
<p>Apply compliance action when a device has not connected to Core in x days</p>	<p>Select the compliance action you want to apply if a device has not connected to Core in the specified number of days.</p> <p>For iOS devices: All compliance actions are supported if MDM is enabled, except for those related to Android devices, When Data Encryption is disabled, and Application Restrictions. Core only checks whether MDM policies are out of date.</p> <p>For macOS devices: You can send an alert and quarantine the device.</p> <p>For Android devices: Only the following compliance actions are supported:</p> <ul style="list-style-type: none"> • Sending alert 	

TABLE 23. SECURITY POLICY FIELDS (CONT.)

Item	Description	Default Policy Setting
	<ul style="list-style-type: none"> • Blocking email access if you are using a Standalone Sentry for email access. • Blocking app tunnels. <p>For Windows devices: Only the following compliance actions are supported:</p> <ul style="list-style-type: none"> • Sending alert • Blocking email access if you are using a Standalone Sentry for email access. • Supported custom compliance actions. 	
Apply compliance action when a policy has been out of date for x days	<p>Select the compliance action you want to apply if a device has not met policy requirements for the specified number of days.</p> <p>For iOS devices: All compliance actions are supported.</p> <p>For macOS devices: You can send an alert and quarantine the device.</p> <p>For Android devices: Supports only the following compliance actions:</p> <ul style="list-style-type: none"> • Sending alert • Blocking email access if you are using a Standalone Sentry for email access. • Blocking app tunnels. <p>For Windows devices: Supports only the following compliance actions:</p> <ul style="list-style-type: none"> • Sending alert • Blocking email access if you are using a Standalone Sentry for email access. • Supported custom compliance actions. 	

TABLE 23. SECURITY POLICY FIELDS (CONT.)

Item	Description	Default Policy Setting
Apply compliance action when a device violates the following App Control rules	Select the compliance action you want to apply when a device violates the specified App Control rules. See the <i>Core Apps@Work Guide</i> .	
iOS and tvOS devices		
For iOS devices only		
Apply compliance action when iOS version is less than	Select the compliance action you want to apply when Core detects an iOS device having a version number less than the specified version.	
Apply compliance action when Data Protection is disabled	Select the compliance action you want to apply when Core detects an iOS device that has the Data Protection feature disabled.	
Apply compliance action when a compromised iOS device is detected	<p>Select the compliance action you want to apply when Core detects an iOS device that has been modified to circumvent manufacturer restrictions.</p> <p>In Mobile@Work, if the compliance action specifies Enforce compliance actions locally on devices, the following compliance actions, if selected, are enforced on the device without connecting to Core:</p> <ul style="list-style-type: none"> • Alert the device user with a banner or notification. • Block AppConnect apps. • The device user becomes unauthorized to use AppConnect apps. • Retire AppConnect apps. • The device user becomes unauthorized to use AppConnect apps and the apps' secure data is deleted. <p>All other compliance actions require the device to be connected with Core.</p>	

TABLE 23. SECURITY POLICY FIELDS (CONT.)

Item	Description	Default Policy Setting
Apply compliance action for the following disallowed devices	Select the compliance action you want to apply when Core detects a specified iOS device, such as AppleTV or iPad 2.	
Apply compliance action when device MDM is deactivated (iOS 5 or higher)	Select the compliance action you want to apply when Core detects that the MDM profile has been removed from the device.	
Enable Activation Lock (Supervised iOS 7 and later devices only)	Select to enable the activation lock feature. See the section "Managing the Activation Lock for iOS devices" in the <i>Core Device Management Guide for iOS and macOS Devices</i> .	
Only join Wi-Fi networks installed by profiles (iOS 10.3 and later with supervised devices only)	Enabling this option filters the Wi-Fi network choices that devices can join to only include the Wi-Fi networks installed by profiles. Toggling the value of this option causes Core to push the Wi-Fi configurations to any devices with this security policy.	
macOS		
Apply compliance action when macOS version is less than	Select a compliance action to apply when the macOS version on the device is less than the version you select from the drop-down list.	
Apply compliance action when Full Disk Encryption (FileVault) is disabled	Select a compliance action to apply when full disk encryption (FileVault) is disabled on the device.	
Apply compliance action when device MDM is deactivated	Select a compliance action to apply when the MDM (mobile device management) profile is deactivated on the device.	
For Android devices only		

TABLE 23. SECURITY POLICY FIELDS (CONT.)

Item	Description	Default Policy Setting
Apply compliance action when Android version is less than x	Select the compliance action you want to apply when Core detects an Android device having a version number less than the specified version.	
Apply compliance action when a compromised Android device is detected	Select the compliance action you want to apply when Core detects an Android device that has been “rooted,” that is, root access has been given to an app.	
Apply compliance action when Data Encryption is disabled	<p>Select the compliance action you want to apply when Core detects an Android device that has the Data Encryption feature disabled.</p> <hr/> <p> The quarantine action Remove All Configurations has no impact when data encryption is disabled.</p> <hr/>	
Apply compliance action when Samsung Knox device attestation fails	Select the compliance action you want to apply when Core detects that a Samsung Knox device has failed an attestation check.	
Apply compliance action when device administrator is deactivated	<p>Select the compliance action you want to apply when Core detects that the device administrator privilege has been removed from the Mobile@Work app.</p> <hr/> <p> The quarantine action Remove All Configurations has no impact when the device administrator is deactivated.</p> <hr/>	
Apply compliance action when USB debug is enabled	Select the compliance action you want to apply when Core detects that USB debugging was enabled.	
Bypass Factory Reset Protection	<p>Applies to Android Enterprise devices in “work managed” mode only.</p> <p>When enabled, Android’s Factory Reset Protection feature is bypassed, and factory reset devices will be unlocked.</p>	enabled

TABLE 23. SECURITY POLICY FIELDS (CONT.)

Item	Description	Default Policy Setting
	<p>When disabled, Android's Factory Reset Protection is active. A factory reset device will be locked and will require the owner's Google Account credentials before the device can be set up again.</p> <hr/> <p> No administrative code exists to unlock a factory reset device if bypass is disabled.</p> <hr/>	
For Windows devices only		
Apply compliance action when Windows version is less than x	Select the compliance action you want to apply when Core detects an Windows device having a version number less than the specified version.	
Don't allow simple password	Check this box to allow the use of a PIN, but not a simple password such as 1234 or 1111.	
Apply compliance action when Data Encryption is disabled	Select the compliance action you want to apply when Core detects a Windows Phone 8.1 device that has the Data Encryption feature disabled.	
Application Restrictions	For Windows devices, select the check box, then select the restriction from the drop-down list.	

Privacy policies

Note the following:

- Privacy policies are supported on Windows 10 devices.
- Privacy policies are **not** supported on macOS devices.
- Location and Apps privacy settings currently apply only to iOS devices.

Privacy policies specify which files to synchronize with Core and whether activity or content should be synchronized for each type of data. Privacy policies also specify which information the Mobile@Work app should include in its log.

To create a privacy policy, go to **Policies & Configs > Policies**. Click **Add New > Privacy**. Use the following guidelines to create or edit privacy policies:

The following table summarizes fields and descriptions in the **Privacy Policy** window.

TABLE 24. PRIVACY POLICY FIELDS

Item	Description	Default Policy Setting
Name	<p>Required. Enter a descriptive name for this policy. This is the text that will be displayed to identify this policy throughout the Admin Portal. This name must be unique within this policy type.</p> <p>Tip: Though using the same name for different policy types is allowed (e.g., Executive), consider keeping the names unique to ensure clearer log entries.</p>	Default Privacy Policy
Status	Select Active to turn on this policy. Select Inactive to turn off this policy.	Active
Priority	<p>Specifies the priority of this custom policy relative to the other custom policies of the same type. This priority determines which policy is applied if more than one policy is associated with a specific device. Select Higher than or Lower than, then select an existing policy from the drop-down list. For example, to give Policy A a higher priority than Policy B, you would select "Higher than" and "Policy B".</p> <p>Because this priority applies only to custom policies, this field is not enabled when you create the first custom policy of a given type.</p>	
Description	Enter an explanation of the purpose of this policy.	Default Privacy Policy
Apps	<p>All Apps: Instructs the device to return to the status of all the installed apps on devices with this policy.</p> <p>App Catalog apps: Instructs the device to return the installed status of only the apps in Apps@Work on devices with this policy. App Control rules are not applied.</p>	App Catalog Apps
SMS Log	<p>For Android devices only:</p> <p>Specify synchronization for SMS:</p>	None

TABLE 24. PRIVACY POLICY FIELDS (CONT.)

Item	Description	Default Policy Setting
	<p>Sync Content - Clear Text: Select to archive mobile data in Core.</p> <p>Sync Content - Encrypted: Select to archive the mobile data in encrypted format.</p> <p>None: Select to collect no SMS data.</p>	
Call Log	<p>For Android devices only:</p> <p>Specify synchronization for Call:</p> <p>Sync - Clear Text: Archive mobile data.</p> <p>Sync - Encrypted: Archive the same data in encrypted format.</p> <p>None: Do not collect Call statistics or store Call data.</p>	None
iOS Location-Based Wakeups	<p>For iOS devices only:</p> <p>iOS 6 and earlier devices use Significant Location Change for background wakeups. These wakeups impact jailbreak detection and updates to certain policies.</p> <p>The significant location change service provides a low-power way to get the current location of an iOS device and be notified when significant changes occur. This feature governs whether the OS can periodically bring Mobile@Work into memory.</p> <p>The following options are available:</p> <p>Enabled on iOS 6 and earlier: Recommended if you want to support devices running iOS 6 and earlier.</p> <p>Enabled: Select this only if you want to continue using SLC.</p> <p>Disabled: Select this only if you want to discontinue use of SLC, regardless of the device version. Selecting this option greatly reduces the likelihood that jailbreaks will be detected on devices that do not support silent APNS or are running Core Mobile@Work 6.0 and earlier supported releases.</p>	Disabled

TABLE 24. PRIVACY POLICY FIELDS (CONT.)

Item	Description	Default Policy Setting
	<p> On iOS 8, 8.1, and 8.1.1, disabling Location Services in the OS or in Mobile@Work may result in device users receiving a notification indicating that the current configuration requires enabling access to Location Services.</p> <hr/> <p>In Core, a setting in the Default Privacy Policy allows toggling location based wakeups on or off. If this setting is enabled, and a user disables Location Services or disallows Location Services for Mobile@Work, they will receive the notification. This notification does not mean that the device is out of compliance, rather, it indicates that Core has enabled location-based wake ups, which the device will be unable to perform.</p>	
Location	<p>Specify which location data, if any, is stored on Core.</p> <hr/> <p> The Sync Cell Tower option is only available to Android devices.</p> <hr/> <p>None: No location data is stored.</p> <p>Sync Cell Tower: Cell tower data is stored.</p> <p>Sync GPS if available: GPS data is stored.</p>	None
Collect Roaming Status	<p>When enabled, roaming information is collected from the device and roaming status displays in Device & Users > Devices on the Device Details panel.</p> <p>When disabled, Mobile@Work for Android does not report any roaming status to Core. Available in Mobile@Work for Android version 7.0 or later.</p>	Disabled
Enable Configuration Profiles	<p>Clear this setting if you do not want Core to send non-AppConnect-related configurations and certificates to MAM-only iOS devices, including the Apps@Work web clip and certificate.</p>	Enabled

TABLE 24. PRIVACY POLICY FIELDS (CONT.)

Item	Description	Default Policy Setting
	For more information, see "Configurations and certificates for MAM-only devices" in the <i>Core Apps@Work Guide</i> .	
Prompt User to Enable Location Services if Wi-Fi/MTD configuration is pushed (Android enterprise)	Administrators have the ability to prompt device users to enable the device's location setting and to do it silently based on the nature of the device user. This setting is useful if the device user resides in a EU country that has GDPR requirements. If this check box is selected, the device user is prompted to enable the location setting during the registration process. If the device user does not grant permission, the configuration will fail. To resolve this, the device user will need to manually enable the device's location setting, thus triggering a device check-in to get the Wi-Fi / MTD configurations installed onto the device. Applicable only for Work managed device (DO) mode and Managed device with Work profile mode on Android 10+ devices.	Disabled
Disable Auto-Grant Location Permissions for Work Profile Devices	<p>When this option is selected, a warning displays: Wi-Fi and MTD configurations can partially fail on older Android versions and device will fail to be located if user denies permission.</p> <p>Note the following:</p> <ul style="list-style-type: none"> • If the Privacy Policy > Disable Auto-Grant Location Permissions for Work Profile Devices field is de-selected, then the client will auto-grant Location Permissions, irrespective of configuration being pushed. • If the Privacy Policy > Disable Auto-Grant Location Permissions for Work Profile Devices field is selected, then the client will not auto-grant Location Permissions. The client will only seek Location Permissions if it detects configurations that require Location Permissions. • Depending upon server-wide settings, Location Permissions is auto-granted for Android 10 and 11 devices to use for Wi-Fi and MTD configuration. Additionally, the administrator may want to locate a device on-demand. 	Disabled

TABLE 24. PRIVACY POLICY FIELDS (CONT.)

Item	Description	Default Policy Setting
	Not applicable to Android 12 devices.	
<i>App Filters</i>	For iOS apps only	
iOS Installed App Inventory	<p>All Apps: Instructs devices to report to Core the apps installed to devices.</p> <hr/> <p> Select All Apps: if you are converting unmanaged apps to managed apps. See Core Apps@Work Guide.</p> <hr/> <p>Managed Apps Only (iOS 7 and later): Instructs devices to report to Core the managed apps installed to devices. For devices running iOS 7 through the most recently released version of iOS as supported by MobileIron.</p> <p>Specified Apps Only (iOS 7 and later): Instructs devices to report to Core the status of installed apps and managed apps whose bundle identifiers you specify here. For devices running iOS 7 through the most recently released version of iOS as supported by MobileIron.</p> <p>See the <i>Core Apps@Work Guide</i> for information about managed apps.</p>	Managed Apps Only (iOS 7 and later)
<i>Windows 10 Inventory</i>	This feature is supported by Windows 10 devices only.	
App Store Inventory	Displays all the App Store apps installed on the device. The options are Enable and Disable	Disable
Non Store Inventory	Displays all the Non Store apps installed on the device. The options are Enable and Disable	Disable
System Inventory	Displays all the System Inventory apps installed on the device. The options are Enable and Disable	Disable
Win 32 Inventory	Displays all the Win 32 Inventory apps installed on the device. The options are Enable and Disable	Disable

TABLE 24. PRIVACY POLICY FIELDS (CONT.)

Item	Description	Default Policy Setting
	 For Windows 10 devices with more than 100 apps, the App inventory is updated in the database.	
<i>Android Warning Banner on the Device Reboot</i>		
Enable Warning Banner	<p>For Android devices only:</p> <p>Administrators can add a warning banner that displays upon device reboot. This is helpful for companies that require all approved mobile operating systems, such as Android 9.0, to be managed according to a security baseline / guidance. Device users will see the warning banner upon device reboot and will have to acknowledge it before continuing use of the device.</p> <p>This feature is applicable only to:</p> <ul style="list-style-type: none"> • Samsung devices with Samsung Knox API 2.2 • Samsung devices in Work Managed Device mode • Samsung devices in Work Profile on Company Owned Device mode <p>Procedure</p> <ol style="list-style-type: none"> 1. Select the Enable Warning Banner check box. A text box displays. 2. Enter the text that you want to appear on the device. 3. Click Save. The default policy will be applied to all smart phones and labels to which no other policy has been applied. 	Unchecked

Lockdown policies

 Lockdown policies do not apply to iOS or macOS devices.

Lockdown policies specify which features should be disabled in the event that device access must be restricted. To create a lockdown policy, go to **Policies & Configs > Policies > Add New > Lockdown**. Some policy changes can prompt users to restart their device after the policy is applied to the device.

As part of a Lockdown policy, administrators can set a message on the Lock screen on company-owned Android devices. This informs the device holder who the owner of the device is. A maximum of 256 characters can be entered into the message.

Lock screen messages are applicable in the following modes:

- Work Profile Managed Device
- Managed Device with Work Profile
- Work Profile for Company Owned Device
- Work Managed Device - Non-GMS mode

Both device and user attributes (default and custom) can be used with the Lock screen message.

Extended lockdown policies for Android and Android Enterprise devices are supported on Samsung Knox devices. Support for specific settings sometimes depends on the Android OS version, the Mobile@Work version, and the Samsung Knox API version on the device. Extended lockdown policies are also available for Android Enterprise devices that are Work Managed Devices. Refer to the *Core Device Management Guide for Android enterprise* for details.

This section includes the following topics:

- [General lockdown policy fields](#)
- [When work profile accounts can be modified](#)
- [Lockdown policy fields for Windows devices](#)

Related topics

- [Lockdown policy fields for all Android devices and Android Enterprise devices](#)
- [Lockdown policy fields for all Android Enterprise devices](#)

- [Lockdown policy fields for Android Enterprise devices in Work Profile mode](#)
- [Lockdown policy fields for Android Enterprise devices in Work Managed Device mode and Managed Device with Work Profile mode](#)
- [Lockdown policy fields for Android Enterprise devices in Work Profile for Company Owned Device mode](#)
- [Lockdown policy fields for Samsung Knox Workspace \(3.0\) Android Enterprise Managed Device with Work Profile mode](#)
- [Lockdown policy fields for Android Enterprise devices with Samsung Restrictions in Work Managed Device mode and Managed Device with Work Profile mode](#)
- [Lockdown policy fields for Samsung Knox devices in Device Admin mode](#)

General lockdown policy fields

This section describes fields that are available for Android, Android enterprise, and Windows devices.

TABLE 25. LOCKDOWN POLICY FIELDS: GENERAL

Item	Description	Default Policy Setting
Name	<p>Required. Enter a descriptive name for this policy. This is the text that will be displayed to identify this policy throughout the Admin Portal. This name must be unique within this policy type.</p> <p>Tip: Though using the same name for different policy types is allowed (e.g., Executive), consider keeping the names unique to ensure clearer log entries.</p>	Default Lockdown Policy
Status	Select Active to turn on this policy. Select Inactive to turn off this policy.	Active
Priority	Specifies the priority of this custom policy relative to the other custom policies of the same type. This priority determines which policy is applied if more than one policy is associated with a specific device. Select "Higher than" or "Lower than", then select an existing policy from the drop-down list. For example, to give Policy A a higher priority than Policy B, you would select "Higher than" and "Policy B". See "Prioritizing policies" in the Device Management Guide for more information.	

TABLE 25. LOCKDOWN POLICY FIELDS: GENERAL (CONT.)

Item	Description	Default Policy Setting
	Because this priority applies only to custom policies, this field is not enabled when you create the first custom policy of a given type.	
Description	Enter an explanation of the purpose of this policy.	Default Lockdown Policy
Bluetooth	<p>Enable or disable access to Bluetooth features. You can enable both Audio and Data or just Audio.</p> <p>Caution:Core recommends against disabling audio because hands-free Bluetooth access is disabled. Legal requirements for hands-free use of devices while driving is widespread.</p> <hr/> <p> The Bluetooth settings are supported on Samsung Knox devices. However, enabling audio only is supported only with Mobile@Work 9.0.1.0-9.0.1.1. See “Bluetooth lockdown for Samsung Knox devices” in the <i>Core Device Management Guide for Android and Android Enterprise Devices</i> for more information.</p> <hr/>	Enable Audio & Data
Camera	Enable or disable camera access.	Enable
Camera User Control	When checked the Camera policy is considered enforced no matter the state of the camera. GPS location is not considered when user control is checked.	Unchecked
NFC	Enable or disable NFC (Near-field Communication) data exchange when the device touches another device.	Enable
USB Mass Storage	Enable or disable access to the device’s USB storage from a computer.	Enable
SD Card	Enable or disable access to the secure data card.	Enable
Wi-Fi	<p>Enable or disable access to wireless LANs.</p> <p>Caution: Disabling Wi-Fi on Wi-Fi-only devices is not recommended. A factory reset will be necessary to re-enable Wi-Fi on such devices.</p>	Enable

TABLE 25. LOCKDOWN POLICY FIELDS: GENERAL (CONT.)

Item	Description	Default Policy Setting
	 Wi-Fi lockdown is supported on Samsung Knox devices.	
Roaming Data	Enable or disable access to data services while roaming.	Enable
Copy / Paste	 This feature is not supported on Windows Phone 8.1 devices. <hr/> Enable or disable access to copy / paste functionality.	Enable
Screen Capture	This feature is supported on the following devices: <ul style="list-style-type: none"> • Windows Phone 8.1 and 10 • Android version 6.0 (or supported newer versions) with Android enterprise Enable or disable screen capture.	Enable
GPS	If GPS User Control is disabled, specify whether GPS is enabled or disabled on the device.	Enable
GPS User Control	Enable or disable the device user's ability to turn GPS on and off.	Enable

When work profile accounts can be modified

One Android Enterprise setting in the lockdown policy is **Allow the user to create and modify accounts**. This setting applies only to work profile accounts. It does not impact personal accounts.

If this lockdown policy setting **is** selected, the device user or an Android Enterprise app **can** add, modify, or delete work profile accounts on the device in **Settings > Accounts**.

A four-hour time period begins after Mobile@Work receives a lockdown policy in which the setting **Allow the user to create and modify accounts** is **not** selected. During that time period, the device user and Android Enterprise apps on the device can continue to add, modify, and delete work profile accounts. After the time period ends, work profile accounts cannot be added, modified, or deleted. Therefore, during this time period, the Divide Productivity or Gmail app can add the account that you specify in the **Configuration Choices** section for the app in the App Catalog on the Admin Portal. Make sure that your device users launch the Divide Productivity or Gmail app within the four-hour time period.

Notes

- Restarting a device does not restart the time period.
- Changing settings in the **Configuration Choices** section for Divide Productivity and Gmail in the App Catalog on the Admin Portal will have no impact to the account settings on the device after the time period is over. An exception to this rule exists for two app configurations. You can change these app configurations at any time, and the account settings on the device will be updated. These two app configurations are:
 - Default email signature
 - Default sync window

Lockdown policy fields for Windows devices

These lockdown options are applied to Windows devices.

TABLE 26. LOCKDOWN POLICY FIELDS: WINDOWS

Item	Description	Default Policy Setting
Internet Sharing	Enable or disable Internet sharing.	Enable
Microsoft Store	Enable or disable access to the Windows Store. <hr/>  You cannot deactivate this feature for Windows 10 Desktop devices.	Enable
Manual Email Set-up	Enable or disable ability to manually add an email account on the device.	Enable
VPN while Roaming	Enable or disable VPN when device is out of network.	Enable
Hotspot Discovery	Enable or disable Hotspot Discovery.	Enable
Microsoft Account	Enable or disable Microsoft SkyDrive or Live Account.	Enable
Save as of MS-Office	Enable or disable the Save As operation for a MS-Office document.	Enable

TABLE 26. LOCKDOWN POLICY FIELDS: WINDOWS (CONT.)

Item	Description	Default Policy Setting
	 This feature is not supported on Windows Phone 8.1 or Windows 10 Desktop devices.	
Browser	Enable or disable Internet Explorer. The option does not have any impact on any other browsers installed from the Windows Store.  This feature is not supported on Windows Phone 8.1 devices.	Enable
Manual Wi-Fi Setup	Enable or disable ability to manually add a Wi-Fi setup.  This feature is not supported on Windows 10 Desktop devices.	Enable
Wi-Fi Sense Hotspots	Enable or disable the device to automatically connect to Wi-Fi Hotspots and friend social network.	Enable
Sharing Of MS-Office Files	Enable or disable sharing MS-Office files.  This feature is not supported on Windows Phone 8.1 devices.	Enable
Sync User Settings to Device(s)	Enable or disable the device to automatically sync user settings to the Windows device.	Enable
Action Center Notifications	Enable or disable Action Center notifications.  This feature is not supported on Windows Phone 8.1 devices.	Enable
Developer Unlock	Enable or disable Developer Unlock.	Enable

TABLE 26. LOCKDOWN POLICY FIELDS: WINDOWS (CONT.)

Item	Description	Default Policy Setting
Search to Use Location	Enable or disable the Access to my location feature on the device. Disabling this feature impacts the Cortana and Bing.	Enable
Manual Root Certificate Installation	<p>Enable or disable ability to manually install a root certificate on the device. If disabled, the device user cannot install a root certificate to the device.</p> <hr/> <p> This feature is not supported on Windows Phone 8.1 devices.</p> <hr/>	Enable
Store Images From Visual Search	Enable or disable the Visual Search option in Bing.	Enable
Voice Recording	<p>Enable or disable voice recording in Cortana.</p> <hr/> <p> This feature is not supported on Windows Phone 8.1 devices.</p> <hr/>	Enable
Return Without Password	<p>Enable or disable ability for the device user to set grace period for locking. If enabled, the device user can set the grace period for locking the device. If disabled, the Security policy sets the grace period, and the option is not available to the device user.</p> <hr/> <p> This feature is not supported on Windows Phone 8.1 devices.</p> <hr/>	Enable
Cortana	Enable or disable Cortana.	Enable
Block Browser Popups	Enable or disable to block popups in browsers.	Enable
Browser Password Manager	Enable or disable the use of a browser password manager.	Enable
MS Error Reporting	Provides full, enhanced, basic, or security level error reporting.	Full

TABLE 26. LOCKDOWN POLICY FIELDS: WINDOWS (CONT.)

Item	Description	Default Policy Setting
Let Apps Run In Background	Allows administrators to turn off all applications running in the background to preserve battery usage on Windows devices that are on limited power or using cellular services.	User In Control
Windows Phone - Corporate Owned Devices Only <i>For Windows devices only.</i>		
Reset Phone	Enable or disable the device user's ability to reset the device to factory defaults.	Enable
MDM Un-enrollment	Enable or disable the device user's ability to remove the device from management by Core.	Enable

Lockdown policy fields for all Android devices and Android Enterprise devices

These lockdown options apply to all Android devices and all Android Enterprise devices.

TABLE 27. LOCKDOWN POLICY FIELDS: ANDROID AND ANDROID ENTERPRISE DEVICES

Item	Description	Default Policy Setting
Lockscreen Widgets	<p>Enable or disable the ability to add widgets to the lockscreen. Placing widgets on the lockscreen means device users can perform tasks without unlocking the device.</p> <hr/> <p> Though Samsung Knox devices have a feature that is very similar, it is not the Android lockscreen widgets feature, which is what Core controls. This option has no effect on Knox devices.</p> <hr/> <p>See also: Block Fingerprint and Block SmartLock settings in the Device Management Guide for Android Devices.</p>	Enable
Microphone	Enable or disable access by apps to the microphone. This feature does not impact voice calls.	Enable

TABLE 27. LOCKDOWN POLICY FIELDS: ANDROID AND ANDROID ENTERPRISE DEVICES (CONT.)

Item	Description	Default Policy Setting
Always Connect Device to Managed Wi-Fi	<p>When enabled, device will automatically connect to a managed Wi-Fi if one is available. This prevents users from connecting to a nearby access point if a managed Wi-Fi is available.</p> <p>If a managed Wi-Fi is listed under Turn Off Wi-Fi for these SSIDs, enabling Always Connect Device to Managed Wi-Fi will overrule that setting and will connect to the managed Wi-Fi.</p>	Disable
Debugging (USB, work profile and managed device)	Enable or disable the device user's ability to enable debugging on the USB, work profile, and managed profile.	Enable
Enable Network Logging on Android	<p>Enable Network Logging on Android - When enabled, network and connectivity information is collected. Network logging can be used to troubleshoot any issues with device connectivity for work apps and can be used for historical forensics. Once enabled, Core allows administrators to collect the logs on-demand. Network logs contain DNS lookup and connect() library call events. These library functions are recorded while network logging is active:</p> <ul style="list-style-type: none"> • getaddrinfo() • gethostbyname() • connect() <p>When network logging is enabled for Work Profile devices, the network logs will only include work profile network activity, not activity on the personal profile.</p>	Disable

Lockdown policy fields for all Android Enterprise devices

Whether a lockdown policy field applies to an Android Enterprise device depends on the Android Enterprise mode that the device is registered in. The modes—Work Managed Device mode, Managed Device with Work Profile (COPE) mode on Android devices versions 8-10, and Work Profile on Company Owned Devices Android versions 11 and later supported versions—are described in "Modes for Android Enterprise devices" in the *Core Device Management Guide for Android and Android Enterprise Devices*.

Lockdown options in this section apply to all Android Enterprise devices in all modes. On personally owned devices, these options do not impact the personal side of the device.

TABLE 28. LOCKDOWN POLICY FIELDS: ANDROID ENTERPRISE (ALL MODES)

Item	Description	Default Policy Setting
Allow screen capture	Allows screen capture of apps or data inside the Android Enterprise profile	Selected
Allow the user to turn on location sharing	Allows device GPS location to be shared with Work apps. Applicable to Android 6.0 and supported newer versions. For important information about Android 10-specific Wi-Fi settings, See "Wi-Fi network priority for Android devices" in the <i>Core Device Management Guide for Android and Android Enterprise Devices</i> .	Selected
Allow modification of applications in Settings or launchers	<p>Allows user to change application settings such as clearing cache, deleting data, uninstalling, or force stopping apps in App settings screen.</p> <hr/> <p> Use "Block uninstall" option in App Catalog app details to prevent user from uninstalling the app.</p> <hr/>	Selected
Allow the user to configure user credentials	Allows user to change credentials in the Work profile, in Android Settings > Security > Trusted Credentials > Work.	Selected
Allow the user to create and modify accounts	<p>Allows user to create or modify accounts in the Work profile, in Android Settings > Account.</p> <p>For more information, see "When work profile accounts can be modified" on page 154.</p>	Selected
Allow the user to transfer app data over NFC	<p>Allows use of NFC to transfer app data.</p> <p>Applicable to Android 6.0 and supported newer versions.</p>	Selected
Google Play Auto-Update Policy	Determines the automatic update policy that Google Play Store uses to update apps on the device. On the device, you can view these options by opening the Google Play Store app and selecting Settings. The option in Google Play Store settings is named Auto-update apps .	User Defined

TABLE 28. LOCKDOWN POLICY FIELDS: ANDROID ENTERPRISE (ALL MODES) (CONT.)

Item	Description	Default Policy Setting
	<p>The choices for this lockdown policy field are:</p> <ul style="list-style-type: none"> • User Defined- The device user can set the Auto-update apps setting in Google Play Store. • Never - Google Play Store never automatically updates apps on the device. • Wi-Fi Only - Google Play Store automatically updates apps on the device but only using Wi-Fi, not cellular, connections. • Always - Google Play Store automatically updates apps on the device using either Wi-Fi or cellular connections. <p>The device user can change the Auto-update apps setting in Google Play Store only if you select User Defined on the lockdown policy.</p> <hr/> <p> The Google Play Auto-Update Policy value only takes effect when there are Android for enterprise apps assigned to a device.</p>	
Enable system apps	<p>Allows user access to the system apps that are enabled by the administrator. This could include the system phone and camera. This is useful when a device initially disables system apps and then the administrator wants to enable it. Enabling does not work if the package of the system app is not present in the configuration.</p> <hr/> <p> Because of Android limitations, in order to remove an app from the System Apps blacklist, it is not enough for the administrator to remove the application's package name from "Disabled system apps" list box in the Lockdown Policy. Due to Android limitations, the app's package name should also be listed in the "Enabled system apps" list box.</p>	Not selected

TABLE 28. LOCKDOWN POLICY FIELDS: ANDROID ENTERPRISE (ALL MODES) (CONT.)

Item	Description	Default Policy Setting
	<p> When removing an application from the system apps blacklist, the administrator needs to also add it to the whitelist. This ensures the blacklisted app becomes accessible.</p> <hr/> <p> Administrators need to be aware that there are consequences when changing system apps.</p>	
Disable system apps	<p>Prevents the user from using the system apps restricted by the administrator.</p> <hr/> <p> Because of Android limitations, in order to remove an app from the System Apps blacklist, it is not enough for the administrator to remove the application's package name from "Disabled system apps" list box in the Lockdown Policy. Due to Android limitations, the app's package name should also be listed in the "Enabled system apps" list box.</p> <hr/> <p> When removing an application from the system apps blacklist, the administrator needs to also add it to the whitelist. This ensures the blacklisted app becomes accessible.</p> <hr/> <p> Administrators need to be aware that there are consequences when changing system apps.</p>	Not selected
Ensure Verify apps	Restricts the user from disabling the "Verify Apps" option in Android.	Selected
Restrict Input Methods	Leave blank to permit ONLY system input methods, and add specific package names to enable third-party input apps.	Not selected

TABLE 28. LOCKDOWN POLICY FIELDS: ANDROID ENTERPRISE (ALL MODES) (CONT.)

Item	Description	Default Policy Setting
	This does NOT apply to devices if users have already selected a third-party input app. This configuration only restricts new changes to the input method.	
Restrict accessibility services	<p>Leave blank to permit ONLY system input methods, and add specific package names to enable third-party input apps.</p> <p>This does NOT apply to devices if users have already selected a third-party accessibility service. This configuration only restricts new changes to the accessibility service.</p>	Not selected

Lockdown policy fields for Android Enterprise devices in Work Profile mode

Whether a lockdown policy field applies to an Android Enterprise device depends on the Android Enterprise mode that the device is registered in. The modes—Work Managed Device mode, Managed Device with Work Profile (COPE) mode on Android devices versions 8-10, and Work Profile on Company Owned Devices Android versions 11 and later supported versions—are described in "Modes for Android Enterprise devices" in the *Core Device Management Guide for Android and Android Enterprise Devices*.

Lockdown options in this section apply to Android Enterprise devices in Work Profile mode.

TABLE 29. LOCKDOWN POLICY FIELDS: ANDROID ENTERPRISE IN WORK PROFILE MODE

Item	Description	Default Policy Setting
Allow copy and paste	Allows copy and paste from apps inside the Android Enterprise profile to apps outside the profile.	Selected
Allow caller ID across profiles	<p>Allows caller ID to be visible to phone app in all profiles.</p> <hr/> <p> When the caller ID is permitted across profiles, work contacts can be viewed by the personal apps for incoming calls. This applies to Android 6.0 through the most recently released versions as supported by MobileIron.</p> <hr/>	Selected

TABLE 29. LOCKDOWN POLICY FIELDS: ANDROID ENTERPRISE IN WORK PROFILE MODE (CONT.)

Item	Description	Default Policy Setting
Allow work calendar sharing with personal profile	Select to 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 (for example calendar apps like Google calendar.) If the work event is tapped within the personal profile, a view of the event displays. Tapped again, it opens the event in the work calendar. Applicable to Managed devices with work profiles.	Not selected
Allow contact search across profiles	<p>Allows personal space Contacts app sharing across the profile.</p> <hr/> <p> This is supported on Android 7.0 devices through the most recently released version as supported by MobileIron.</p> <hr/>	Selected
Allow contact sharing on Bluetooth devices.	<p>Allows the caller ID to be visible on another Bluetooth device such as your car's Bluetooth screen.</p> <hr/> <p> This is supported on Android 6.0 devices through the most recently released version as supported by MobileIron.</p> <hr/>	Selected
Allow unknown sources in Personal and Work Profile	<p>Allow installation of apps from untrusted sources in the Personal and Work Profile.</p> <ul style="list-style-type: none"> If checked, the user is allowed to install the app from an unknown source on both the personal and work profile of the device. <hr/> <p> When this field is selected, the "Allow Unknown Sources in Work Profile" check box displays. Selecting it indicates to restrict the Allow Unknown Source setting to the Work Profile mode only. Use case: This allows third-party apps like games from outside the Google Play store to be installed in the personal profile.</p> <hr/> <ul style="list-style-type: none"> If unchecked, the user is unable to install from an unknown source on either the personal or the work profile of the device. 	Not selected

TABLE 29. LOCKDOWN POLICY FIELDS: ANDROID ENTERPRISE IN WORK PROFILE MODE (CONT.)

Item	Description	Default Policy Setting
Android 8: Allow Auto-Fill	Allows password autofill.	Selected
Android 8: Allow work app notifications in personal profile	When device user is in personal profile, notifications from Mobile@Work apps will display.	Selected
Android 8: Allow Bluetooth Sharing	Allows Bluetooth sharing with other devices.	Selected
Android 9: Allow Printing	Allows the printing of documents from Mobile@Work apps.	Selected
Android 9: Allow Share into Profile	Allows sharing from outside the Work Profile to inside the Work Profile	Selected
Android 11+: Enable Cross profile whitelisting of Apps	Allows users to share information from specific apps from within the work profile to the personal side of the device. This allows data from the Work Profile container to share data to the exact same app that is located on the personal side. Selecting + displays a list and you must add at least one app in order for this configuration to apply.	Not selected
Android 11+: Enable Maximum Profile Timeout	Select to set a maximum time window the work profile can be turned off before Core suspends personal apps on the device. You can set a time between 72 and 8760 hours. 8760 hours is one year of time. Default value is set to 72 hrs if the option is selected. The device user sees a message prompting to turn on the work profile to enable suspended apps. Available for Android 11+ devices in Work Profile on Company Owned Device.	

TABLE 29. LOCKDOWN POLICY FIELDS: ANDROID ENTERPRISE IN WORK PROFILE MODE (CONT.)

Item	Description	Default Policy Setting
Android 12+: Enable 5G Slicing	<p>Administrators can set all app traffic through an enterprise 5G network slice. Instead of setting up slices through APNs, administrators can set devices to route the traffic from all apps in the work profile to an enterprise network slice through the UE Route Selection Policy (URSP) rules. Administrators can turn on or off Work Profile app traffic routing to the enterprise network slice on a per-employee basis. In the Device Details page, the 5G Slicing status is indicated. Advanced searching on 5G is also part of this feature, as is making compliance rules.</p> <hr/> <p> Requires support from 5G service provider.</p>	Disabled
Managed Device		
Android 11: Enable Common Criteria (CC) mode	<p>Select to enable Common Criteria mode for Android 11 + devices.</p> <hr/> <p> If Common Criteria mode is turned off after being enabled previously, all existing Wi-Fi configurations will be lost.</p> <hr/> <p>Applicable to Managed Device with Work Profile mode and Work Profile on Company Owned Device mode.</p>	Disabled
Configure Private DNS settings	<p>Private DNS allows more privacy for device users than using public DNS servers. It provides a way for enterprises to secure device user activity and enterprise hostnames from being learnt by unwanted DNS servers. Private DNS allows devices to discover DNS over TLS and provide specific DNS server hostnames to prevent leaking of DNS resolution.</p> <p>Devices will use DNS-over-TLS prior to attempting name resolution in cleartext. Selecting this box expands to display:</p> <ul style="list-style-type: none"> • Off - Private DNS cannot be disabled from the Admin Portal. Device user can disable private DNS setting, if allowed to change the settings. 	Disabled

TABLE 29. LOCKDOWN POLICY FIELDS: ANDROID ENTERPRISE IN WORK PROFILE MODE (CONT.)

Item	Description	Default Policy Setting
	<ul style="list-style-type: none"> • Opportunistic - The device will attempt to find a server that supports private DNS. If it cannot find one, it will fall back to non-private DNS (cleartext). • Use Specific DNS Server - enter the hostname of server that implements DNS over TLS (RFC7858). This value cannot be empty. Once added, it can only be updated. <p>Applicable to: Android 10+ devices in Work Managed Device mode.</p>	
Allow user to override Private DNS settings	The hostname of a server that implements DNS over TLS (RFC7858). This value cannot be empty.	Disabled

Lockdown policy fields for Android Enterprise devices in Work Managed Device mode and Managed Device with Work Profile mode

Whether a lockdown policy field applies to an Android Enterprise device depends on the Android Enterprise mode that the device is registered in. The modes — Work Managed Device mode, Managed Device with Work Profile (COPE) mode on Android devices versions 8-10, and Work Profile on Company Owned Devices Android versions 11 and later supported versions— are described in "Modes for Android Enterprise devices" in *Core Device Management Guide for Android and Android Enterprise Devices*.

Lockdown options in this section apply to Android Enterprise devices in Work Managed Device mode and Managed Device with Work Profile (COPE) mode on Android devices versions 8-10.

TABLE 30. LOCKDOWN POLICY FIELDS: ANDROID ENTERPRISE IN WORK MANAGED DEVICE MODE AND MANAGED DEVICE WITH WORK PROFILE MODE

Item	Description	Default Policy Setting
Device Restrictions		
Allow camera	Allows camera to function.	Enabled
Allow master volume un-mute	Allows the user to un-mute master volume. Note: volume is not muted by default.	Enabled

TABLE 30. LOCKDOWN POLICY FIELDS: ANDROID ENTERPRISE IN WORK MANAGED DEVICE MODE AND MANAGED DEVICE WITH WORK PROFILE MODE (CONT.)

Item	Description	Default Policy Setting
Allow microphone un-mute	Allows the user to un-mute microphone	Enabled
Allow automatic date & time	If checked, the user can change date and time. If unchecked, user can make changes but system will reset the date and time automatically.	Enabled
Allow automatic timezone	Allows timezone to be set automatically. Note: the user can re-enable the ability to update time and timezone if this setting is disallowed.	Enabled
Allow safe boot of the device	Allows user to reboot the device into safe mode.	Enabled
Allow factory reset	Allows the user to initiate a factory reset of the device.	Enabled
Allow the user to mount physical external media	Allows the user to mount external media such as SD cards or external drives.	Enabled
Allow the user to transfer files over USB	Allows user copy, paste, and transfer data and files using USB drives.	Enabled
Allow use of USB storage	Allows data to be stored on USB drives.	Enabled
Keep device on while plugged in	Allows device to remain powered on when it is plugged in to a power source. When this field is enabled, the device does not go into sleep mode.	Disabled
Allow Keyguard (no effect if password or PIN is set)	Allows a keyguard, or lockscreen, on the device under the condition that the device has not been enabled using a PIN, password, or pattern.	Enabled
Allow backup service	Allows the user to backup and restore their devices using Google services on managed devices running Android 8.0 through the most recently released versions as supported by MobileIron.	Enabled

TABLE 30. LOCKDOWN POLICY FIELDS: ANDROID ENTERPRISE IN WORK MANAGED DEVICE MODE AND MANAGED DEVICE WITH WORK PROFILE MODE (CONT.)

Item	Description	Default Policy Setting
Allow install from unknown sources on the device	Allows administrator to enable installation of apps from unknown sources to device. Unless this field is selected, the work profile never allows installation of apps from unknown sources.	Disabled
Phone & Network Restrictions		
Allow SMS	Allow the user to send and receive SMS messages.	Enabled
Allow outgoing calls	Allow user to place outgoing calls.	Enabled
Allow data roaming	Allow the use of data while user is traveling outside of data plan area. Note: the user can re-enable this feature from settings.	Enabled
Allow Wi-Fi	<p>If Allow Wi-Fi is:</p> <ul style="list-style-type: none"> • enabled (default), the device user can turn Wi-Fi on or off • not enabled, the device user cannot turn Wi-Fi on <hr/> <p>Caution: Turning off Wi-Fi on a Wi-Fi only device will make the device unable to communicate with Core or any network. A factory reset will be needed to restore Wi-Fi capability on the device.</p> <hr/>	Enabled
Allow Wi-Fi to be configured	Allows the user to configure Wi-Fi.	Enabled
Allow Wi-Fi sleep policy to be configured	Allows user to configure the Wi-Fi sleep policy. On a device, the user can re-enable this feature from Settings. For this field, the server policy settings are applied when the device checks into Core. If the user modifies the Wi-Fi sleep policy on a device and then you, as the administrator, change the "Allow Wi-Fi sleep policy to be configured" field, the user modifications for this field are overwritten by the lockdown policy that resides on the server when the device checks in.	Enabled
Allow Bluetooth	If Allow Bluetooth is:	Enabled

TABLE 30. LOCKDOWN POLICY FIELDS: ANDROID ENTERPRISE IN WORK MANAGED DEVICE MODE AND MANAGED DEVICE WITH WORK PROFILE MODE (CONT.)

Item	Description	Default Policy Setting
	<ul style="list-style-type: none"> enabled (default), the device user can turn Bluetooth on or off not enabled, the device user cannot turn Bluetooth on 	
Allow Bluetooth to be configured	Allows the user to configure Bluetooth on managed devices.	Enabled
Allow Bluetooth Outbound Sharing	Allows the user to share files using Bluetooth on managed devices running Android 8.0 through the most recently released versions as supported by MobileIron.	Enabled
Allow Emergency Broadcasts to be configured	Allows the user to configure Emergency Broadcasts.	Enabled
Allow mobile network to be configured	Allows the user to configure the mobile network.	Enabled
Allow tethering and mobile hotspots to be configured	Allows the user to configure tethering and hotspots.	Enabled
Allow VPN to be configured	<p>Allows the user to configure VPN.</p> <hr/> <p> This setting must be enabled to allow the application of a managed VPN. As a workaround, enable Always-on VPN in Android Enterprise settings and select Tunnel as the App Identifier.</p> <hr/>	Enabled
Managed Device		
Android 11: Enable Common Criteria (CC) mode	Select to enable Common Criteria mode for Android 11 + devices.	Disabled

TABLE 30. LOCKDOWN POLICY FIELDS: ANDROID ENTERPRISE IN WORK MANAGED DEVICE MODE AND MANAGED DEVICE WITH WORK PROFILE MODE (CONT.)

Item	Description	Default Policy Setting
	<div style="border: 1px solid red; padding: 5px; margin-bottom: 10px;">  If Common Criteria mode is turned off after being enabled previously, all existing Wi-Fi configurations will be lost. </div> <p>Applicable to Managed Device with Work Profile mode and Work Profile on Company Owned Device mode.</p>	

Lockdown policy fields for Android Enterprise devices in Work Profile for Company Owned Device mode

Whether a lockdown policy field applies to an Android Enterprise device depends on the Android Enterprise mode that the device is registered in. The modes — Work Managed Device mode, Managed device with Work Profile (COPE) mode on Android devices versions 8-10, and Work Profile on Company Owned Devices Android version 11 and supported later versions— are described in "Modes for Android Enterprise devices" in *Core Device Management Guide for Android and Android Enterprise Devices*.

Lockdown options in this section apply to Android Enterprise devices in Work Profile for Company Owned Device applicable to Android devices version 11 and supported later versions.

TABLE 31. LOCKDOWN POLICY FIELDS: ANDROID ENTERPRISE IN WORK PROFILE FOR COMPANY OWNED DEVICE MODE

Item	Description	Default Policy Setting
Device Restrictions		
Allow camera	Allows camera to function.	Enabled
Allow master volume un-mute	Allows the user to un-mute master volume. Note: volume is not muted by default.	Enabled
Allow microphone un-mute	Allows the user to un-mute microphone	Enabled

TABLE 31. LOCKDOWN POLICY FIELDS: ANDROID ENTERPRISE IN WORK PROFILE FOR COMPANY OWNED DEVICE MODE (CONT.)

Item	Description	Default Policy Setting
Allow automatic date & time	If checked, the user can change date and time. If unchecked, user can make changes but system will reset the date and time automatically.	Enabled
Allow automatic timezone	Allows timezone to be set automatically. Note: the user can re-enable the ability to update time and timezone if this setting is disallowed.	Enabled
Allow safe boot of the device	Allows user to reboot the device into safe mode.	Enabled
Allow factory reset	Allows the user to initiate a factory reset of the device.	Enabled
Allow the user to mount physical external media	Allows the user to mount external media such as SD cards or external drives.	Enabled
Allow the user to transfer files over USB	Allows user copy, paste, and transfer data and files using USB drives.	Enabled
Allow use of USB storage	Allows data to be stored on USB drives.	Enabled
Keep device on while plugged in	Allows device to remain powered on when it is plugged in to a power source. When this field is enabled, the device does not go into sleep mode.	Disabled
Allow Keyguard (no effect if password or PIN is set)	Allows a keyguard, or lockscreen, on the device under the condition that the device has not been enabled using a PIN, password, or pattern.	Enabled
Allow backup service	Allows the user to backup and restore their devices using Google services on managed devices running Android 8.0 through the most recently released versions as supported by MobileIron.	Enabled

TABLE 31. LOCKDOWN POLICY FIELDS: ANDROID ENTERPRISE IN WORK PROFILE FOR COMPANY OWNED DEVICE MODE (CONT.)

Item	Description	Default Policy Setting
Allow install from unknown sources on the device	Allow installation of apps from untrusted sources in the personal profile. Unless this field is selected, the work profile never allows installation of apps from unknown sources.	Disabled
Phone & Network Restrictions		
Allow SMS	Allow the user to send and receive SMS messages.	Enabled
Allow outgoing calls	Allow user to place outgoing calls.	Enabled
Allow data roaming	Allow the use of data while user is traveling outside of data plan area. Note: the user can re-enable this feature from settings.	Enabled
Allow Wi-Fi	<p>If Allow Wi-Fi is:</p> <ul style="list-style-type: none"> • Enabled (default), the device user can turn Wi-Fi on or off • Not enabled, the device user cannot turn Wi-Fi on <hr/> <p> Caution: Turning off Wi-Fi on a Wi-Fi only device will make the device unable to communicate with Core or any network. A factory reset will be needed to restore Wi-Fi capability on the device.</p> <hr/>	Enabled
Allow Wi-Fi to be configured	Allows the user to configure Wi-Fi.	Enabled
Allow Wi-Fi sleep policy to be configured	Allows user to configure the Wi-Fi sleep policy. On a device, the user can re-enable this feature from Settings. For this field, the server policy settings are applied when the device checks into Core. If the user modifies the Wi-Fi sleep policy on a device and then you, as the administrator, changes the "Allow Wi-Fi sleep policy to be configured" field, the user modifications for this field are overwritten by the lockdown policy that resides on the server when the device checks in.	Enabled

TABLE 31. LOCKDOWN POLICY FIELDS: ANDROID ENTERPRISE IN WORK PROFILE FOR COMPANY OWNED DEVICE MODE (CONT.)

Item	Description	Default Policy Setting
Allow Bluetooth	If Allow Bluetooth is: <ul style="list-style-type: none"> • Enabled (default), the device user can turn Bluetooth on or off • Not enabled, the device user cannot turn Bluetooth on 	Enabled
Allow Bluetooth to be configured	Allows the user to configure Bluetooth on managed devices.	Enabled
Allow Bluetooth Outbound Sharing	Allows the user to share files using Bluetooth on managed devices running Android 8.0 through the most recently released versions as supported by MobileIron.	Enabled
Allow Emergency Broadcasts to be configured	Allows the user to configure Emergency Broadcasts.	Enabled
Allow mobile network to be configured	Allows the user to configure the mobile network.	Enabled
Allow tethering and mobile hotspots to be configured	Allows the user to configure tethering and hotspots.	Enabled
Allow VPN to be configured	Allows the user to configure VPN. <hr/>  This setting must be enabled to allow the application of a managed VPN. As a workaround, enable Always-on VPN in Android Enterprise settings and select Tunnel as the App Identifier. <hr/>	Enabled
Managed Device		
Android 11:	Select to enable Common Criteria mode for Android 11 + devices.	Disabled

TABLE 31. LOCKDOWN POLICY FIELDS: ANDROID ENTERPRISE IN WORK PROFILE FOR COMPANY OWNED DEVICE MODE (CONT.)

Item	Description	Default Policy Setting
Enable Common Criteria (CC) mode	<p> If Common Criteria mode is turned off after being enabled previously, all existing Wi-Fi configurations will be lost.</p> <hr/> <p>Applicable to Managed Device with Work Profile mode and Work Profile on Company Owned Device mode.</p>	
Android 12+: Enable 5G Slicing	<p>Administrators can set all app traffic through an enterprise 5G network slice. Instead of setting up slices through APNs, administrators can set devices to route the traffic from all apps in the work profile to an enterprise network slice through the UE Route Selection Policy (URSP) rules. Administrators can turn on or off Work Profile for Company Owned Devices app traffic routing to the enterprise network slice on a per-employee basis. In the Device Details page, the 5G Slicing status is indicated. Advanced searching on 5G is also part of this feature, as is making compliance rules.</p> <hr/> <p> Requires support from 5G service provider.</p>	Disabled
Security Logging		
Enable Security Logging on Android	When enabled, information is collected for security auditing purposes. These help administrators identify suspicious activity by remotely tracking device activity, including app launches, Android Debug Bridge (adb) activity, and screen unlocks. These logs become available to device administrators on demand. To protect the privacy of the user, some information (such as personal app launch events) are hidden, or redacted (for example, details of the physical volume mount events).	Disabled

Lockdown policy fields for Samsung Knox Workspace (3.0) Android Enterprise Managed Device with Work Profile mode

The lockdown options in this section apply to Android Enterprise Managed Device with Work Profile (COPE) mode for Samsung Knox version 3.0. These lockdowns allow you to set a variety of restrictions, such as allowing Google accounts to auto sync, providing content sharing, and sharing of calendar information outside a container. You must select the **Enable Samsung Workspace restrictions** check box to display the following fields.



The API s in the following table may require a Samsung Knox license. If you do not have a Samsung Knox license, these fields may not be supported.

TABLE 32. LOCKDOWN POLICY FIELDS: SAMSUNG KNOX WORKSPACE (3.0) ANDROID ENTERPRISE IN MANAGED DEVICE WITH WORK PROFILE MODE

Item	Description	Default Policy Setting
Whitelisted Google Accounts	Allows you to whitelist specific Google Accounts. To add an account, click the + button and type in the name of the Google account. To delete a Google account, select the account and then click the - button.	None
Allow camera	Allows the camera on the phone to function.	Disabled
Allow content sharing	Allows content sharing	Disabled
Allow email account creation	Allows the device user to create an email account.	Disabled
Allow NFC	Enable or disable NFC (Near-field Communication) data exchange when the device touches another device.	Disabled
Allow USB	Enable or disable the USB protocol.	Disabled
Allow New Admin Install	Enable or disable the installation of another administration app from all sources, unless the app install is performed by the administrator enforcing this policy. This policy can only be applied if there are no other administrators activated with the exception of Mobile@Work clients.	Disabled
Allow Google Accounts Auto Sync	Enable or disable the ability of Google accounts to sync automatically. This option does not block the Google Play Store from updating installed apps.	Disabled

TABLE 32. LOCKDOWN POLICY FIELDS: SAMSUNG KNOX WORKSPACE (3.0) ANDROID ENTERPRISE IN MANAGED DEVICE WITH WORK PROFILE MODE (CONT.)

Item	Description	Default Policy Setting
Enable Certificate Revocation Status (CRL) Check	Enable or disable the Certificate Revocation List (CRL) check for revocation of the server-certificate chain during the SSL mutual authentication process.	Disabled
Allow sharing of calendar information outside container	Enable or disable sharing of calendar information outside of the container.	Disabled

Lockdown policy fields for Android Enterprise devices with Samsung Restrictions in Work Managed Device mode and Managed Device with Work Profile mode

These lockdown options are applied to Android Enterprise Samsung devices in the Work Managed Device mode and Managed Device with Work Profile (COPE) mode. You must select the **Enable Samsung Restrictions** check box in order to display the Samsung Restrictions drop-down menu.

TABLE 33. LOCKDOWN POLICY FIELDS: ANDROID ENTERPRISE DEVICES WITH SAMSUNG RESTRICTIONS IN WORK MANAGED DEVICE MODE AND MANAGED DEVICE WITH WORK PROFILE MODE

Item	Description	Default Policy Setting
Android Browser	Enable or disable access to the Android browser.	Enable
Email Account Creation	Enable or disable the device user's ability to configure an email account on the device.	Enable
Factory Reset	Enable or disable the ability for users to reset the device to factory defaults.	Enable
Google Backup	Enable or disable backup to Google servers.	Enable
Google Play	Enable or disable access to Google Play.	Enable
Incoming SMS	Enable or disable incoming SMS messages. The user is not informed if SMS is blocked.	Enable
Outgoing SMS	Enable or disable outgoing MMS messages.	Enable
Incoming MMS	Enable or disable incoming MMS messages.	Enable

TABLE 33. LOCKDOWN POLICY FIELDS: ANDROID ENTERPRISE DEVICES WITH SAMSUNG RESTRICTIONS IN WORK MANAGED DEVICE MODE AND MANAGED DEVICE WITH WORK PROFILE MODE (CONT.)

Item	Description	Default Policy Setting
	The user is not informed if MMS is blocked.	
Outgoing MMS	Enable or disable outgoing MMS messages.	Enable
Make Passwords Visible	Select Enable to allow users to change the “ Make Passwords Visible ” setting on their device. Select Disable to prevent users from changing this setting and make password characters not visible.	Enable
Developer options	Enable or disable this option to make USB debugging available to developers on Samsung Knox devices.	Enable
OTA Upgrade	<p>Enable or disable over-the-air upgrades of the device firmware.</p> <p>Over-the-air upgrades require the device to be in recovery mode. Therefore, for devices to perform an over-the-air upgrade, enable both Recovery Mode and OTA Upgrade in the lockdown policy.</p> <hr/> <p>WARNING: Do not disable Setting Changes in the lockdown policy if OTA Upgrade is enabled. Disabling Setting Changes when OTA Upgrade is enabled can result in a non-functional device because setting changes are required for upgrade.</p> <hr/>	Enable
Recovery Mode	Enable or disable the device from entering Recovery Mode. Caution: use Disable with care. Disabling recovery mode on a device may make the device unrecoverable if there is an issue with the device’s operating system.	Enable
Roaming Voice Calls	Enable or disable voice calls while roaming.	Enable
Safe Mode	<p>Enable or disable the user’s ability to reboot a Samsung Knox device into Safe Mode.</p> <hr/> <p>i A device running in Safe mode is not protected by MobileIron, because only system apps run in Safe mode.</p> <hr/>	Enable

TABLE 33. LOCKDOWN POLICY FIELDS: ANDROID ENTERPRISE DEVICES WITH SAMSUNG RESTRICTIONS IN WORK MANAGED DEVICE MODE AND MANAGED DEVICE WITH WORK PROFILE MODE (CONT.)

Item	Description	Default Policy Setting
Setting Changes	<p>Enable or disable the device user access to the settings app.</p> <hr/> <p>WARNING: Do not disable Setting Changes if OTA Upgrade is enabled. Disabling Setting Changes when OTA Upgrade is enabled can result in a non-functional device because setting changes are required for upgrade.</p> <hr/>	Enable
Tethering - Bluetooth	<p>Enable or disable Bluetooth tethering.</p> <p>Refer to “Bluetooth lockdown for Samsung Knox devices” in the <i>Core Device Management Guide for Android and Android Enterprise Devices</i>.</p>	Enable
Tethering - USB	Enable or disable USB tethering.	Enable
Tethering - Wi-Fi	Enable or disable Wi-Fi tethering.	Enable
USB Media Player	Enable or disable the USB media player.	Enable
Manual Date Time Change	Enable or disable the ability to manually change the date and time.	Enable
Certificate Revocation Status (CRL) Check	Enable or disable the Certificate Revocation List (CRL) check for revocation of the server-certificate chain during the SSL mutual authentication process.	Disabled
Google Crash Report	An administrator can use this API to enable or disable sending a crash report to Google. If disabled, all possible Google crash reports are blocked.	Enable
Google Accounts Auto-sync	Enable or disable Google accounts auto-sync.	Enable
Multi-user mode	Enable or disable the Multi-user mode.	Enable
New admin installation	Enable or disable new administrator installation.	Enable
Allow cellular data	Enable or disable the ability for users to use cellular data.	Enable

TABLE 33. LOCKDOWN POLICY FIELDS: ANDROID ENTERPRISE DEVICES WITH SAMSUNG RESTRICTIONS IN WORK MANAGED DEVICE MODE AND MANAGED DEVICE WITH WORK PROFILE MODE (CONT.)

Item	Description	Default Policy Setting
	<p> If you disable both cellular data and Wi-Fi on a device, Core can no longer communicate with the device. The device may need a factory reset to restore functionality.</p>	
Allow USB HID Protocol	Enable or disable the USB Human Interface Device (HID) protocol.	Enable
Restricted Apps	<p>List apps that you want to prevent from being installed or run on Samsung Knox devices.</p> <p>Click + to add an application identifier (app ID) for the app. The app ID is case-sensitive. You can use the wild card character * to cover a set of apps, such as all apps from a particular vendor.</p> <p>For example, com.abcdef.* restricts all application IDs beginning with com.abcdef.</p> <p>However, to ensure that pre-existing apps get restricted, provide the complete app ID. Do not use a wild card character.</p>	(empty)
Allowed Apps	<p>List the apps that you that are exceptions to the apps covered by a wild card character in the Restricted Apps section.</p> <p>Click + to add an application identifier (app ID) for the app. The app ID is case-sensitive.</p>	(empty)
Turn Off Wi-Fi for SSIDs	<p>Prevent Samsung Knox devices from accessing the Wi-Fi SSIDs listed in this section.</p> <p>Click + to add an SSID. The SSID is case-sensitive.</p> <hr/> <p> Do not restrict Wi-Fi SSIDs that are configured for the device.</p> <hr/> <p> In Mobile@Work 9.0.0.0 for Android, connection to SSIDs listed in this section can occur if the SSID is managed and Always Connect Device to Managed Wi-Fi is enabled.</p>	(empty)

Lockdown policy fields for Samsung Knox devices in Device Admin mode

These lockdown options are applied to Samsung Knox devices in Device Admin mode.

TABLE 34. LOCKDOWN POLICY FIELDS: SAMSUNG(DDEVICE ADMIN MODE)

Item	Description	Default Policy Setting
Android Browser	Enable or disable access to the Android browser.	Enable
Email Account Creation	Enable or disable the device user's ability to configure an email account on the device.	Enable
Cellular Data	<p>Enable or disable the ability for users to use cellular data.</p> <hr/> <p> If you disable both cellular data and Wi-Fi on a device, Core can no longer communicate with the device. The device may need a factory reset to restore functionality.</p> <hr/>	Enable
Factory Reset	Enable or disable the ability for users to reset the device to factory defaults.	Enable
Google Backup	Enable or disable backup to Google servers.	Enable
Google Play	Enable or disable access to Google Play.	Enable
Incoming MMS	<p>Enable or disable incoming MMS messages.</p> <p>The user is not informed if MMS is blocked.</p>	Enable
Incoming SMS	<p>Enable or disable incoming SMS messages.</p> <p>The user is not informed if SMS is blocked.</p>	Enable
Make Passwords Visible	Select Enable to allow users to change the " Make Passwords Visible " setting on their device. Select Disable to prevent users from changing this setting and make password characters not visible.	Enable
Developer options	Enable or disable this option to make USB debugging available to developers on Samsung Knox devices.	Enable
Management Removal	Enable or disable the device user's ability to remove the Samsung DM Agent from Android devices.	Enable
OTA Upgrade	Enable or disable over-the-air upgrades of the device firmware.	Enable

TABLE 34. LOCKDOWN POLICY FIELDS: SAMSUNG(DVICE ADMIN MODE) (CONT.)

Item	Description	Default Policy Setting
	<p>Over-the-air upgrades require the device to be in recovery mode. Therefore, for devices to perform an over-the-air upgrade, enable both Recovery Mode and OTA Upgrade in the lockdown policy.</p> <hr/> <p>WARNING: Do not disable Setting Changes in the lockdown policy if OTA Upgrade is enabled. Disabling Setting Changes when OTA Upgrade is enabled can result in a non-functional device because setting changes are required for upgrade.</p>	
Outgoing MMS	Enable or disable outgoing MMS messages.	Enable
Outgoing SMS	Enable or disable outgoing SMS messages.	Enable
Recovery Mode	Enable or disable the device from entering Recovery Mode. Caution: use Disable with care. Disabling recovery mode on a device may make the device unrecoverable if there is an issue with the device's operating system.	Enable
Roaming Voice Calls	Enable or disable voice calls while roaming.	Enable
Safe Mode	<p>Enable or disable the user's ability to reboot a Samsung Knox device into Safe Mode.</p> <hr/> <p>i A device running in Safe mode is not protected by MobileIron, because only system apps run in Safe mode.</p>	Enable
Setting Changes	<p>Enable or disable the device user access to the settings app.</p> <hr/> <p>WARNING: Do not disable Setting Changes if OTA Upgrade is enabled. Disabling Setting Changes when OTA Upgrade is enabled can result in a non-functional device because setting changes are required for upgrade.</p>	Enable
Tethering - Bluetooth	Enable or disable Bluetooth tethering.	Enable

TABLE 34. LOCKDOWN POLICY FIELDS: SAMSUNG(DEVICE ADMIN MODE) (CONT.)

Item	Description	Default Policy Setting
	Refer to "Bluetooth lockdown for Samsung Knox devices" in the <i>Core Device Management Guide for Android and Android Enterprise Devices</i>	
Tethering - USB	Enable or disable USB tethering.	Enable
Tethering - Wi-Fi	Enable or disable Wi-Fi tethering.	Enable
Unknown Sources	Enable or disable installation of apps from sources other than Google Play.	Enable
USB Media Player	Enable or disable the USB media player.	Enable
YouTube App	Enable or disable access to YouTube App.	Enable
Manual Date Time Change	Enable or disable the ability to manually change the date and time.	Enable
Certificate Revocation Status (CRL) Check	Enable or disable the Certificate Revocation List (CRL) check for revocation of the server-certificate chain during the SSL mutual authentication process.	Disable
Google Crash Report	An administrator can use this API to enable or disable sending a crash report to Google. If disabled, all possible Google crash reports are blocked.	Enable
Google Accounts Auto-sync	Enable or disable Google accounts auto-sync.	Enable
Multi-user mode	Enable or disable the Multi-user mode	Enable
New admin installation	Enable or disable new administrator installation	Enable
Allow USB HID Protocol	Enable or disable the USB Human Interface Device (HID) protocol.	Enable
Restricted Apps	List apps that you want to prevent from being installed or run on Samsung Knox devices.	(empty)

TABLE 34. LOCKDOWN POLICY FIELDS: SAMSUNG(DEVICE ADMIN MODE) (CONT.)

Item	Description	Default Policy Setting
	<p>Click + to add an application identifier (app ID) for the app. The app ID is case-sensitive. You can use the wild card character * to cover a set of apps, such as all apps from a particular vendor.</p> <p>For example, com.abcdef.* restricts all application IDs beginning with com.abcdef.</p> <p>However, to ensure that pre-existing apps get restricted, provide the complete app ID. Do not use a wild card character.</p>	
Allowed Apps	<p>List the apps that you that are exceptions to the apps covered by a wild card character in the Restricted Apps section.</p> <p>Click + to add an application identifier (app ID) for the app. The app ID is case-sensitive.</p>	(empty)
Turn Off Wi-Fi for these SSIDs	<p>Prevent Samsung Knox devices from accessing the Wi-Fi SSIDs listed in this section.</p> <p>Click + to add an SSID. The SSID is case-sensitive.</p> <hr/> <p> Do not restrict Wi-Fi SSIDs that are configured for the device.</p> <hr/> <p>In Mobile@Work 9.0.0.0 for Android, connection to SSIDs listed in this section can occur if the SSID is managed and Always Connect Device to Managed Wi-Fi is enabled.</p>	(empty)

Sync policies

Sync policies specify how Mobile@Work (Apps@Work on Windows) behaves on the device and interacts with Core. These interactions include synchronizing profiles, configurations, and app inventory.



For Windows Phone 8.1 devices, only Sync Interval is applied. The sync interval is applied when the device registers with Core. Any changes to the sync interval after the device has registered are not applied to the device. If you change the sync policy with sync-interval and user-added value, the device syncs the first three times at a 3 min interval time period and then it syncs with the specified user sync interval time.

The following table summarizes fields and descriptions in the **Sync Policy** window.

TABLE 35. SYNC POLICY FIELDS

Item	Description	Default Policy Setting
Name	<p>Required. Enter a descriptive name for this policy. This is the text that will be displayed to identify this policy throughout the Admin Portal. This name must be unique within this policy type.</p> <p>Though using the same name for different policy types is allowed (e.g., Executive), consider keeping the names unique to ensure clearer log entries.</p>	Default Sync Policy
Status	Select Active to turn on this policy. Select Inactive to turn off this policy.	Active
Priority	<p>Specify a priority for this policy in relation to other custom policies of this type. Priority determines which policy is applied in the case of a conflict. For example, if a device has two labels assigned to it, and each label has a different sync policy, then the priority determines which policy is applied.</p> <p>Select "Higher than" or "Lower than" and select the relative policy from the drop-down list. Because priority applies only to custom policies, this setting is not available when you create the first custom policy of this type. Default policies are not included in prioritization.</p>	
Description	Enter an explanation of the purpose of this policy.	Default Sync Policy
Server IP/Host Name	Displays the IP address or host name of the Core instance that the Client will communicate with. This setting is completed automatically when the first phone registration is requested.	

TABLE 35. SYNC POLICY FIELDS (CONT.)

Item	Description	Default Policy Setting
Use TLS	Specify whether to use Transport Layer Security for interactions between Core and the Mobile@Work app (Apps@Work on Windows devices) installed on devices.	selected
Migrate Mobile@Work Client	<p>Select to migrate Mobile@Work for Android from using port 9997 without mutual authentication to using port 443 <i>with</i> mutual authentication. The device users do not need to re-register with Core.</p> <p>For more information, see "Migrating Mobile@Work for Android to use mutual authentication" in the <i>Core Device Management Guide for Android and Android Enterprise Devices</i>.</p>	
Sync While Roaming	<p>Specifies which data, if any, should be synchronized with Core while the device is roaming.</p> <p>All Activity and Content: Causes all activity and content to be synchronized while the device is roaming.</p> <p>Only Activity and SMS Content: Restricts synchronized data to activity and SMS content while the device is roaming. Eliminates synchronization of some data to reduce the cost of data transfer when additional charges may apply. This option is selected by default.</p> <p>Only Roaming Status: Restricts synchronized data to roaming status while the device is roaming. Eliminates synchronization of most data to minimize the cost of data transfer when additional charges may apply. Synchronizing roaming status ensures that location data is communicated to the server and that roaming alerts can be generated in a timely fashion. International roaming alerts are not generated.</p>	Only Activity and SMS Content

TABLE 35. SYNC POLICY FIELDS (CONT.)

Item	Description	Default Policy Setting
	<p>No Sync: Prevents all data from being synchronized while the device is roaming. Roaming alerts may not be generated by Event Center in a timely fashion because the device cannot communicate its roaming status. Thus, if international roaming alerts have been configured, the Mobile@Work app (Apps@Work on Windows devices) on the device generates a local roaming alert.</p>	
Android Notification Mechanism	<p>Specifies the type of notification for device updates.</p> <p>Google Cloud Messaging: Device depends on Google Cloud Messaging (GCM) to receive notifications and updates from Core.</p> <p>Notification URL: Device uses the push notification URL to receive update notifications.</p> <p>Auto: Depending on the state of the device it will choose one of the notification mechanisms described above.</p> <hr/> <p> To configure the Android notification mechanism, mutual authentication must be enabled. See "Mutual authentication between devices and Mobile Core" in the <i>Core Device Management Guide for Android and Android Enterprise Devices</i>.</p>	Auto
Mutual Certificate Authentication Renewal Window	<p>Enter the number of days prior to the expiration date that you want to allow devices to renew their identity certificate used for mutual authentication with Core. Enter a value between 1 and 60.</p> <p>A blank value defaults to 60 days.</p> <p>Related topics</p> <p>"Mutual authentication between devices and Core" in the Core Device Management Guide.</p>	60

TABLE 35. SYNC POLICY FIELDS (CONT.)

Item	Description	Default Policy Setting
Heartbeat Interval	<p> Heartbeat Interval on iOS is only supported when the app is in use (not running in the background). As such, using the heartbeat interval on iOS is not recommended.</p> <hr/> <p>Specify the maximum amount of time that the Mobile@Work app (Apps@Work on Windows devices) will wait before sending a request to Core to confirm that the client and server are connected.</p> <hr/> <p> Mobile@Work (Apps@Work on Windows devices) does not connect to the server according to this interval unless the Client is Always Connected option is selected.</p> <hr/> <p>Core will close the network connection for clients that have been inactive for twice the interval specified for this setting, thereby reducing demand on Core.</p> <p>Why: Increasing the heartbeat interval can help preserve battery life. Decreasing the heartbeat interval helps Mobile@Work (Apps@Work on Windows devices) detect disconnection from the Core more quickly.</p>	14
Sync Interval	<p>Specify the frequency for starting the synchronization process between the device and Core.</p> <p>For iOS devices only:</p> <p>This setting determines how often Core sends a check-in notification to iOS devices, which determines the frequency of jailbreak detection.</p> <hr/> <p> Decreasing this interval requires additional resources that may increase the drain on phone batteries.</p>	240
iOS Location-Based Wakeups Interval	For iOS devices only:	15 minutes

TABLE 35. SYNC POLICY FIELDS (CONT.)

Item	Description	Default Policy Setting
	<p>Specifies the minimum duration between attempts to send iOS device details to Core. This duration is adhered to when iOS brings Mobile@Work into memory following major location change events.</p> <p>When enabled, this setting specifies the minimum time period between server polling intervals if a significant location change wakes the app. For example, if the location-based wakeup interval is set to 15 minutes, but a significant location change wakes a given app at 5, 12, and 16 minute intervals, the app will only poll Core at the 16 minute interval. The default interval is 15 minutes.</p> <p>See “iOS location-based wakeups interval and syncing with Core” in the <i>Core Device Management Guide for iOS and macOS Devices</i>.</p>	
MTD wakeup interval	Enter an MTD iOS wake-up interval in minutes. This interval determines how often Mobile@Work wakes up and scans an iOS device. Setting this field to a low interval value, such as fifteen minutes, is more taxing on the device's battery than setting it at a higher interval value such as 60 minutes.	60 minutes
Client is Always Connected	<p>This feature is not supported on iOS devices.</p> <p>Specify whether Mobile@Work (Apps@Work on Windows devices) should remain connected to Core during the sync interval. Keeping the client connected ensures timely communication between Mobile@Work (Apps@Work on Windows devices) on the device and Core. You might consider disabling this feature if battery drain becomes an issue. See “Android devices and the Client Is Always Connected” in the <i>Core Device Management Guide for Android and Android Enterprise Devices</i>.</p>	Disabled



Managing Labels

This section describes basic operations to perform with labels, including how to apply a device to a label, search for a label, remove a device from a label, filter labels, as well as create and edit labels. In addition, complex operations are provided such as how to create a dynamic label, calculating devices impacted by changing or removing labels, and creating a label based on custom LDAP user attributes.

Apply to Label	191
Device label search	192
Using search for device labels	192
Remove from label	193
Applying a device to a label	193
Removing a device from label	194
Using labels to establish groups	194
Using search for device labels	195
Notifying all device users using labels	196
Default labels	197
Filter and manual type labels	199
Editing Labels	201
Copying a label to a new label	203
Viewing devices currently associated with a label	203
Associating a filter with a label	204
Searching for device labels	205
Calculating devices impacted by changing or removing labels	207
Creating a label based on custom LDAP user attributes	210

- ["Apply to Label" on the next page](#)
- ["Device label search" on page 192](#)
- ["Using search for device labels" on page 192](#)
- ["Remove from label" on page 193](#)
- ["Applying a device to a label" on page 193](#)
- ["Removing a device from label" on page 194](#)
- ["Using search for device labels" on page 195](#)
- ["Using labels to establish groups" on page 194](#)
- ["Default labels" on page 197](#)
- ["Filter and manual type labels" on page 199](#)

- ["Creating labels" on page 199](#)
- ["Editing Labels" on page 201](#)
- ["Copying a label to a new label" on page 203](#)
- ["Viewing devices currently associated with a label" on page 203](#)
- ["Associating a filter with a label" on page 204](#)
- ["Deleting labels" on page 209](#)
- ["Searching for device labels" on page 205](#)
- ["Viewing label use" on page 209](#)
- ["Calculating devices impacted by changing or removing labels" on page 207](#)
- ["Creating a label based on custom LDAP user attributes" on page 210](#)

Apply to Label

Applying a device to a label tags the phone as part of the associated group. When you specify a label for an action, you perform the action on all devices having the label. See ["Using labels to establish groups" on page 194](#) for more information on labels.

Procedure

1. Log into the Admin Portal.
2. Go to **Device & Users > Devices**.
3. Select the check box for the device.
4. Click **Apply To Label** from the **Actions** menu.
5. Select the label to apply from the **Apply To Label** dialog.

Only labels that have not already been associated with this device will be displayed. For example, iOS devices are automatically applied to the iOS label, Android devices to the Android label, and so on. Also, automatic labels that are not applicable to this device do not appear in the list. For example, the Windows label and Windows Phone label will not appear for a device from a different platform.

6. Click **Apply**.

For more information about labels for Android enterprise, see the *Core Apps@Work Guide*.

Device label search

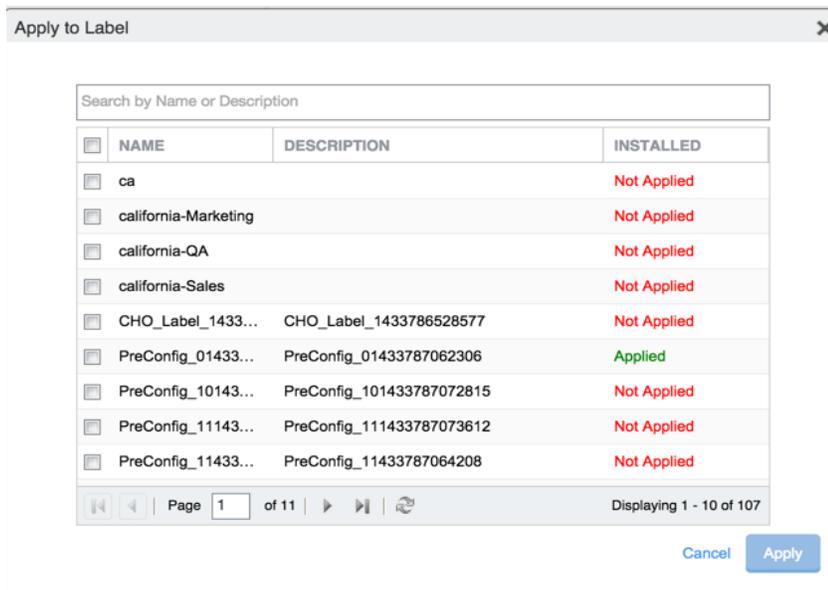
When you apply devices to labels, you can use search criteria to find the label you want to use. You no longer need to scroll through the list to find the label you want.

Using search for device labels

When you apply devices to labels, you specify search criteria to filter the label list to the label you want to use.

Procedure

1. From the Admin Portal, go to **Devices & Users > Devices**.
2. Check one or more devices that you want to apply to a label.
3. In **Apply to Label**, enter one or more characters in **Search by Name or Description**.



The screenshot shows a dialog box titled "Apply to Label" with a search bar and a table of results. The search bar contains "ca". The table has columns for NAME, DESCRIPTION, and INSTALLED. The results are as follows:

NAME	DESCRIPTION	INSTALLED
ca		Not Applied
california-Marketing		Not Applied
california-QA		Not Applied
california-Sales		Not Applied
CHO_Label_1433...	CHO_Label_1433786528577	Not Applied
PreConfig_01433...	PreConfig_01433787062306	Applied
PreConfig_10143...	PreConfig_101433787072815	Not Applied
PreConfig_11143...	PreConfig_111433787073612	Not Applied
PreConfig_11433...	PreConfig_11433787064208	Not Applied

At the bottom of the dialog, there are "Cancel" and "Apply" buttons. The page indicator shows "Page 1 of 11" and "Displaying 1 - 10 of 107".

For example, enter "ca" to find all labels that begin with the letters "ca". Core displays the labels that match what you entered.

4. Check the label you want to use from the search results.
5. Click **Apply**.

Remove from label

Removing a device from a label removes the following from the device:

- The tag that makes it a part of the associated group (see [Using labels to establish groups](#) for more information on labels).
- Policies applied to that label.
- Apps applied to that label.
- iBooks applied to that label (iOS only).

Procedure

1. Log into the Admin Portal.
2. Go to **Device & Users > Devices**.
3. Select the check box for the device or devices.
4. Click **Actions > Remove From Label**.
5. Select the label from the **Remove From Label** dialog.
6. Click **Remove**.

Applying a device to a label

Applying a device to a label tags the device as part of the associated group. When you specify a label for an action, you perform the action on all devices having the label. See "[Using labels to establish groups](#)" on the [next page](#) for more information on labels.

Procedure

1. From the Admin Portal, go to **Device & Users > Devices**.
2. Select the check box for the device.
3. Click **Apply To Label** from the **Actions** menu.

4. Select the label to apply from the **Apply To Label** dialog.

Only labels that have not already been associated with this device will be displayed. For example, iOS devices are automatically applied to the iOS label, Android devices to the Android label, and so on. Also, automatic labels that are not applicable to this device do not appear in the list. For example, the Windows label and Windows Phone label will not appear for a device from a different platform.

5. Click **Apply**.

Removing a device from label

Removing a device from a label removes the following from the device:

- The tag that makes it a part of the associated group (see [Using labels to establish groups](#) for more information on labels).
- Policies applied to that label.
- Apps applied to that label.
- iBooks applied to that label (iOS only).

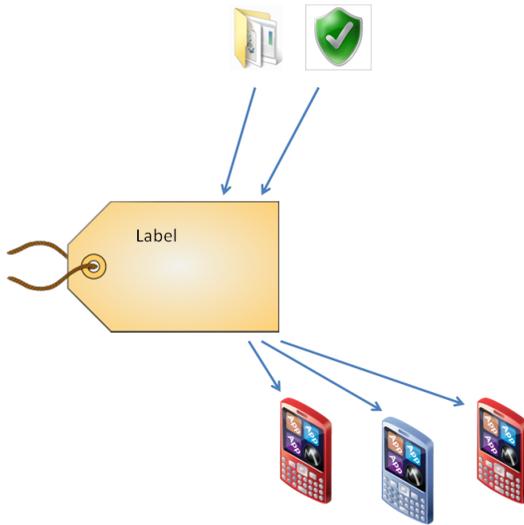
Procedure

1. From the Admin Portal, go to **Device & Users > Devices**.
2. Select the check box for the device or devices.
3. Click **Actions > Remove From Label**.
4. Select the label from the **Remove From Label** dialog.
5. Click **Remove**.

Using labels to establish groups

You can use labels for devices, apps, policies, and events. This process forms a group. For example, you might create a label called "Executives" to tag devices belonging to employees at the executive level. You can then locate all of these devices quickly in a search, or apply policies based on whether a device has this label.

FIGURE 1. USING LABELS TO ESTABLISH GROUPS



Using search for device labels

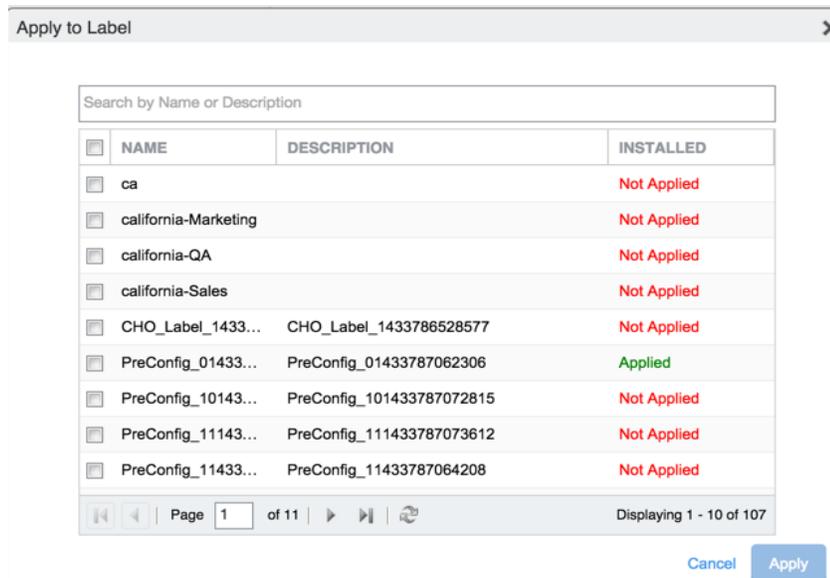
When you apply devices to labels, you specify search criteria to filter the label list to the label you want to use.

Procedure

1. Log into the Admin Portal.
2. Go to **Devices & Users > Devices**.
3. Check one or more devices that you want to apply to a label.

- In **Apply to Label**, enter one or more characters in **Search by Name or Description**.

FIGURE 1. SEARCH BY NAME OR DESCRIPTION.



For example, enter "ca" to find all labels that begin with the letters "ca". Core displays the labels that match what you entered.

- Check the label you want to use from the search results.
- Click **Apply**.

Notifying all device users using labels

You can send out push notifications to all device users using labels. Core releases prior to 11.1.0.0 limited the number of broadcast messages to 200 at a time. From Core 11.1.0.0 through the most recently released version as supported by MobileIron, the Core **Send Message To Label(s)** option sends messages in batches of 200, until all device users are notified.



This option is applicable only for devices that support the **Send Message** action.

Procedure

1. From the **Devices & Users > Labels** page, select a label that contains the users you want to notify.
2. From the Actions menu, select **Send Message**. The Send Message To Label(s) dialog box opens.
3. Select the message mode: **Email**, **Push Notification**, or **Data Channel**. **Push Notification** is the default.
4. Enter your message text into the Message field (plain text only).
5. Click **Send Message**. The message is sent to all devices.

Monitoring and verifying the sent messages

You can monitor the process of sending a message to a large number of device users from the **Logs > Audit Logs** page.

Procedure

1. After sending a message to device users through a label, go to **Logs > Audit Logs** page.
2. In the **Filters** pane, set the **Action Date** to include when you sent the message.
3. Open the **Device** filters from the list of filters.
4. Select **Send Message** to display the audit logs for your message.

Default labels

The following system labels are always available, by default:

TABLE 36. DEFAULT LABELS

Label	Description
All-Smartphones	Automatically applied to all devices at registration.
Android	Automatically applied to registered devices that have the Android platform selected during registration.
Company-Owned	Automatically applied to registered devices that have the Company check box selected during registration.
Employee-Owned	Automatically applied to registered devices that have the Employee check box selected during registration.
iOS	Automatically applied to registered devices that have the iOS platform selected during registration.
iOS and tvOS	Automatically applied to registered devices that have the iOS and tvOS platform selected during registration.
macOS	Automatically applied to registered Apple devices that have macOS selected during registration.
Signed-Out	Automatically applied to any multi-user iOS device that does not have a signed-in user.
tvOS	Automatically applied to registered devices that have the tvOS platform selected during registration.
Windows	Automatically applied to Windows 10 devices.
Windows Phone	Automatically applied to Windows Phone devices.



You cannot delete default labels.

Filter and manual type labels

Labels fall into the following categories:

- Filter
- Manual

Filter labels (also called dynamic labels) use specific criteria to define a group of devices. Manual labels have no criteria associated with them; you select each device associated with a manual label.

When you initially create a label, it is stored as a filter label. If you use the Advanced Search feature to specify the criteria for a label, then it remains a filter label. Otherwise, if you select devices in an Admin Portal screen and apply the label to them, then the label becomes a manual label.

Creating labels

There are two ways to create a label:

- Use Advanced Search and save the criteria to a new label.
- Create a new label.

Procedure

1. From the Admin Portal, go to **Device & Users > Labels**.
2. Click **Add Label**. The Add Label window opens.

The screenshot shows the MobileIron CORE Admin Portal interface. The top navigation bar includes 'Dashboard', 'Devices & Users', 'Admin', 'Apps', 'Policies & Configs', 'Services', 'Settings', and 'Logs'. The 'Devices & Users' section is active, with sub-tabs for 'Devices', 'Users', 'Labels', 'ActiveSync', and 'Apple DEP'. The 'Labels' tab is selected, and an 'Add Label' button is visible. The main content area displays a table of existing labels with columns for NAME, DESCRIPTION, TYPE, and CRITERIA. One label is visible: 'All-Smartphones' with description 'Label for all devices irrespective of OS', type 'Filter', and criteria '"common.retired"=false'. An 'Add Label' modal window is open in the foreground, containing the following fields and options:

- Name:** A text input field containing 'Label Name'.
- Description:** A text area for entering a description.
- Type:** Radio buttons for 'Manual' and 'Filter' (selected).
- Criteria:**
 - Buttons for 'All' and 'Any' (selected).
 - Text: 'of the following rules are true'.
 - Fields for 'Field', 'Operator', and 'Value' with a '+' icon to add more rules.
 - Text input for a search expression: 'Type search expression here. E.g (platform = "iOS" AND status = "Pending")' with a 'Reset' link.
 - Checkbox: 'Exclude retired devices from search results' (checked).
- Table:** A table with columns 'DISPLAY NAME', 'CURRENT PHONE NUMBER', 'MODEL', and 'STATUS'.
- Buttons:** 'Cancel' and 'Save' at the bottom right.

Refer to the guidelines in the [Add label window](#) table to complete the fields.

3. Click **Save**. You can now apply this label to devices, policies, and configurations. See "[Applying a device to a label](#)" on page 193.

Add label window

The following system labels are always available, by default:

TABLE 37. ADD LABEL FIELDS

Field	Description	Example
Name	<p>Enter a unique name that clearly identifies the purpose of the label. The following characters are allowed when entering a label name. All other characters, including spaces, are prohibited.</p> <ul style="list-style-type: none"> • Letters (uppercase and lowercase) • Numbers (0-9) • Dashes (-) • Underscores (_) • Periods (.) • At sign (@) • Dollar sign (\$) • Hash tag (#) • Extended ASCII/UTF-8 	ExecutiveTeam
Description	Provide additional meaning and usage information.	For members of the executive staff reporting to John Smith
Type	<p>By default, the type is Filter.</p> <p>Change it to Manual if you want to manually associate devices with the label.</p>	
Criteria	<p>If the type is Filter, use the query builder to create a search expression that defines the devices to apply the label to. Alternatively, manually enter a search expression. The matching devices are automatically displayed.</p> <p>For information and help with manual and dynamic searches, see Device field definitions in the Managing Devices chapter of the <i>Core Device Management Guide</i> for your operating system.</p>	("common.platform"="IOS" OR "common.platform"="Android") AND "common.home_operator_name"="AT&T"

Editing Labels

In **Device & Users > Labels**, you can edit:

- The name and description of any existing label.
- The type of a label (manual or filter).

 You can change a label's type only if it is not assigned to any devices.

- The criteria of a filter label.

If you change a label's type from manual to filter, you can use the query builder to define the filter.

However, if you are **changing** a filter label's criteria, only manual editing is available to edit the criteria. The query builder is not available.

You can determine the string for the criteria by first navigating to **Devices & Users > Devices** and clicking **Advanced Search**. Use the user interface to create the criteria string and then copy it for pasting into the **Edit Label** dialog.

 You cannot edit the criteria of pre-defined labels such as All-SmartPhones, Android, iOS, Company-Owned, and so on.

Procedure

1. From the Admin Portal, go to **Device & Users > Labels**.
2. Select a label.
3. Click **Actions > Edit Label**.
4. Edit the name and/or description.

The label name must be unique.

5. Click **Manual** or **Filter** to change the label type.

 **IMPORTANT:** You can change a label's type only if it is not assigned to any devices.

6. For filter labels, edit the criteria.

If the type was already filter, manually edit the criteria.

If you changed the type to filter, either use the query builder or manually edit the filter.

7. Click **Save**.

Copying a label to a new label

You can copy a label to a new label. You choose which device space the new label will belong to. This action is especially useful when creating similar labels in multiple spaces.

Procedure

1. Log into the Admin Portal.
2. Go to **Device & Users > Labels**.
3. Select a label.
4. Click **Actions > Save as**.
5. Enter a name for the new label.
6. Enter a description for the new label.
7. Choose which device space the new label will belong to. You select the device space from the set of device spaces for which you have the role **Manage label**.



If the global space is the only defined space, the dialog does not display the space drop-down box.

Although you cannot modify the criteria when copying a filter label, you can edit the criteria of the new label.

8. Click **Save**.

Viewing devices currently associated with a label

You can view the devices currently associated with a specific label.

Procedure

1. Log into the Admin Portal.
2. Go to **Device & Users > Labels**.
3. Click the link in the **View Devices** column.

The devices are filtered by the label, and shown on the Devices page (**Device & Users > Devices**).

4. To return to the Labels page, click the **Labels** tab.

Associating a filter with a label

You can use the Advanced Search feature in the **Device & Users > Devices** page to associate a filter (search) with a label. The resulting dynamic label represents the devices defined by the filter at a given time.

Example: Creating a label for devices by operator

You can create a label for all devices having a specific operator.

Procedure

1. Log into the Admin Portal.
2. Go to **Device & Users > Devices**.
3. Click **Advanced Search**.
4. In the **Field** drop-down, type operator and select either Current Operator Name or Home Operator Name.
5. Select a logical operator from the operator drop-down.
6. Select the Country and Operator.
7. Click **Save To Label**, and provide a name and description for the new label.

Example: Creating a label for devices by LDAP group

You can create a label for all devices associated with a specific LDAP group.

Procedure

1. Log into the Admin Portal.
2. Go to **Device & Users > Devices**.
3. Click **Advanced Search**.
4. In the Field drop-down, click to expand **User Fields > LDAP > Groups**.

5. Select **Name**.
6. Select a logical operator from the operator drop-down.
7. Select an LDAP group from the drop-down.



The drop-down shows the LDAP groups that are selected in **Services > LDAP**, in the **LDAP Groups** section of the **Modifying LDAP Settings** dialog.

8. Click **Save To Label**, and provide a name and description for the new label.

Example: Creating a label with filter criteria for a specific device

When you create a label with filter criteria for a specific device storage capacity, you must use storage values in bytes only.

To create a label for all devices associated with a device storage capacity:

1. Log into the **Admin Portal**.
2. Go to **Device & Users > Devices**.
3. Click **Advanced Search**.
4. In the **Field** drop-down, click to expand **Common Fields > Storage Capacity**.
5. Enter the capacity in bytes.
6. Select a logical operator from the operator drop-down: **<**, **>**, or **=**.
7. Click **Save To Label**, and provide a name and description for the new label.

Searching for device labels

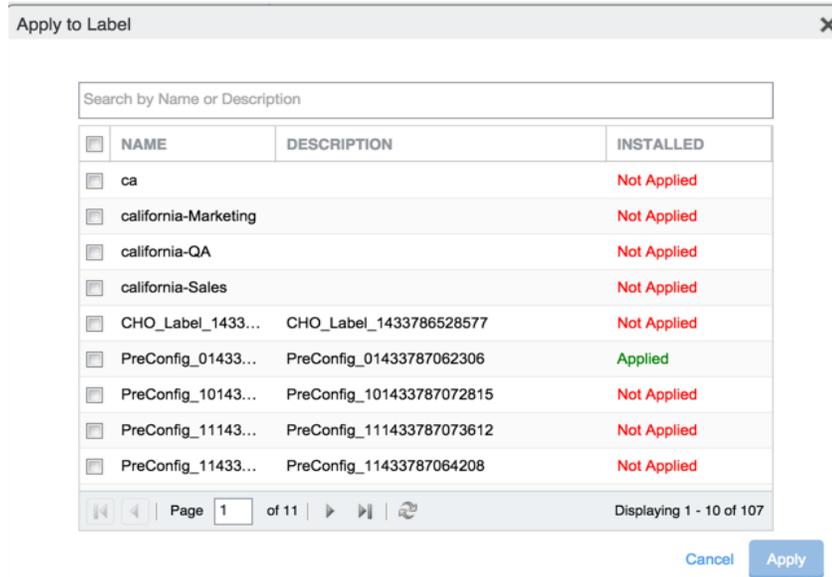
When you apply devices to labels, you can specify search criteria rather than scroll through the list when selecting the label.

Procedure

1. From the Admin Portal, go to **Devices & Users**.
2. Select **Devices**.

3. Check one or more devices that you want to apply to a label.
4. In **Apply to Label**, enter one or more characters in **Search by Name or Description**.

FIGURE 1. SEARCH BY NAME OR DESCRIPTION



For example, enter "ca" to find all labels that begin with the letters "ca". Core displays the labels that match what you entered.

5. Check the label you want to use from the search results.
6. Click **Apply**.

Calculating devices impacted by changing or removing labels

Before you change what is applied to a label, or delete a label, you would like to know if that action impacts a large number of devices. Knowing that a large number of devices are affected by an action might cause you to rethink your actions.

You can set a threshold for the number of devices impacted by the following actions:

- Removing a configuration from a label.
- Deleting a label.

If either of these actions impact the number of devices you set as a threshold or more, you are notified, and can decide to modify or cancel the action.

The default threshold Core uses is 100 devices, which can be changed in **Settings**.

If deleting a label or removing a configuration from a label affects a number of devices that exceeds the threshold, you receive an alert that:

- Lets you know that the action would affect more than the threshold number of devices.
- Asks you if you want to cancel the action or continue.
- Requests that you enter a reason for the action if you continue.

For example, if you set the threshold to 90 devices, alerts are sent if 91 or more devices are affected by the action.

Setting the device impact threshold

The default number of devices for the Device Impact Threshold is 100. You can set this to a different number, if your Core implementation requires.

Procedure

1. Log into the Admin Portal.
2. Go to to **Settings > System Settings**.
3. Go to **General > Enterprise**, enter the number of devices in **Device Impact Threshold**.
4. Click **Save**.

The correct threshold differs among deployments. What you are determining is the number of devices you will put at risk with a label action without wanting a warning first and a reason that you can track if the action causes problems.

For some deployments that number can be ten devices. For other deployments it may be 500 devices. If you are not certain what number to specify:

- Start with the default number, 100 devices.
- If many label actions impact more than 100 devices, you might find the warning messages occur too often.
- If you want to understand the impact of all label and configuration label removals for some period of time, you can lower **Device Impact Threshold** to monitor the effects of these actions.

Responding to label action alerts

If either removing a configuration from a label or deleting a label affects more than the set threshold of devices, a message displays letting you know that the action affects more than the threshold number of devices and asking you for guidance.

Procedure

1. If you decide to cancel the action, click **No**.
2. To complete the action, enter the reason why you are continuing in **Reason**, and then click **Yes**.

Viewing label use

Core provides a consolidated view of all places each label is used in your Core instance. You can view how many of the following objects are applied to each label:

- Devices
- Users
- Policies
- Configurations
- Apps

Viewing your label use helps you understand how changing, adding, or deleting labels will affect your managed devices.

Procedure

1. From the Admin Portal, go to **Device & Users > Labels**.
2. Click the up arrow next to the label that you want to investigate.
3. The expanded display lists the number of devices, users, policies, configurations, and apps applied to the label.
4. To return to the label list, click the down arrow for the label you are viewing.

Deleting labels

You can delete unused or out of date labels.

Procedure

1. Log into the Admin Portal.
2. Go to **Device & Users > Labels**.
3. Select the label you want to delete.
4. Click **Delete**.



Default labels cannot be deleted. See [Default labels](#).

Creating a label based on custom LDAP user attributes

If you have one or more custom user attributes defined in your LDAP settings, you can create a label using the custom attributes.

There are two types of custom LDAP attributes available in advanced search.

- Custom 1 through Custom 4 are always available in the field list in advanced search, and appear as "custom1" through "custom4".
- Custom Attribute 1, Custom Attribute 2, and so on, are available in advanced search only if they are assigned in LDAP settings. These custom attributes appear in the field list as the value they were assigned in the setting. For example, if Custom Attribute 1 is set to "Manager" in LDAP settings, it appears in the advanced search field list as "Manager", under **User Fields > LDAP > User Attributes**.

To view the custom attributes in the LDAP settings, go to **Services > LDAP**. Click the LDAP instance to open the LDAP details. If you make changes to LDAP settings, LDAP is synced automatically.

Procedure

1. Log into the Admin Portal.
2. Go to **Device & Users > Devices**.
3. Click the advanced search icon.
4. In the query builder, click **Field** and select the custom attribute, found under **User Fields > LDAP > User Attributes**.

Complete your search criteria using the query builder or by manually editing the expression.

5. Click **Save To Label**.
6. Type a name and description for the new label.



Using the Dashboard

This chapter provides procedures for the most common uses of Core:

Dashboard overview	211
Dashboard charts	211
Arranging the devices dashboard charts	214
Changing the charts included in the dashboard	214
Devices associated with chart sections in the devices dashboard	214
Displaying device lists from devices dashboard charts	215
Adding an app chart to the apps dashboard	217

Dashboard overview

The **Dashboard** page provides a snapshot of the devices known to Core. Also, if apps analytics is enabled, the apps dashboard shows information about app usage.

Each chart on the devices dashboard can be displayed as a:

- Pie chart
- Bar chart
- Table

To switch among the chart choices, select the chart-type icon at the bottom of the chart. Note that the **New Device Registrations** chart and the **Pending Device Registrations** chart are displayed only as tables.

Core continuously updates the information in the devices dashboard.

Dashboard charts

The dashboard displays charts offering device and app insights and analytics. The devices dashboard is always displayed. The apps dashboard is displayed only if you have enabled it.

The devices dashboard contains the following charts:

TABLE 38. DEVICES DASHBOARD CHARTS

Chart	Description
Device By Status	Displays the percentage of phones having each registration status (for example, Pending).
Device By Compliance	Displays the percentage of devices that are in compliance with the assigned policy.
Device By OS Type	Displays the percentage of devices running each supported operating system.
Device By OS Version	Displays the percentage of devices running each version of the supported operating systems.
Device Roaming By Country	Displays the percentage of devices that are roaming for each country.
Device By Ownership	Displays the percentage of devices that are company-owned and the percentage of devices that are user-owned.
Device By Operator	Displays the percentage of devices each service provider reported, including Wi-Fi.
New Device Registrations	Displays the latest phones to begin the registration process.
Pending Device Registrations	Displays the phones that have a status of Pending.
Devices by Phishing Protection Enabled	Displays the number of users that have / have not enabled MTD Phishing Protection on their device. For more information, see the <i>Mobile Threat Defense solution Guide for Core</i> .

The apps dashboard includes the following charts:

TABLE 39. APPS DASHBOARD CHARTS

Chart	Description
Top installed apps	Displays the top ten most installed apps. You can filter the chart by All, Public, and In-House. You can click the data points to drill down to specific app details.
Top 5 rated in-house Apps	Displays the "Top 5 Rated In-House Apps" in Apps@Work for iOS, macOS, and Android across all managed devices. The chart includes the rating and the number of raters for each app. You can click the data points to drill down to specific app details.
In-House app distributions requiring install	Displays the 5 in-house apps most needing action to improve their distribution.
Public app distributions requiring install	Displays the 5 public apps most needing action to improve their distribution.
App distribution	The single app chart displays the number of devices the app (or a specific version of the app) has been distributed to and is eligible to be distributed to.

Viewing the App Dashboard

In order to view the Apps tab in the Dashboard:

- The app analytics feature needs to be enabled.
- The user with global space permissions needs to be granted View App Dashboard or View Device Dashboard permissions.

If the app analytics feature is disabled, the Apps tab will not display in the Dashboard. For how to set app analytics, see "EXEC PRIVILEGED mode commands" in the *Core Command Line Interface (CLI) Reference*.

Procedure

1. Go to **Admin > Admins**.
2. Select the user, click **Action > Edit Roles**. The Edit Roles dialog box opens.
3. Scroll to the App Management section.
4. Select the View app dashboard check box.

5. The permissions display in the right panel of the dialog box.
6. Click **Save**.

Arranging the devices dashboard charts

You can drag & drop the devices dashboard charts from one position to another on your screen, to align the charts in any order you choose. When you move a chart, you move it to the position of one of the other charts or an empty spot on the dashboard.

Procedure

1. Log into the Admin Portal.
2. Click on the dashboard chart name.
3. Drag the chart to the new position.

Changing the charts included in the dashboard

You can remove any of the charts from the dashboard and add them back to the dashboard when you choose.

Procedure

1. Log into the Admin Portal.
2. Click the X in the upper-right corner of the chart to remove it from the dashboard.
3. Click **Add**, select a chart from the list, and then click **Add Chart** to add a closed chart to the dashboard.

The chart is added as the last chart on your display.

Devices associated with chart sections in the devices dashboard

Each category of information in a dashboard chart can be displayed as a list of devices.

Example:

- If you display the **Device By OS Type** chart as a bar graph, clicking the bar for Android displays all the registered devices using Android. Similarly, clicking the bar for iOS or Windows displays all the registered devices using iOS or Windows.
- If you display **Device By Status** as a pie chart, clicking one of the chart slices displays a list of the devices included in that chart slice.



The device list page also displays the advanced search box with the query that produces the list of devices associated with the chart category.

Listing the devices associated with a category in a dashboard chart:

- Identifies which devices belong to a category.
- Enables more-informed decisions about device actions.

Using the Advanced Search box displayed with the device list you can:

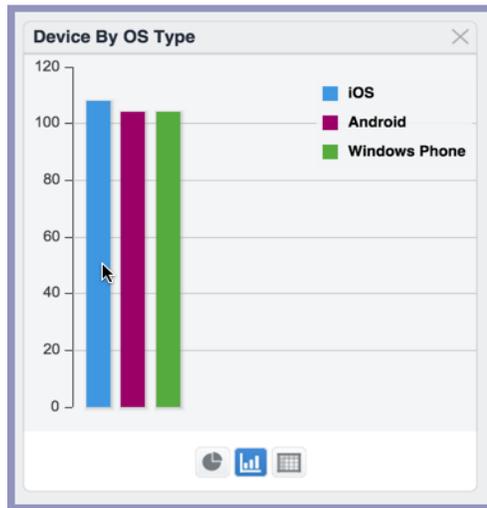
- Generate precise category-based search criteria.
- Modify the category search criteria.
- Save the category search criteria as a label.
- Rerun the query using the Search button.

Displaying device lists from devices dashboard charts

You can use the devices dashboard charts to display device lists by specified criteria.

Procedure

1. In the Admin Portal, go to **Dashboard > Devices**.
2. Click a category from one of the dashboard charts (for example, click a slice in a pie chart or a bar in a bar graph).



The devices included in that category are displayed in a separate window.

The advanced search box displays at the top of this window.

3. Click the **X** at the top of the window when you are done.

The advanced search box displays the filter that generates the device list. You can:

- Use the filter to rerun the search.
- Modify the filter to generate a different set of devices.
- Save the filter as a label, creating a dynamic label that represents the devices defined by the filter at a given time.
- Click the **Reset** button to delete any changes you made to the original query.
- Click the **Clear** button to delete the current query criteria.

Adding an app chart to the apps dashboard

When the apps dashboard is enabled, you can add additional charts for individual apps.



When changing the name of an app in the App Catalog after creating an app chart with that app, the new app name is not reflected in the app chart. If you want the new app name to be reflected in the app chart, you must delete the app chart with that app and create a new app chart.

Procedure

1. In the Admin Portal, select **Dashboard**.
2. Select **Apps**.
3. Click **Add**.
4. Select the Chart Type from the drop-down list.
5. In the text field provided, type the name of the app for which you want to create a single app chart.

A list of apps matching the name in the text field appears under **Selected App**.

6. Select the app in under **Selected App**.
7. Click **Add Chart**.

A new chart with the title **App Distribution** appears in the apps dashboard for the selected app

Deleting an app chart

You can delete an app chart by clicking the **X** in the upper right-hand corner of the app's **App Distribution** chart.