Core 11.4.0.0 Device Management Guide

for Windows Devices

October 2021

For complete product documentation, see:
Ivanti product documentation page

Contents

New features and enhancements

This release includes the following new features and enhancements.

- There are no new features for Windows with this release.

Managing Devices

This section addresses the management of devices.

- "Registering Devices" below
- "General management of devices" on page 30
- "Searching for Devices" on page 34
- "Securing Devices" on page 63

Registering Devices

A device is available for management by Core after it has been registered by a device user or administrator.

The topics in this section include the following advanced topics:

- "Registration methods" on the next page
- "Terms of service" on page 12
- "Invite users to register" on page 17
- "ActiveSync device registration" on page 19
- "Managing operators and countries" on page 19
- "Specifying eligible platforms for registration" on page 22
- "Setting the registration PIN code length for device user registration" on page 22
- "Customizing registration messages" on page 23
- "Configuring the default ownership for newly registered devices" on page 29
- "Disabling analytics data collection" on page 29

Refer to the *Getting Started with Core* for the most commonly used registration topics, such as:

- Single device registration
- Bulk device registration
- Tracking registration status
- Restricting the number of devices a user registers
- Registration considerations

Registration methods

Registering a device designates it for management by Core.

ⓘ Support for Android 5.0 and 5.1 has ended. Core server will still allow existing registered devices with Android 5.0 / 5.1 to run.

Before you begin

"Setting the registration PIN code length for device user registration" on page 22

The following registration methods are available:

- "Admin invites users to register" below
- "Admin registers ActiveSync devices" on page 12

The process resulting from these methods may vary by device OS.

Admin invites users to register

For users who are mobility savvy and do not require significant assistance, you can send an invitation and enable them to register their own phones. You can send an invitation to multiple users from the Users Management screen. The invitation includes instructions on how to log into the user portal to register phones.

The administrator needs to know the following information for the device:

- Phone number (if any)
- Country

- Platform

Related topics

"Invite users to register" on page 17

- Schedule email reminders, see "Customizing registration messages" on page 23

Registration restrictions for Android devices

From the **Device Registration** page, you can specify conditions that Android devices must meet to qualify for registration. You can limit Android devices by operating system (OS) version, security patch level, or by manufacturer and model.

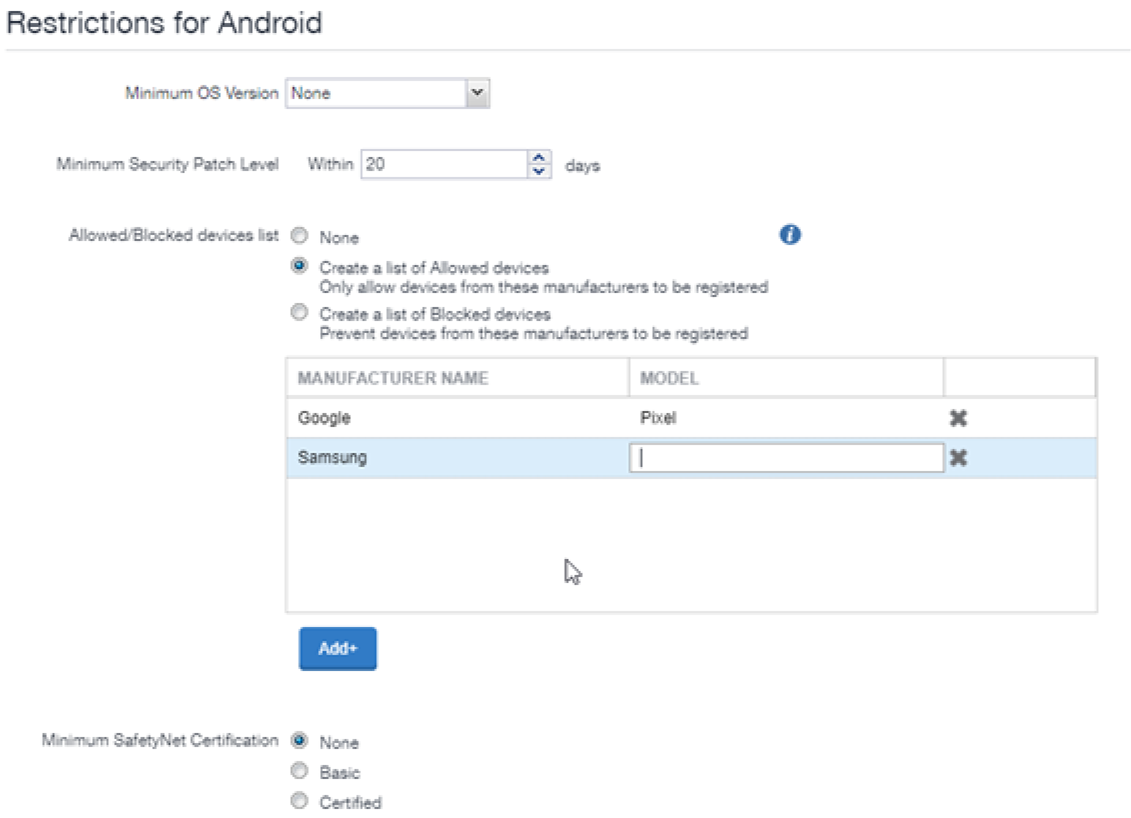
Before you begin

- Complete "Registration methods" on the previous page.

Procedure

1. From the **Settings > System Settings > Users & Devices > Device Registration** page, scroll down to the **Restrictions for Android** section. Choose from these optional filter settings:

   FIGURE 1. REGISTRATION RESTRICTIONS FOR ANDROID DEVICES



Restrictions for Android

Minimum OS Version: None

Minimum Security Patch Level: Within 20 days

Allowed/Blocked devices list:
○ None
● Create a list of Allowed devices
Only allow devices from these manufacturers to be registered
○ Create a list of Blocked devices
Prevent devices from these manufacturers to be registered

MANUFACTURER NAME	MODEL	
Google	Pixel	✖
Samsung		✖

Minimum SafetyNet Certification:
● None
○ Basic
○ Certified

2. **Minimum OS version**: Select a minimum OS version from the drop-down menu from Android 6.0 or supported newer versions. The default is **None**.

3. **Minimum Security Patch Level**: Enter an integer specifying within how many days a device can be non-compliant for the minimum security patch level before rejecting the device. The default is **None**.

4. **Allowed/Blocked devices list**: The options are:

   - **None**: The default. Do not create an Allowed or Blocked devices list.
   - **Create a list of Allowed devices**: Only allow devices of these makes and models to be registered.
   - **Create a list of Blocked devices**: Prevent devices of these makes and models to be registered.

   To enter specific manufacturers and models, click **Add+** to open text fields in the **Manufacturer Name** and **Model** columns. Enter allowed or restricted device information.

5. Click **Save**.

Related topics

"Disabling the QR code and registration URL" on page 30

Users register additional devices

Once a device has been registered, an authorized user can use the user portal to register additional devices without administrative help. This is often used with adding devices for users who do not require assistance.

Prerequisites

- Users must have the **User Portal** role assigned, with the **Device Registration** option enabled.
- The user needs to know the following information for the device:
  - phone number (if any)
  - country
  - platform

Related topics

"Self-service User Portal" on page 430

Admin registers ActiveSync devices

If you have a Sentry configured, then you can see the devices that are connecting to your ActiveSync server. To incorporate these devices into your Core inventory, you can use the Register button in the ActiveSync Associations screen. This is often used with devices accessing email via ActiveSync.

Prerequisites

- Sentry must be installed and configured.
- The user (local or LDAP) associated with the device must be available for selection at the time of registration.
- For iOS, Android, and Windows devices, the User Portal role must be assigned to the user.
- You need to know the following information for the device:
  - phone number (if any)
  - country code
  - platform

Related topics

"ActiveSync device registration" on page 19

Terms of service

You can optionally define terms of service text to be displayed to users during:

- Device registration on iOS, macOS, Android, and Windows devices.
- Logging into AppConnect apps on iOS and Android devices.

Device users must accept the terms of service before they can continue with registration or with accessing AppConnect apps.

You can search for users by terms of service acceptance and date of acceptance. You can create one terms of service agreement for each supported language. The same terms of service text is used for both registration and AppConnect app access.

Regarding terms of service during registration:

- Presenting the terms of service is part of the registration process when using Mobile@Work. Users must accept the terms of service agreement in order to complete registration.
- Configuring a terms of service agreement or updating it applies only to users who register after you complete the configuration. Previously registered users do not accept the terms of service agreement. However, you can require existing users to accept the terms of service agreement by retiring their devices and requesting them to re-register.
- If both custom terms of service and the privacy policy are enabled, users will have to accept the privacy policy first.

Regarding terms of service for accessing AppConnect apps:

- In addition to providing the terms of service text, you must enable terms of service on the AppConnect global policy.
- Also on the AppConnect global policy, you indicate whether:
    - Users must accept the terms of service each time they are prompted for their AppConnect passcode or biometric authentication. If you update the terms of service text for a user's language, the user sees the updated text on all subsequent AppConnect logins.
    - The user must accept the terms of service only once. However, if you update the terms of service text for a user's language, on the next AppConnect login, the user is prompted once more to accept the terms of service.
- If you delete the terms of service, but do not disable it on the AppConnect global policy, users continue to be prompted to accept the terms of service with whatever the last terms of service text was.
- For information about enabling terms of service when logging into AppConnect apps, see "Configuring the AppConnect global policy" in the *AppConnect Guide for Core*.

Creating a terms of service agreement

Before you begin

Set up the system default language as described in "Setting the system default language " on page 428.

If there is no terms of service available in the primary language of a given device, or if more than one agreement is defined for more than one device language on a device, the terms of service agreement defaults to the system default language.

Procedure

1. In the Admin Portal, go to **Settings > System Settings > Users & Devices > Registration**.
2. Scroll down to the **End User Terms of Service** section.
3. Click **Add+**.
4. Select the language for the terms of service.
5. For **Type**, select **System** for iOS, macOS and Android devices. Select **AAD enrollment** for Windows devices.
6. Enter the text for the terms of service.

   You can adjust the editor to use rich or plain text by clicking the Source Edit icon.
7. Click **Save**.
8. Optionally, repeat steps 3 through 6 to add a terms of service agreement for each supported language, and for Windows devices versus iOS, macOS, and Android devices.

ⓘ To edit a terms of service agreement, click the **Edit** link next to the relevant language.

ⓘ To delete a terms of service agreement, click the **Delete** button next to the relevant language.

Related topics

"Register devices in AAD and MDM" on page 247

Searching for devices by terms of service agreement criteria

You can search for devices based on whether users have agreed to the terms of service, and the date on which terms of service were accepted.

The following table describes the searchable criteria related to terms of service. Corresponding fields are displayed on each device's Device Details tab.

TABLE 1. SEARCHABLE CRITERIA FOR TERMS OF SERVICE

Criterion	Description
Terms of Service Accepted	A false value means the user did not accept the terms of service at registration, which means the device was registered before a terms of service agreement was required, or a terms of service agreement was never configured. A true value indicates the device user accepted the terms of service agreement at registration.
Terms of Service Accepted Date	Filters for the exact time users accepted the terms of service agreement at registration. This search is useful if you want to locate the version of the terms of service agreement accepted by a specific user for a particular device.
AppConnect Terms of Service	The value **DECLINED** means the user did not accept the terms of service for using AppConnect, which means the device user logged into AppConnect before a terms of service agreement was required, or a terms of service agreement was never configured. The value **ACCEPTED** indicates the device user accepted the terms of service agreement when logging into AppConnect.
AppConnect Terms of Service Date	Filters for the exact time users accepted the terms of service agreement when logging into AppConnect. This search is useful if you want to locate the version of the terms of service agreement accepted by a specific user for a particular device.

Procedure

1. In the Admin Portal, go to **Devices & Users > Devices**.
2. Click **Advanced Search**.
3. Add one or more of the search rules regarding terms of service.
   a. From the **Field** drop-down list, select the field of interest:
      - **Common Fields > Terms of Service Accepted**.
      - **Common Fields > Terms of Service Accepted Date**.
      - **Common Fields > AppConnect Terms of Service**.
      - **Common Fields > AppConnect Terms of Service Date**.

b. Provide the appropriate value:

- **Terms of Service Accepted**: Select **true** or **false** in the **Select Value** field.
- **Terms of Service Accepted Date**: Enter the number of units in the **Value** field and select the units (such as days, weeks, or months) in the **Date** field.
- **AppConnect Terms of Service**. Enter **ACCEPTED** or **DECLINED** in the **Value** field
- **AppConnect Terms of Service Date**. Enter the number of units in the **Value** field and select the units (such as days, weeks, or months) in the **Date** field.

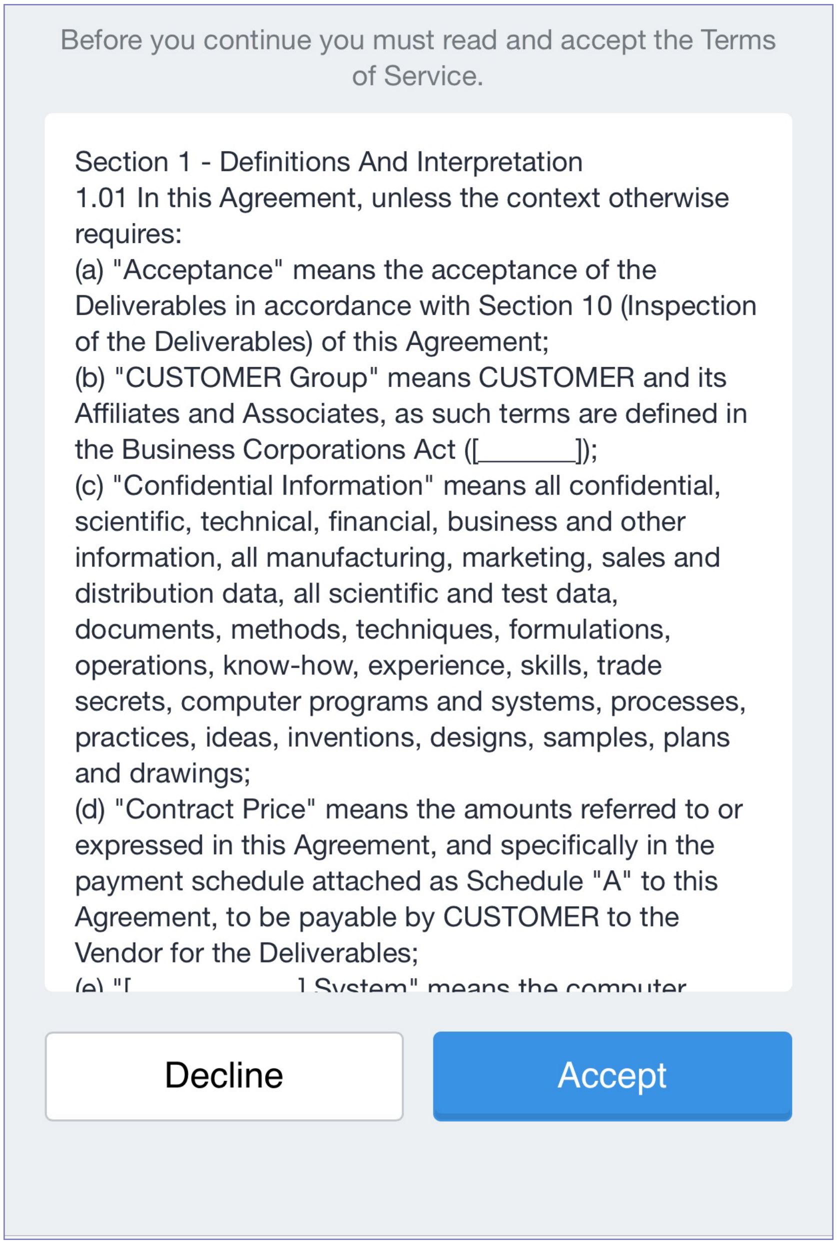
The search criteria you selected are displayed in the search field.

4. Click **Search**.
5. The results are displayed.
6. Optionally, save your search to a label by clicking **Save to Label**.
7. If Notes for Audit Logs is enabled, a text dialog box opens. Enter the reason for the change and then click **Confirm**. For more information, see "Best practices: label management" on page 402.

Terms of Service for users

Device users can easily scroll through and accept an administrator-defined terms of service agreement in their web browser or Mobile@Work client, as in the following example.

FIGURE 1. TERMS OF SERVICE FOR USERS



Before you continue you must read and accept the Terms of Service.

Section 1 - Definitions And Interpretation
1.01 In this Agreement, unless the context otherwise requires:
(a) "Acceptance" means the acceptance of the Deliverables in accordance with Section 10 (Inspection of the Deliverables) of this Agreement;
(b) "CUSTOMER Group" means CUSTOMER and its Affiliates and Associates, as such terms are defined in the Business Corporations Act ([_______]);
(c) "Confidential Information" means all confidential, scientific, technical, financial, business and other information, all manufacturing, marketing, sales and distribution data, all scientific and test data, documents, methods, techniques, formulations, operations, know-how, experience, skills, trade secrets, computer programs and systems, processes, practices, ideas, inventions, designs, samples, plans and drawings;
(d) "Contract Price" means the amounts referred to or expressed in this Agreement, and specifically in the payment schedule attached as Schedule "A" to this Agreement, to be payable by CUSTOMER to the Vendor for the Deliverables;
(e) "[   ] System" means the computer

Invite users to register

This feature is supported on macOS devices.

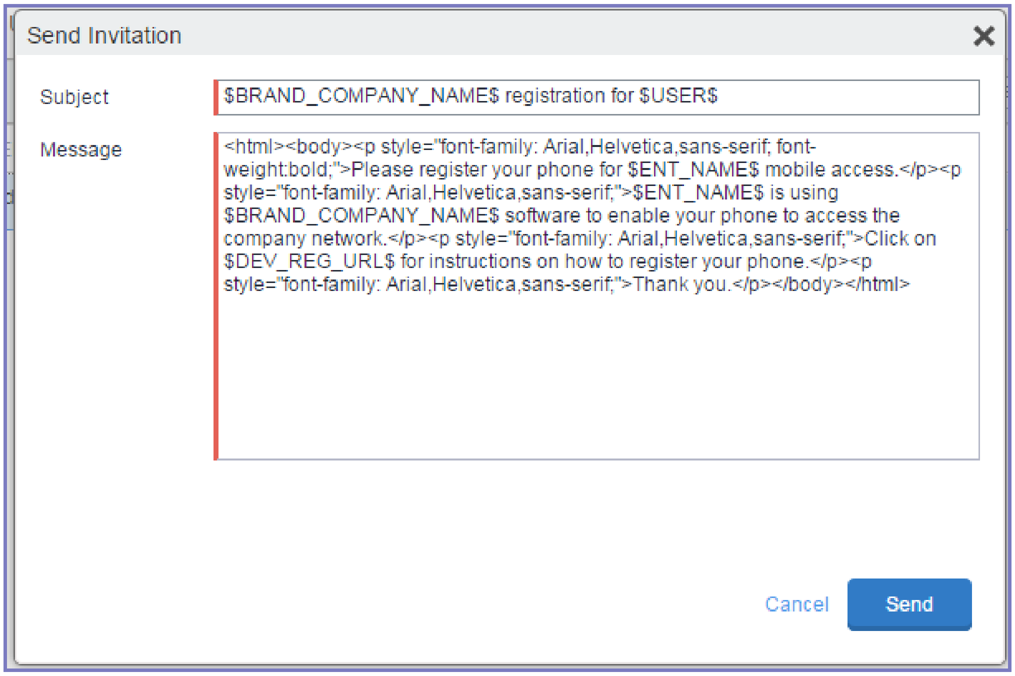
Administrators can invite users to perform self-service registration through the user portal. See "Self-service User Portal" on page 430 for information on this self-service user portal. The administrator sends invitations that provide the instructions necessary to complete the registration process.

Language-specific templates are not currently available for invitations.

See "Registration methods" on page 8 for points to consider before using this registration method.

Procedure

1. Go to **Devices & Users > Users**.
2. Select the type of user accounts you want to work with:
   a. Select **Authorized Users** from the To drop-down list to select from local user accounts.
   b. Select **LDAP Entities** from the To drop-down list to select users from the configured LDAP server.
3. Click the check box next to each user you want to invite.
4. Click **Actions** and then click **Send Invitation**.



Subject: $BRAND_COMPANY_NAME$ registration for $USER$

Message:

```
<html><body><p style="font-family: Arial,Helvetica,sans-serif; font-
weight:bold;">Please register your phone for $ENT_NAME$ mobile access.</p><p
style="font-family: Arial,Helvetica,sans-serif;">$ENT_NAME$ is using
$BRAND_COMPANY_NAME$ software to enable your phone to access the
company network.</p><p style="font-family: Arial,Helvetica,sans-serif;">Click on
$DEV_REG_URL$ for instructions on how to register your phone.</p><p
style="font-family: Arial,Helvetica,sans-serif;">Thank you.</p></body></html>
```

5. Review the default text for the invitation and make any changes.

   The text is displayed here with HTML markup. The user will receive the formatted version.

6. Click **Send**.

What the user sees

This registration method results in user notification via email. The email contains instructions for registering devices via the user portal. See "Self-service User Portal" on page 430 for information on what the user is expected to do to complete the registration process.

ActiveSync device registration

The **ActiveSync** view displays the devices that are accessing ActiveSync. This view is populated only if you have a Sentry configured. From this view, you can decide to register selected devices.

See "Registration methods" on page 8 for points to consider before using this registration method.

Procedure

1. Go to **Devices & Users > ActiveSync**.

2. Select a device to be registered.

3. Click **Actions > Register**.

4. See “Single device registration” in the ***Getting Started with Core*** for instructions on completing the registration process.

Managing operators and countries

Core provides a default list of operators for users to select from during registration. You can enable or disable operators to determine whether they appear in the list of operators displayed during registration of US devices and other devices having a country code of 1.

For non-US devices, country selection is an important part of the registration process. Core also provides a default list of countries enabled for registration purposes. You may need to adjust this list to enable additional countries.

This section explains how to customize displayed operators and countries.

Enabling operators

Enabling an operator displays it in the list of operators presented to users during registration.

Procedure

1. In the Admin Portal, go to **Services >Operators**. By default, the Operators screen shows only Enabled operators.
2. Select **Disabled** or **All** from the **Status** drop-down.
3. Click the check box next to each operator you want to enable.
4. Click **Actions > Enable**.

Enabling additional 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.

Procedure

1. In Admin Portal, go to **Settings > System Settings > Users & Devices > Registration.**
2. Scroll to the **Countries for Registration** section.
3. Select countries from the **Disabled Countries** list.
4. Click the arrow button to move them to the **Enabled Countries** list.
5. Click **Save**.

Disabling operators

Disabling an operator removes it from the list of operators presented to users during registration.

Procedure

1. In the Admin Portal, go to **Services >Operators**.
2. By default, the **Operators** screen shows only Enabled operators.

3. Click the check box next to each operator you want to disable.

4. Click **Actions > Disable**.

Filtering operators

You can use filters to display only those operators you want to work with in the Operators screen. You can:

- Search for a specific operator
- Display operators by country
- Display operators by status

Searching for an operator

Procedure

1. Enter a portion of the operator's name in the **Search by Name** field.
2. Click the search icon to display the matching operators.
3. Click the x that appears in the search field to return to the default display.

Displaying operators by country

To narrow the list of operators by country, select a country from the **Country** drop-down list.

Displaying operators by status

To display operators by status, select from the **Status** drop-down list. The following options are available:

- Enabled
- Disabled
- All

Specifying eligible platforms for registration

In some cases, you may want to exclude from registration all devices of a particular platform. For example, if corporate policy dictates that a particular device platform will not be supported, you may want to prevent users from selecting the platform during self registration. Likewise, you may want to prevent help desk personnel from mistakenly registering the unsupported platform in the Admin Portal.

Procedure

1. In Admin Portal, go to **Settings** > **System Settings** > **Users & Devices** > **Registration**.
2. Scroll to the **Platforms for Registration** section.
3. In the **Enabled Platforms** list, select the platform you want to exclude.

   Shift-click platforms to select more than one.
4. Click the left arrow button to move the selected platforms to the **Disabled Platforms** list.
5. Click **Save**.

   All methods of registration now exclude the selected platforms.

Setting the registration PIN code length for device user registration

This feature is supported on Android, iOS and macOS devices.

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 Admin Portal, go to **Settings** > **System Settings** > **Users & Devices** > **Registration**.
2. Select a **Registration PIN code Length,** which is the minimum length for the PIN (6-12 characters).
3. Click **Save**.

Limit for failed attempts to enter a registration password

After the sixth failed attempt to enter a registration password, Core locks the device user’s account for 30 seconds. The device user sees a message stating that the account is locked and will be released after the specified interval.

PIN-based authentication for all available Windows devices

If only PIN registration is enabled, password is not required. However you will be asked to enter your email during registration.

If the user removes the account from the Windows device, a new PIN is required to re-register the device.

If the PIN expires you must first retire the device in the Admin Portal, then re-register the device. This generates a new PIN. Re-provisioning is not supported (**Devices & Users > Devices > Action > Actions > Re-provision Device**).

The User Portal role is required even if PIN registration is configured.

Customizing registration messages

This feature is supported on iOS, macOS, Windows, and Android devices.

The registration process is a critical part of deployment. You can customize the registration messages involved in this process by editing the registration templates. Registration templates enable you to specify content and basic formatting using HTML markup.

Core sends multiple messages related to registration:

- registration SMS
- registration email and reminder email
- post registration email

These messages may vary by:

- platform
- language

In addition, messages may vary by device type:

- phones
- PDAs

To accommodate this range of messages:

- Separate registration templates are provided for each language/platform combination.
- Each registration template contains separate text for each registration message type.
- Each registration template contains separate text for phones and PDAs.
- For when Core discovers device users that have not downloaded the MDM profile, reminder email scheduling capabilities are provided

Viewing registration templates

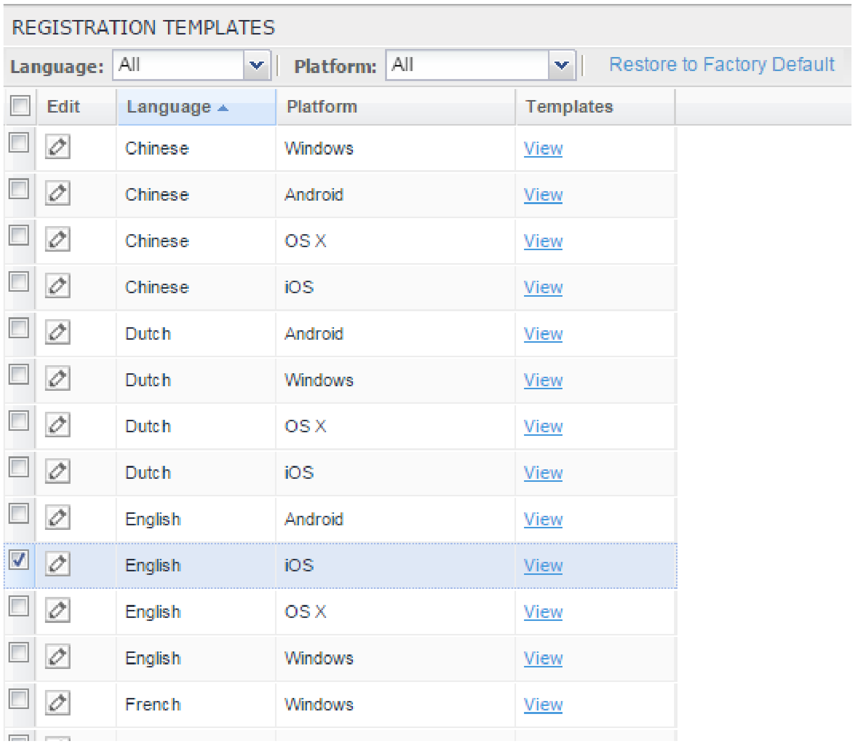
To view Core message templates:

1. In Admin Portal, click **Settings > Templates**.
2. Select **Registration Templates**.
3. Click the **View** link for the template you want to view.

Editing registration messages

To edit registration messages:

1. In Admin Portal, select **Settings > Templates > Registration Templates**.
2. Select the template you want to edit and click the **Edit** pencil icon.



REGISTRATION TEMPLATES

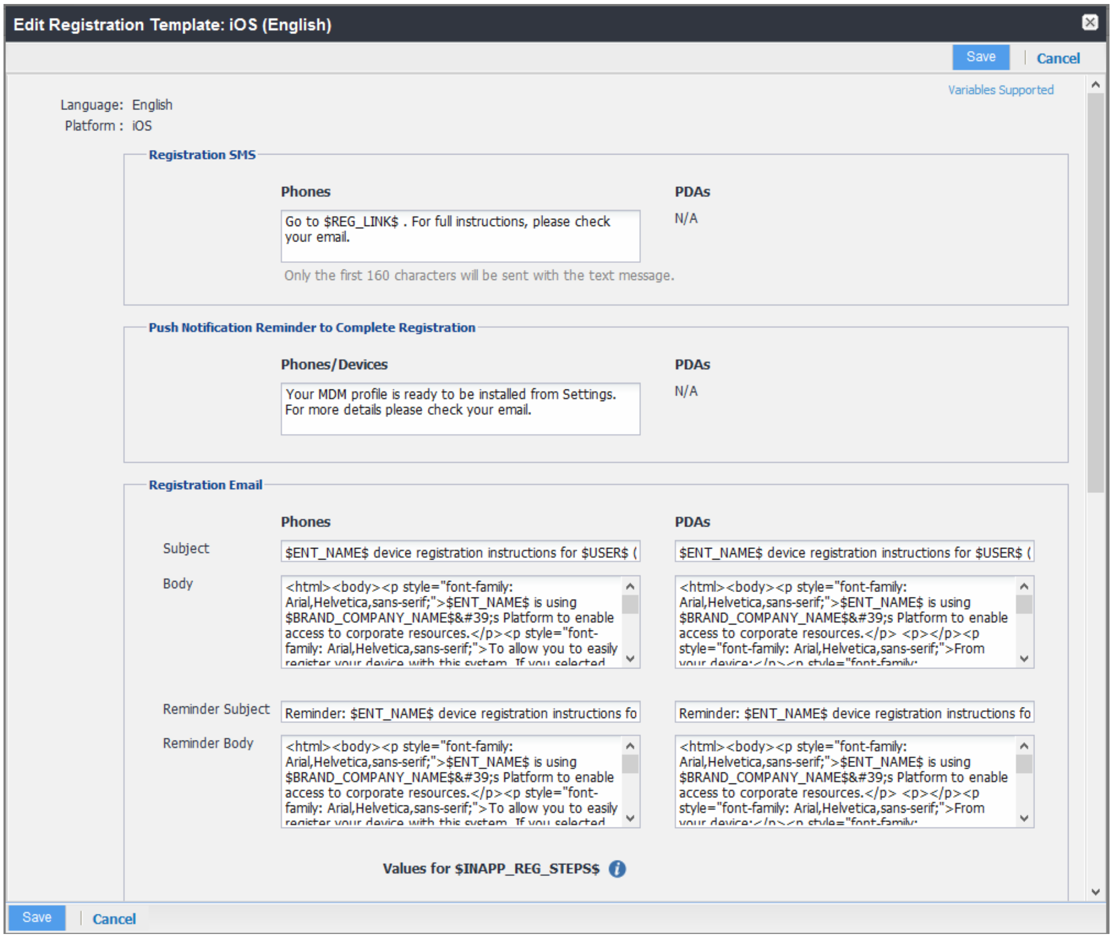
Language: All | Platform: All | Restore to Factory Default

□	Edit	Language ▲	Platform	Templates
□	✎	Chinese	Windows	View
□	✎	Chinese	Android	View
□	✎	Chinese	OS X	View
□	✎	Chinese	iOS	View
□	✎	Dutch	Android	View
□	✎	Dutch	Windows	View
□	✎	Dutch	OS X	View
□	✎	Dutch	iOS	View
□	✎	English	Android	View
☑	✎	English	iOS	View
□	✎	English	OS X	View
□	✎	English	Windows	View
□	✎	French	Windows	View

Registration messages are displayed with the HTML markup that provides the basic formatting for the content.

3. Make changes to the displayed registration messages.

Do not add the <head> html tag in the registration template fields.



Edit Registration Template: iOS (English)

Language: English
Platform : iOS

Registration SMS

Phones

Go to REG_LINK . For full instructions, please check your email.

Only the first 160 characters will be sent with the text message.

PDAs

N/A

Push Notification Reminder to Complete Registration

Phones/Devices

Your MDM profile is ready to be installed from Settings. For more details please check your email.

PDAs

N/A

Registration Email

Phones

Subject: ENT_NAME device registration instructions for $USER$ (

Body:

```
<html><body><p style="font-family:
Arial,Helvetica,sans-serif;">$ENT_NAME$ is using
$BRAND_COMPANY_NAME$&#39;s Platform to enable
access to corporate resources.</p><p style="font-
family: Arial,Helvetica,sans-serif;">To allow you to easily
register your device with this system. If you selected
```

Reminder Subject: Reminder: ENT_NAME device registration instructions fo

Reminder Body:

```
<html><body><p style="font-family:
Arial,Helvetica,sans-serif;">$ENT_NAME$ is using
$BRAND_COMPANY_NAME$&#39;s Platform to enable
access to corporate resources.</p><p style="font-
family: Arial,Helvetica,sans-serif;">To allow you to easily
register your device with this system. If you selected
```

PDAs

Subject: ENT_NAME device registration instructions for $USER$ (

Body:

```
<html><body><p style="font-family:
Arial,Helvetica,sans-serif;">$ENT_NAME$ is using
$BRAND_COMPANY_NAME$&#39;s Platform to enable
access to corporate resources.</p> <p></p><p
style="font-family: Arial,Helvetica,sans-serif;">From
your device:</p><p style="font-family:
```

Reminder Subject: Reminder: ENT_NAME device registration instructions fo

Reminder Body:

```
<html><body><p style="font-family:
Arial,Helvetica,sans-serif;">$ENT_NAME$ is using
$BRAND_COMPANY_NAME$&#39;s Platform to enable
access to corporate resources.</p> <p></p><p
style="font-family: Arial,Helvetica,sans-serif;">From
your device:</p><p style="font-family:
```

Values for $INAPP_REG_STEPS$

4. Click the **Variables Supported** link in the right corner of the dialog box to display a guide to the supported variables. See "Using variables in registration messages" below for additional details.

5. Click **Save**.

Next steps

"Customizing registration messages" on page 23

Using variables in registration messages

Each field in a registration template has a set of supported variables, most of which are required. Supported and required variables also differ by OS. Use the following variables to guide your customization. You can also click the Variables Supported link to display this information. **All variables except $BRANDING_COMPANY_NAME$ are also required in the specified field.**

Registration message variables

The following table gives the of variables used in types of registration messages.

TABLE 2. VARIABLES USED IN DIFFERENT TYPES OF REGISTRATION MESSAGES

Type	Supported Variables
Registration SMS (Phones)	REG_LINK
Registration Email	
Subject (Phones)	ENT_NAME, $USER$, $PHONE$
Subject (PDAs)	ENT_NAME, $USER$, $PHONE$
Body (Phones)	ENT_NAME, $BRAND_COMPANY_NAME$, $PHONE$, $PASSCODE$, $PASSCODE_TTL$, REG_LINK
Body (PDAs)	$PASSCODE$, $PASSCODE_TTL$, REG_LINK
Reminder Subject (Phones)	ENT_NAME, $USER$, $PHONE$
Reminder Subject (PDAs)	ENT_NAME, $USER$, $PHONE$
Reminder Body (Phones)	ENT_NAME, $BRAND_COMPANY_NAME$, $PHONE$,$PASSCODE$, $PASSCODE_TTL$, REG_LINK
Reminder Body (PDAs)	$PASSCODE$, $PASSCODE_TTL$, REG_LINK
Post-Registration Email	
Subject (Phones)	$BRAND_COMPANY_NAME$, $USER$, $PHONE$
Subject (PDAs)	$BRAND_COMPANY_NAME$, $USER$, $PHONE%
Body (Phones)	$BRAND_COMPANY_NAME$, $PHONE$
Body (PDAs)	$BRAND_COMPANY_NAME$, $PHONE$

Variables used inside registration messages

The following table gives the description of variables used inside registration messages.

TABLE 3. DESCRIPTION OF VARIABLES IN REGISTRATION MESSAGES

Variable	Description
$BRAND_COMPANY_NAME$	An internal variable.
ENT_NAME	The name of the organization using Core to secure the device. See the field **EnterpriseName** in **Settings > System Settings > General > Enterprise**.
$INAPP_REG_STEPS$	Combines $SERVER_URL$, the user's LDAP password, $PASSCODE$, and $USER_ID$.
$PASSCODE$	The registration PIN generated for the device by Core.
$PASSCODE_TTL$	The number of hours that the registration PIN remains valid. See the field **Passcode Expiry** in **Settings > Systems Settings > Users & Devices > Registration.**
$PHONE$	The phone number associated with the device.
REG_LINK	The URL that users access to complete the registration process (i.e., https://server name:port/v/passcode for Windows and other platforms).
$SERVER_URL$	The Core server address used for registration.
$USER$	The name of the user associated with the device, as displayed in Core.
$USER_ID$	The user ID for the user associated with the device, as defined in the user account on Core.

Filtering registration messages

In the Registration Templates page, you can filter registration messages by:

- language
- platform

Procedure

1. If you want to restrict the templates displayed based on language, select the preferred language from the **Language** list.
2. If you want to restrict the templates displayed based on device platform, select the preferred platform from the **Platform** list.

Restoring registration messages to default content

To restore a registration message to the default content provided by Ivanti:

1. In the **Settings > Registration Templates** page, select the template you want to restore.
2. Click **Restore to Factory Default**.

Configuring the default ownership for newly registered devices

By default, all newly registered devices are configured as company-owned. You can change this default setting to employee-owned (and back) on the Registration page.

Alternatively, you can change the ownership of a device after registration by:

- selecting **More** > **Change Ownership** in the User Portal. For more information, see "About changing device ownership in the user portal" on page 434.
- selecting **Devices & Users** > **Devices** > **Actions** > **Change Ownership** in Core.

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

   OR

   Employee owned
3. Click **Save**.

Disabling analytics data collection

Ivanti collects data to analyze the use of Core to help us provide customer support, perform bug fixes, improve product functionality and reliability and fulfill obligations to our customers. You can view details about data collected in our product privacy notice: https://www.ivanti.com/company/legal/privacy-policy.

The data is collected from:

- Mobile@Work
- Apps@Work

Procedure

1. In Core, go to **Settings** > **System Settings** > **General** > **Analytics**.
2. Select the **Disable data collection from Mobile@Work and Apps@Work** check box.
3. Click **Save**. A confirmation dialog opens.
4. Click **Yes** to confirm or **No** to cancel and allow analytics data collection.

Disabling the QR code and registration URL

When new users are invited to register with Core, a QR code and registration URL display by default. If your organization prefers not to show users a QR code and registration URL, an administrator can disable the feature from the **Device Registration** page of the Core admin portal.

Procedure

1. Go to **Settings** > **System Settings** > **Users & Devices** > **Device Registration** page.
2. Deselect **Display QR Code and Registration URL** by clicking it.
3. Click **Save**.

Related topics

To disable the user Activity page in the self-service portal (SSP), see "Disabling device history logs in the self-service user portal" on page 443.

General management of devices

Communicating with devices

You can send a message to any known user. Messages can be sent via text, email or push notifications. Only users having enrolled devices can receive push notifications.

You can have multiple message modes selected; if you do not want to have multiple message formats done, be sure to deselect the check box.

You can monitor the process of sending a message to a large number of device users from the **Logs > Audit Logs** page. For more information, see "Monitoring and verifying the sent messages" in *Getting Started with Core*.

Sending a message to devices

Procedure

1. Go to **Devices & Users > Devices**.
2. Select the device(s) you want to message.
3. Click **Actions > Send Message**.
    - To send an SMS message, select the **SMS** check box and enter text into the **Message (Plain text)** field. For Android devices only, the text will be sent via the data channel if the Mobile@Work client has an active connection to Core.
    - To send an email, select **Email** and enter text into the **Message (Plain text)** and **Subject (Email Only)** fields. See also: "Sending a company-branded email" below.
    - To send a push notification, select the **Push Notification** check box and enter text into the **Message (Plain text)** field.

> A push notification message can also include URLs which the users can access.

4. (Optional) You can select the **Data Channel** option to use for any of the message modes.
5. Click **Send Message**.

Sending a company-branded email

You can send a company-branded HTML email to single or bulk users. You can also send branded email messages using **Settings > Templates** - see "Customizing Event Center messages" on page 382.

Before you begin

- Create your company-branded email in HTML format in a text editor.

Procedure

1. Go to **Devices & Users > Devices**.
2. Select the device(s) you want to send your email to.
3. Click **Actions > Send Message**.

   The Send Message dialog box opens.
4. Select the **Email** check box.
5. Select **Send HTML email instead of plain text email**. More fields display.
6. Copy and paste the HTML email into the **Message (HTML Email)** field.
7. (Optional) You can select the **Data Channel** option to use for any of the message modes.
8. Click **Send Message**.

App Updates for Android Enterprise

Auto-updates for apps on Android Enterprise devices can be set through a Maintenance Window. and app updates on Android Enterprise devices can also be controlled by fields for setting an app update priority and for defining a minimum version for apps. The two fields are found within App Settings for individual apps and are called **Update Priorty** and **Minimum Version Code**.

Auto-Update Maintenance Window

You can choose to set a Maintenance Window for auto-updates that will override the update settings users configure. By default this option is unchecked.

When active (checked), the start time and duration options appear, they are implemented based on the local time of the device. The maintenance window can be set at any time and will ignore the following constraints: device is charging, device is idle (not actively used), the app to be updated is not running in the foreground. This does not affect the network constraint, which is managed separately.

It can take up to 24 hours for an app update to be added to the Android update queue. After an app is added, it will be updated automatically the next time the device is in the maintenance window if the network constraint is met (the device is connected to a Wi-Fi network). As a result, it can take up to 48 hours for an app to update after a maintenance window is set.

Update Priority

The **Update Priority** field provides the ability to control the app updates behavior on Android Enterprise Devices. This option allows admins to set the priority of updates, providing control of when the app is updated on a device. A drop-down list holds the Options:

- **High Priority** setting forces updates on the device immediately after it is available.
- **Postpone for 90 days** delays app updates so updates are not applied until 90 days after the update is available.
- **Default** mode allows app updates to be available as decided by the Google Play store.

Minimum Code Version

This option sets the minimum version of the app for a given device. If a lower version of the app is installed, then the app will be auto-updated according to the auto-install constraints, instead of waiting for the regular auto-update. You can set a minimum version code for at most 20 apps per device

ⓘ Warning: use of this attribute might affect apps in active use. To get the version codes for apps, please contact the app developer or refer to the example below.

Considerations:

- AE modes supported: Work Profile, Work Managed, and Work Profile on Company Owned Devices
- Apps supported: Public and Private Channel apps on Google Play Store
- As defined by specification, the minimum app version code is a 7 digit numeric code (1234567) which is the minimum version of the app to be installed on the device.

Example:

Installed version of the Whatsapp App is 2.19.10.15 and the latest version available is 2.21.18.17, the minimum version code an admin could enter in EMM console could look like 2210000. In this case app will be upgraded to 2.21.18.17 meeting the minimum version criteria specified by admin. Admins should note this functionality forces an immediate app upgrade and could force an active app session to close abruptly for the upgrade to complete.

Considerations for both Update Priority and Minimum Code Version

ⓘ When the App Update Mode and Minimum Version Code is modified on an app, it is applied to ALL devices which has the app distributed to.

ⓘ The app update applies to public and private apps hosted on Google Play Store. These options are not available for in-house apps.

Searching for Devices

The **Devices** page in the Admin Portal, offers both basic and advanced searching features. The basic search features provide a way to find devices or users using a limited set of criteria. The Advanced search features allow you to create complex search queries using the full set of available criteria. You can also apply advanced search criteria to a new or existing/unassigned or existing/unused label.

The topics in this chapter include the following advanced topics:

- "Basic searching" on the next page
- "Advanced searching" on page 36
- "Using the query builder" on page 56
- "Using a manually edited search expression" on page 57
- "Using both the query builder and manual editing" on page 57
- "Negative operators with advanced search" on page 59
- "Clearing an advanced search" on page 61
- "Searching for retired devices" on page 62
- "Searching for blocked devices" on page 62
- "Saving a search criterion to a label" on page 62

Refer to the *Getting Started with Core* for the most commonly used topics for managing devices, such as:

- Using the Dashboard
- Creating custom attributes

- Deleting retired devices

Basic searching

You can quickly search for devices based on the following criteria:

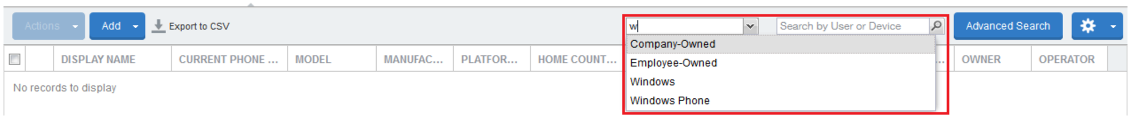
- Label
- User Principal/ID
- User Email Address
- User First/Last Name

To search by label, you can:

- select the appropriate label name from the **Labels** list.
- enter the initial letters of the label name in the **Labels** list.

  The list changes to show only label names containing the letters you entered.

FIGURE 1. SEARCH BY LABEL



No records to display

To search by the other criteria, select any label in the **Labels** list then use the following syntax in the **Search by User or Device** field:

- uid:<User Principal/ID>
- mail:<User Email Address>
- name:<User First/Last Name>

The prefixes mail: and name: are optional. All others are required. For example, to find the devices registered with the email address jdoe@ivanti.com, you can enter the following: mail:jdoe@ivanti.com or or just jdoe@ivanti.com.

Advanced searching

As data sets get larger, it is increasingly important to have a powerful search. You can use advanced search to build complex queries using the full set of available criteria (see "Using the query builder" on page 56 and "Using both the query builder and manual editing" on page 57.) You can also create a new label using the advanced search criteria.

To access advanced search:

1. Log into the Admin Portal.
2. Go to **Device & Users** > **Devices**.
3. Click the **Advanced Search** button located at the top right, above the table to display the query builder.
4. Enter search criteria using the query builder, or type the search expression directly. See "Device field definitions" on the next page.
5. Click **Search**. Verify your results.
6. (Optional) Click **Save to Label** button. This will save your new search query as a new label and in **Devices & Users** > **Labels**, you can utilize this new label as a filtered label.
7. If Notes for Audit Logs is enabled, a text dialog box opens. Enter the reason for the change and then click **Confirm**. For more information, see "Best practices: label management" on page 402.

Searchable fields

To see the complete list of searchable fields in the query builder:

1. Click **Field** to see the categories
2. Click **Expand All**.

The fields are organized alphabetically into the following categories for convenience:

- Device fields: apply to device type based on their operating system.
- OS-specific fields: apply to devices of the selected platform.
- User fields: apply to the device’s user, including LDAP fields for groups and custom attributes.

Device field definitions

This section covers the device field definitions found in the **Devices & Users > Devices** page. They also display in the Advanced Search field on the same page.

TABLE 4. DEVICE FIELD DEFINITIONS

Device Type	Field	Description
Android Fields	Admin Activated	True / false if device activated by admin.
	Android Automated Enrollment (This field is valid for Core 10.6.0.0 or supported newer versions.)	Once automated Android registration is completed, the following values display: • Google Zero Touch • Knox Mobile Enrollment • Non Zero Touch AE Enrollment - this is for Managed Devices / Device Owner types (afw#, QR code, NFC) • Unknown - this value displays if versions before Core 10.6.0.0 were used. This means the "In-App Registration Requirement field in Settings > System Settings > Users & Devices > Device Registration was used. It can also mean that an old client was used with Core version 10.6.0.0 or later.
	Android Client Version Code	Version code of the client.
	Android for Work Capable	True if the device is Android Enterprise capable, otherwise false.
	Attestation	Result of Samsung Attestation.
	Brand	Brand of the device.
	C2DM Token	C2DM token of the device if present, otherwise blank.
	Code Name	Code name of the Mobile@Work client

TABLE 4. DEVICE FIELD DEFINITIONS (CONT.)

Device Type	Field	Description
	Developer Mode	True if the Android device has Developer mode enabled, otherwise false. This is reported on all Android device configurations and also on Knox.
	Device	Brand name of device, for example, Mako.
	Device Encryption Status	Device encryption status.
	Device Roaming Flag	True if the device is roaming, otherwise false.
	Elapsed Time Since Reboot (minutes)	Indicates, in minutes, the amount of time since the device was last rebooted.
	File encryption	True if the Android device has enabled file encryption, otherwise false. This is reported on all Android device configurations and also on Knox.
	GCM/FCM Token Present	GCM token of the device if present, otherwise blank.
	Google Device Account Present	True if the device has a Google Device Account (eg: Android Enterprise), false otherwise.
	ICCID	Integrated Circuit Card Identifier number.
	Kiosk Enabled	True if the device is kiosk enabled, otherwise false.
	Manufacturer OS Version	Manufacturer OS version.
	MDM Enabled	True if MDM is enabled, otherwise false.
	Media Card Capacity	Amount of memory capacity of the media / SD card.
	Media Card Free	Amount of free memory on the media / SD card.
	Multi MDM	Indicates true/false.
	OS API Level	The Android OS API level. See https://developer.android.com/studio/releases/platforms for more details.

TABLE 4. DEVICE FIELD DEFINITIONS (CONT.)

Device Type	Field	Description
		This number is used so administrators can use a numerical comparison of OS versions.
	OS Build Number	OS build number.
	OS Update Path	OS Update Path.
	OS Update Status	OS Update Status.
	OS Version	Lists the OS version of the device.
	Password/PIN Days Before Expiring	Represents the number of days before the password / PIN will expire. This numerical value is controlled by the Security policy's Maximum Password Age field value. This field is a dynamic field, its value decreases every day by 1 until the password / PIN is renewed. At renewal, the value returns to the original number stated in the Maximum Password Age field and starts a new daily count-down. See "Working with default policies" on page 93.
	Platform Flags	Internal string representing the capabilities of the Mobile@Work application.
	Registration Status	Registration status of the device. Registration Status can be used as part of a dynamic label evaluation and criteria for tier compliance. In the **Select Type** drop-down, select one of these options: • Device Admin • Device Admin Not Required • Work Managed Device • Managed Device with Work Profile • Work Profile • Work Profile for Company Owned Device

TABLE 4. DEVICE FIELD DEFINITIONS (CONT.)

Device Type	Field	Description
		- Unknown
	SafetyNet Enabled	True if SafetyNet is enabled, false otherwise.
	SafetyNet Exception	SafetyNet exception during error.
	SafetyNet Status	SafetyNet status if enabled and no error.
	SafetyNet Timestamp	Timestamp of when last SafetyNet check was run.
	Samsung Carrier Code	Samsung Carrier code.
	Samsung DualDAR Enabled	Indicates if the Samsung DualDAR on client is enabled. If not client enabled or device is in Device Owner mode, lists as "Unsupported."
	Samsung DualDAR Version	Represents the Samsung Knox v3 license key for DualDAR. Lists the Samsung DualDAR version if client is enabled. If not client enabled or device is in Device Owner mode, lists as "Unsupported."
	Samsung E-FOTA Capable	True if the device supports Samsung E-FOTA, false otherwise.
	Samsung KNOX Version	Knox version, if present.
	Samsung Model Number	Samsung Model Number.
	Samsung SAFE Version	Samsung Safe Version.
	Screenlock PIN Change Prompt – Showing	Indicates if device user was prompted to change the device's screen lock password / PIN and the device user skipped the prompt. Values are: - Unknown - If coming from an older client device, value is unknown. - True - Indicates the PIN is to expire in 7 days or less.

TABLE 4. DEVICE FIELD DEFINITIONS (CONT.)

Device Type	Field	Description
		• False - (default) Indicates the device user is not being prompted to change the password / PIN (it has not reached its 7-day expiration window.) The value listed stays until the device user successfully changes the password /PIN on the device. See "Working with default policies" on page 93.
	Secure Apps Enabled	True if Secured Apps / AppConnect is enabled, otherwise false.
	Secure Apps Encryption Enabled	True if Secured Apps Encryption is enabled, otherwise false.
	Secure Apps Encryption Mode	Type of Secured Apps / AppConnect Encryption.
	Security Detail	Reason for security failure if it occurs.
	Security Patch Level	Security Patch Level string or timestamp.
	Security Patch Level Date	Date of the Security Patch Level of the OS.
	Security Reason	Reason device is considered jailbroken.
	USB Debugging	True if USB debugging is enabled, otherwise false.
	Wear OS Client installed	True only if one or more paired-watches have Mobile@Work installed on the Wear OS device.
	Wear OS Device is Paired	True if one or more Wear OS device is paired to device via Bluetooth.
	Zebra Build Fingerprint	Fingerprint of the firmware build currently present on the Zebra device.
	Zebra Device Build Id	Current Build ID of the Zebra device.
	Zebra Device System Update	• **Unknown** - Not supported by client or OS version

TABLE 4. DEVICE FIELD DEFINITIONS (CONT.)

Device Type	Field	Description
		- **Current** - The most current update is installed. Applicable to Android 8. 0 or supported newer versions. Applicable to Zebra 6 or supported newer versions. - **Pending** - The client has accepted a system update configuration, but the update is not yet downloaded or installed. Applicable for Zebra 6 or supported newer versions. - **Downloading** - An update is being downloaded. Applicable for Zebra 6 or supported newer versions. - **Available** - An update is available (Android 8 or supported newer versions) or downloaded (Zebra 6 or supported newer versions) but is not yet installed.
	Zebra OTA Capable	True if the device supports Zebra OTA (Over The Air), otherwise false.
	Zebra Patch Version	The version of firmware for the Zebra device to be upgraded to. This is the target firmware version of the firmware applied to the Zebra device through firmware policy.
Common Fields	Anti-phishing native status	Content Blocker anti-phishing status for iOS device, and URL Handler anti-phishing for Android devices when MTD Anti-phishing is configured.
	Anti-phishing VPN status	Status of VPN which analyzes malicious URLs when MTD Anti-phishing is configured.
	APNS Capable	Only true if there is an APNS token for the Mobile@Work client, otherwise false.
	AppConnect Terms of Service	True/false for if the AppConnect Terms of Service was accepted.

TABLE 4. DEVICE FIELD DEFINITIONS (CONT.)

Device Type	Field	Description
	AppConnect Terms of Service Date	Represents the date/time the AppConnect Terms of Service was accepted.
	Authenticator Only	True/false if the device is registered in Authenticator Only mode.
	Azure Client Status Code	Indicates whether device is connected to Azure. The possible values are: • Success - Able to retrieve device ID. • Internal_Error - An unrecoverable error occured either within the client or on server side. • Workplace_Join_Required - Registration of device required. Device user can mitigate this status. • Interaction_Required - An interactive log-in is required. Device user can mitigate this status. • Server_Declined_Scopes - Some scopes were not granted access to. • Server_Protection_Policies_Required - The requested resource is protected by an Intune Conditional Access policy. • User_Canceled -The device user cancelled the web Auth session by tapping the "Done" or "Cancel" button in the web browser. • Account_logged_out - Account logged out.
	Azure Device Compliance Report Status	Lists the device's compliance status in Azure. Possible values are: • In-progress • Successful

TABLE 4. DEVICE FIELD DEFINITIONS (CONT.)

Device Type	Field	Description
		- Failed
	Azure Device Compliance Report Time	The time Core reported the device compliance status to Microsoft Intune. A blank field indicates one of the following: - because that feature is disabled - Core just received the data and has yet to call the Microsoft API - there is an error such as user_Cancelled or Internal Error so server will not report the device to Microsoft
	Azure Device Compliance Status	Indicates Azure account has been deactivated or the device is not in compliance. Possible values are: Compliant / Not Compliant.
	Azure Device Identifier	The device ID reported by Microsoft to the iOS or Android device. For example: 007c8232-9489-4074-9b35-345b16f0a72d. This is Microsoft's ID for that device. Core receives this device ID as device users are required to register to Microsoft Authenticator application in order to use this feature. If unable to retrieve the Device ID, this field is left blank.
	Background Status	True if iOS background status is enabled, otherwise false.
	Battery Level	Percentage of battery left.
	Block Reason	A list of reasons why the device is blocked.
	Blocked	True if the device is blocked, otherwise false.
	Cellular Technology	GSM, CDMA, or blank if the device does not support cellular.
	Client Build Date	The build date of the client, if registered with Mobile@Work client.

TABLE 4. DEVICE FIELD DEFINITIONS (CONT.)

Device Type	Field	Description
	Client Id	The unique client ID if the device was registered with Mobile@Work client.
	Client Last Check-in	Date/Time of last check-in.
	Client Migration Status	Status of Mobile@Work client migration from Core to Cloud (true/false).
	Client Name	The name of the client, if registered with Mobile@Work client.
	Client Version	The version of the client, if registered with Mobile@Work client; otherwise, false.
	Cloud Migration Status	Status of device migration from Core to Cloud (true/false).
	Comment	A field that the admin uses to add their own comments for the device.
	Compliant	True if the device is in compliance, otherwise false.
	Creation Date	The creation date of this device record.
	Current Country Code	Current country code of the device.
	Current Country Name	Current country name of the device.
	Current Operator Name	Short name of the cellular carrier, if there is a cellular service.
	Current Phone Number	Current phone number of device, if the device has cellular service.
	Device Admin Enabled	True if device admin (Android) is enabled, otherwise false.
	Device Encrypted	True if the device is encrypted, otherwise false.
	Device is Compromised	True if the device is compromised, for example, jailbroken.
	Device Locale	Locale of the device.

Table 4. Device field definitions (Cont.)

Device Type	Field	Description
	Device Owner	Company or Personal.
	Device Space	Name of the space the device belongs to.
	Device UUID	Unique ID of the device generated from Core.
	Display Size	Size of device's display.
	EAS Last Sync Time	Exchange ActiveSync last sync time.
	Enrollment specific ID	unique ID that identifies the work profile enrollment in a particular organization, and will remain stable across factory resets
	Ethernet MAC	Ethernet MAC ID.
	Home Country Code	Home (Initial) country code of the device.
	Home Country Name	Home country name of the device.
	Home Operator Name	Home Operator Name.
	Home Phone Number	Home Phone Number.
	IMEI	IMEI (International Mobile Equipment Identity) number.
	IMSI	ISMI (International Mobile Subscriber Identity) number.
	IP Address	Current IP address of the device. As new GDPR fields (such as IP Address and eSIM ID) are added throughout Core releases, the administrators who have configured GDPR already will need to edit the GDPR profile if they want to hide the new fields.
	Language	Language of the device.
	Last Check-in	Last check-in time of the device.

TABLE 4. DEVICE FIELD DEFINITIONS (CONT.)

Device Type	Field	Description
	Manufacturer	Manufacturer of the device.
	MDM Last Check-in	Last MDM check-in time of the device.
	MDM Managed	True if the device is MDM managed, otherwise false.
	Memory Capacity	Memory capacity of the device.
	Memory Free	Amount of free memory in the device.
	MobileIron Threat Defense Status	Mobile Threat Defense Status.
	MobileIron Tunnel App Installed	True / false if the Tunnel app was installed.
	Model	Model of the device.
	Model Name	Model name of the device.
	Modified Date	Date/Time for last updates to device details.
	MTD Activation Status	MTD Activation Status.
	MTD Anti-Phishing Status	MTD Anti-Phishing Status.
	Non-compliance Reason	Reason why the device is not in compliance.
	OS Version	OS version number string.
	Passcode	Contains registration PIN for a preregistered device, empty if none exists.
	Passcode Expiration Time	The expiration time for the registration pin for a prereigstered device, empty if none exists.
	Platform	Operating system of the device.
	Platform Name	Operating system and OS version of the device.
	Processor Architecture	Architecture of the processor for the device.

TABLE 4. DEVICE FIELD DEFINITIONS (CONT.)

Device Type	Field	Description
	Quarantined	True if the device is quarantined, false otherwise.
	Quarantined Reason	Reason for quarantined, empty if the device is not quarantined.
	Registration Date	Registration date of the device.
	Registration IMSI	Registration of ISMI (international mobile subscriber identity) number.
	Registration UUID	Unique ID when registering from the client.
	Retired	True if the device is retired, otherwise false.
	Roaming	True if the device is roaming, otherwise false.
	SD Card Encrypted	True/faise if SD card is encrypted.
	Security State	Security state of the device.
	Serial Number	Serial number of the device.
	Status	Status of the device.
	Storage Capacity	Total storage capacity, in bytes, of the device.
	Storage Free	Number of bytes of free storage on the device.
	Terms of Service Accepted	True if the End user Terms of Service was accepted, otherwise false.
	Terms of Service Accepted Date	Date for when the End User Terms of Service was accepted, otherwise blank.
	Wi-Fi MAC	Wi-FI MAC address of the device.
iOS Fields	Activation Lock Bypass Code	Code to bypass activation lock.
	Activation Lock is Enabled	True if Activation Lock is enabled on the device, otherwise false. Applicable to iOS.
	APNS Token	Mobile@Work client APNS wakeup token. Applicable to iOS.

TABLE 4. DEVICE FIELD DEFINITIONS (CONT.)

Device Type	Field	Description
	Apple Device Mac Address	iPhone (media access control address) MAC address. Applicable to iOS and OS X.
	Apple Device Version	iPhone version code. Applicable to iOS and OS X.
	Apple OS Update Product Key	Available OS update product key. Applicable to iOS and macOS.
	Apple OS Update Product Version	Available OS update product version. Applicable to iOS and macOS.
	Apple OS Update Status	OS update status. Applicable to iOS and macOS.
	Apple User Enrolled Device	True/false the device is enrolled in User Enrollment.
	Bluetooth MAC	Bluetooth MAC address. Applicable to and OS X.
	Build Version	MDM build version. Applicable to iOS and OS X.
	Carrier Settings Version	Carrier settings version. Applicable to iOS.
	Current Mobile Country Code	Current mobile country code. Applicable to iOS.
	Current Mobile Network Code	Current mobile network code. Applicable to iOS.
	Data Protection	Applicable to iOS.
	Data Roaming Enabled	True if device is data roaming enabled, otherwise false. Applicable to iOS.
	DEP Device	True if the device is Apple Device Enrolled, otherwise false. Applicable to iOS, macOS, and tvOS.
	DEP Enrolled	True if the device is Apple Device Enrolled, otherwise false. Applicable to iOS.
	Device Locator Service is Enabled	True if device locator service is enabled, otherwise false. Applicable to iOS.

TABLE 4. DEVICE FIELD DEFINITIONS (CONT.)

Device Type	Field	Description
	Device Name	Name of the device. Applicable to iOS and OS X.
	Do Not Disturb is in Effect	True if Do Not Disturb is enabled, otherwise false. Applicable to iOS.
	Force Encrypted Backup	True if backups are forced to be encrypted, otherwise false. Applicable to iOS.
	Full Disk Encryption Enabled	True if full disk encryption is enabled, otherwise false. Applicable to macOS 10.9+.
	Full Disk Encryption Has Institutional Recovery Key	True if full disk encryption has institutional recovery key, otherwise false. Applicable to macOS 10.9+.
	Full Disk Encryption Has Personal Recovery Key	True if full disk encryption has personal recovery key, otherwise false. Applicable to macOS 10.9+.
	Hardware Encryption Caps	Hardware encryption capabilities. Applicable to iOS.
	iCloud Backup is Enabled	True if Cloud backup is enabled, otherwise false. Applicable to iOS.
	iOS Background Status	True if iOS background status is enabled, otherwise false. Applicable to iOS.
	iOS ICCID	Device's integrated circuit card identifier number. Applicable to iOS.
	IT Policy Result	Applicable to iOS.
	iTunes Store Account Hash	iTunes Store Account Hash.
	iTunes Store Account is Active	Ttrue if iTunes Store Account is active, otherwise false. Applicable to iOS.
	Languages	Language of the device. Applicable to tvOS.
	Last Acknowledged Lock PIN	PIN to unlock a locked macOS device. Applicable to macOS.

TABLE 4. DEVICE FIELD DEFINITIONS (CONT.)

Device Type	Field	Description
	Last Acknowledged Wipe PIN	PIN to proceed after wiping a macOS device. Applicable to macOS.
	Last iCloud Backup Date	Last iCloud backup date. Applicable to iOS.
	Last MTD Sync Time	Last MTD check-in time. Applicable to iOS.
	Locales	Locale of the device. Applicable to tvOS.
	macOS User ID	macOS user ID. Applicable to OS X.
	macOS User Long Name	macOS user's long name. Applicable to OS X.
	macOS User Short Name	macOS user's short name.Applicable to OS X.
	Managed Apple ID	The Apple ID allocated by the company to the device user. For Shared iPad devices, this field is populated once the iPad user logs in.
	Maximum Resident Users	Only for use with iOS Education Shared iPad devices. Tells the device how many users will have their data cache on the device. When the device reaches this number, the next logged-in user that is not already present will be cached and one of the cached users will be removed from the cache (up to Apple which user.) Applicable to iOS.
	MDM Lost Mode Enabled	True if MDM Lost Mode is enabled, otherwise false. Applicable to iOS.
	MDM Service Enrolled	True if the device is was enrolled via MDM Service (non-over air Apple Device Enrollment), otherwise false. Applicable to iOS.
	MEID	Mobile Equipment Identity Number.
	Modem Firmware Version	Modem firmware version. Applicable to iOS.
	Network Tethered	True if the device was reported as currently network tethered, otherwise false. Applicable to macOS.

TABLE 4. DEVICE FIELD DEFINITIONS (CONT.)

Device Type	Field	Description
	Organization Info	Organization for the device. Applicable to iOS.
	Passcode Compliant	True if passcode is in compliance, otherwise false. Applicable to iOS.
	Passcode Compliant with Profiles	True if passcode is compliant with rules specified from profiles. Applicable to iOS.
	Passcode Present	True if Passcode is present on device, otherwise false. Applicable to iOS.
	Personal Hotspot Enabled	True if Personal Hotspot is enabled, otherwise false. Applicable to iOS.
	Product Code	iPhone Product code. Applicable to iOS and OS X.
	Product Name	Product name. Applicable to iOS and OS X.
	Security Reason Code	Security reason code. Applicable to iOS.
	Shared iPad: Active Resident Users	Lists the number of users who have logged into the device and have user sessions stored on the device. The number displayed will never be larger than the Shared iPad: Allocated Resident Users number, even if a Guest/Temporary user logged into that device.
	Shared iPad: Allocated Resident Users	Lists the number of user sessions that can be stored on the device. If more users log in, older users will be removed to make room for the new user. This is configured in the Device enrollment profile and will either be the number set as the Maximum Resident Users or will be calculated if the Quota size is set.
	Shared iPad: Guest/Temporary Session Only	If the device was configured to only allow Guest/Temporary sessions and is true, only guest access is allowed. This is configured in the Device Enrollment Profile. If left blank, the timeout will use the iPad's system defaults. If set to zero, there will be no timeout. Maximum limit is 1800 seconds.

TABLE 4. DEVICE FIELD DEFINITIONS (CONT.)

Device Type	Field	Description
	Shared iPad: Guest/Temporary Session Timeout	Lists the timeout for guest/temporary sessions. This will log out the user after inactivity for the allotted time. Guest/temporary users will be completely logged out, not just have the screen locked. This is configured in the Device Enrollment Profile. If set to zero, there will be no timeout.
	Shared iPad: Is Multi User	True/false if the device is a shared iPad.
	Shared iPad: Maximum Resident Users	Lists the Maximum Resident Users allowed to be set on the device. If the Device Enrollment Profile sets the Maximum Resident Users to a number larger than this, the Allocated Resident Users will be set to this number. This number is controlled by the system based on the size of the device.
	Shared iPad: Quota Size (MB)	Lists the amount of space allocated per user. This is configured in the Device Enrollment Profile and will either be the number set as the Quota size or will be calculated if Maximum Resident Users is set.
	Shared iPad: User Session Timeout	Lists the timeout for logged-in user sessions. This will log out the user after inactivity for the allotted time. Users will be completely logged out, not just have the screen locked. This is configured in the Device Enrollment Profile. Maximum limit is 1800 seconds.
	SIM EID 1, 2, 3	The SIM ID of the carrier assigned to the SIM of a specific device. The EID will be included in the response of the `simdetails` API call. (For more information, see the *V2 API Guide*.) In the Device Details page, clicking on the number in the field opens the SIM Information dialog box allowing the administrator to see SIM information, including the EID. Applicable to iOS 14.0 through the latest version of Core.
	SIM Label 1, 2, 3	The label for the associated SIM card. Up to 3 SIM cards, physical and virtual, are stored.
	SIM MCC 1, 2, 3	SIM card mobile country code associated to the phone number.

TABLE 4. DEVICE FIELD DEFINITIONS (CONT.)

Device Type	Field	Description
	SIM MNC 1, 2, 3	SIM card mobile network code associated to the phone number
	SIM Phone Number 1, 2, 3	The phone number associated with the SIM card / eSIM.
	SIMs	• Lists the number of SIMs associated to the device. This includes embedded SIMs (eSIM) and physical SIMs. • There can be multiple SIMs associated with the eSIM. • For eSIMs in iPhone XS, iPhone XS Max, or iPhone XR with iOS 12.1 or supported newer versions.
	Subscriber Carrier Network	SIM card subscriber carrier network. Applicable to iOS.
	Subscriber MCC	SIM card mobile country code. Applicable to iOS.
	Subscriber MNC	SIM card mobile network code Applicable to iOS.
	Supervised	True if the device is MDM supervised, otherwise false. Applicable to iOS.
	Time Zone	Lists the time zone applied to the device.
	UDID	iPhone unique device identifier. Applicable to iOS and OS X.
	Voice Roaming Enabled	True if voice roaming is enabled, otherwise false. Applicable to iOS.
	VPN IP Address	VPN IP address. Applicable to iOS and tvOS.
	Wakeup Status	Device Wakeup status.
User Fields	Display Name	The display name of the device user.
	Email Address	Device user's email address.
	First Name	Device user's first name.

TABLE 4. DEVICE FIELD DEFINITIONS (CONT.)

Device Type	Field	Description
	Last Admin Portal Login Time	Date of admin's last log in into Core.
	Last Name	Device user's last name.
	LDAP > Attribute Distinguished Name	The Attribute Distinguished Name for an LDAP user.
	LDAP > Groups > LDAP Group Distinguished Name	LDAP Users who are members of an LDAP group with a specific group distinguished name.
	LDAP > Groups > Name	LDAP Users who are members of an LDAP group with a specific group name.
	LDAP > LDAP User Distinguished Name	The LDAP distinguished Name of the user.
	LDAP > LDAP User Locale	An LDAP User who are members of a specific locale.
	LDAP > Organizational Units > LDAP Organizational Units Distinguished Name	LDAP users who are members of an organizational unit with a specific distinguished name.
	LDAP > Principal	Value of the attribute specified as the User ID in the LDAP server configuration.
	LDAP > upn	Value of the attribute specified as the User Principal Name in the LDAP server configuration.
	LDAP > User Account Control > Account Disabled	Indicates whether the LDAP user account is disabled (true/false).
	LDAP > User Account Control > Locked Out	Indicates whether the LDAP user account is locked out (true/false).
	LDAP > User Account Control > Password Expired	Indicates whether the LDAP user 's password has expired (true/false).

TABLE 4. DEVICE FIELD DEFINITIONS (CONT.)

Device Type	Field	Description
	LDAP > User Attributes > custom1, custom2, custom3, custom4	The value of the LDAP user attribute is defined in **Services > LDAP**.
	LDAP > User Attributes > memberOf	The value of the LDAP user attribute is defined in **Services > LDAP**.
	SAM Account Name	The security account name. This was the login name for earlier versions of Windows.
	User ID	The LDAP user ID.
	User UUID	The LDAP Universally Unique Identifier.

For **Windows** field definitions, see https://docs.microsoft.com/en-us/windows/client-management/mdm/healthattestation-csp.

Using the query builder

To use the query builder:

1. Select a field on which to search. **Hint**: you can type a few letters of the field name to see a short list of matching fields, or press **Expand All** within the field list to see all the fields.

   For example, if you select **Status**, the search engine provides only values available for **Status**.

2. Select an operator, such as **Equals**.
3. Click in the **Value** field to enter a value you want to search.
4. Some fields have predetermined values that you can select.
5. Select additional fields and criteria as needed.
6. Click **All** to combine the criteria with a logical AND or click **Any** to combine the criteria with OR.
7. Click **Search** to display the matching devices and their owners.

To include retired devices in the results, uncheck the check box to the left of the **Search** button.

Using a manually edited search expression

To enter a search expression directly into the expression field:

1. Type or paste the search criteria into the expression field. The automatic syntax check displays a status icon next to the expression field. A green icon indicates that the syntax is correct, and a red icon if incorrect.

2. When the syntax is correct, click **Search** to display the matching devices and their owners.

Using both the query builder and manual editing

Use the query builder to start an expression, look up field syntax, and select predetermined values. Then, edit the expression directly as needed.

1. Select fields and criteria.

2. Click **All** to combine multiple criteria with a logical AND or **Any** to combine multiple criteria with OR. You can manually edit individual logical operators in the expression field.

3. In the expression field, edit the expression directly.

4. For example, you can add parentheses, change logical operators, or manually edit field names or values.

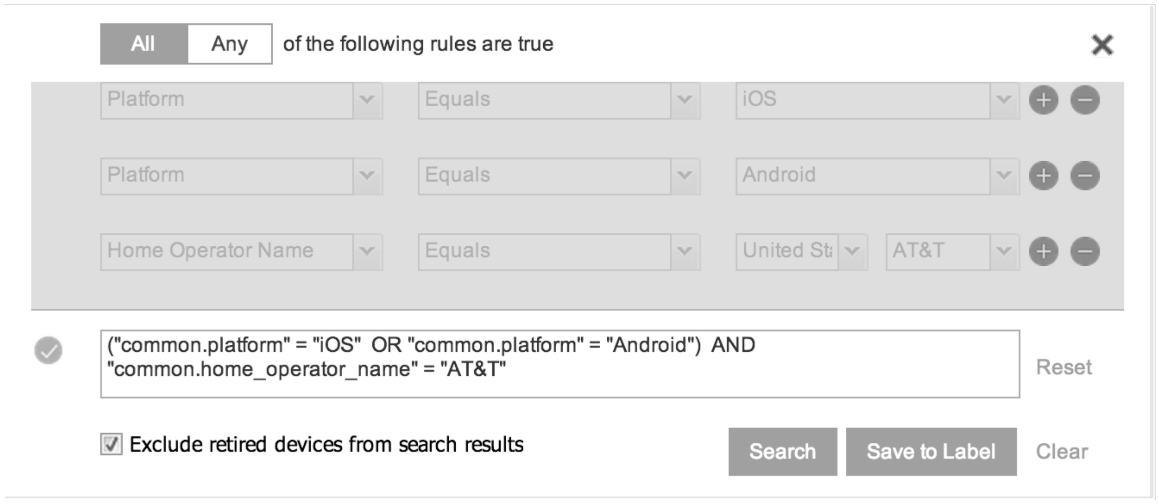
5. The automatic syntax check displays a status icon next to the expression field. A green icon indicates that the syntax is correct, and a red icon if incorrect.

6. When the syntax is correct, click **Search** to display the matching devices and their owners.

Once you manually edit the expression, the query builder is covered with a gray box to indicate it no longer represents the current state of the expression. Click the **Reset** link to remove your manual edits and continue using the query builder.

Example: Find all iOS or Android devices that use AT&T as their service operator.

FIGURE 1. SERVICE OPERATOR IN QUERY BUILDER



Platform | Equals | iOS

Platform | Equals | Android

Home Operator Name | Equals | United St | AT&T

("common.platform" = "iOS" OR "common.platform" = "Android") AND "common.home_operator_name" = "AT&T"

☑ Exclude retired devices from search results

Build the expression to match the above example.

1. Click **Advanced Search** to open the query builder.
2. Select **Platform** in the first field, select **Equals** for the operator, then select **iOS** as the platform.
3. Click the plus icon to add another row for criteria.
4. Select **Platform**, **Equals**, and **Android** as the field, operator, and platform value, respectively.
5. Click the plus icon to add a third row for criteria.
6. Select **Home Operator Name** for the field and **Equals** for the operator.

   Notice that the value field adjusts automatically to display service operator values by country.
7. Accept the first value field and select **AT&T** in the second value field.

Manually edit the expression.

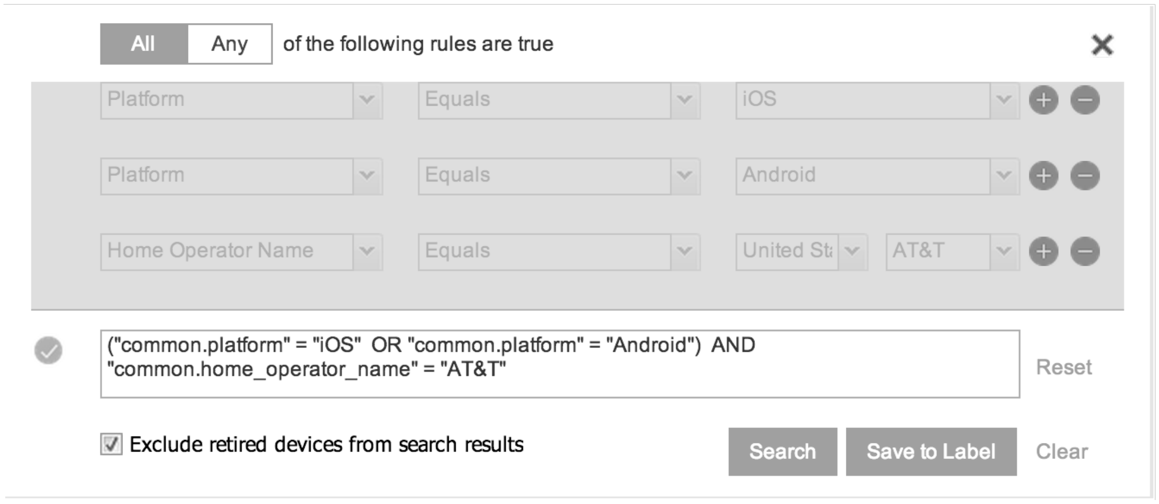
1. Replace the first **AND** with **OR**.

   The syntax is checked automatically as you type. Note a red icon indicating incorrect syntax while you edit the expression.

2. Add parentheses around the phrase to read:

```
("common.platform" = "iOS" OR "common.platform" = "Android") AND
“common.home_operator_name” = “ATT&T”
```

Note a green icon indicating correct syntax has replaced the red icon. Your advanced search will look the same as the original image (see below).



All of the following rules are true

Platform Equals iOS

Platform Equals Android

Home Operator Name Equals United St AT&T

("common.platform" = "iOS" OR "common.platform" = "Android") AND "common.home_operator_name" = "AT&T"

☑ Exclude retired devices from search results

To revert to the original expression without your manual edits, click the **Reset** link to the right of the expression.

3. Click **Search** to display the matching devices and their owners.

Negative operators with advanced search

Using negative operators enables you to create filters that exclude devices instead of including them. For example, you can search for:

- Devices that use any platform other than iOS
- Devices with a current country code other than US

TABLE 5. NEGATIVE OPERATORS WITH ADVANCED SEARCH

Operator	Action	Example
Does not equal	Returns a list of devices that do not match the criteria specified in the value field for the selected field.	Select: • **Home Country Name** as the field • **Does not equal** in **Operator** • **United States** in **Country Name** The search returns a list of devices that do not have United States as their home country name.
Does not contain	Returns a list of devices that do not contain the string specified in the selected field. • Used only with strings. • Available only in the expression field.	Select or enter: • Go to **Common Fields** and select **Device Space**. • In the expression field, enter: does not contain • Place the cursor between the two quote marks in the expression field and enter: **Global** The search returns a list of devices that are not assigned to the **Global** space.

Examples for advanced search with negative operators

To display a list of devices that have countries other than the United States as the assigned home country, create an advanced search expression that provides the necessary information.

1. Go to **Device & Users > Devices.**
2. Click the large magnifying glass icon located at the top right to initiate an advanced search.
3. In **Field**, select **Common Fields**.
4. Select **Home Country Name**.

5. Select **Does not equal** from the list in **Operator**.
6. Select **United States** from the list of countries in **Country Name**.
7. Click **Search**.
8. **Optional:** To save the search to a label, click **Save to Label** and then provide an existing label name or a new label name and description.
9. If Notes for Audit Logs is enabled, a text dialog box opens. Enter the reason for the change and then click **Confirm**. For more information, see "Best practices: label management" on page 402.

Suppose you want to list users within an LDAP group that have a Home Country Code other than the United States (US).

To create the advanced search expression that provides the needed list:

1. Go to **Device & Users** > **Devices**
2. Click the large magnifying glass icon located at the top right to initiate an advanced search.
3. In the expression field enter the following, including quote marks:

   “user.ldap.groups.name” = “Corp_Users” AND “common.home_country_code” != “US”
4. Click **Search**.
5. **Optional:** To save the search to a label, click **Save to Label** and then provide a new label name and description.
6. If Notes for Audit Logs is enabled, a text dialog box opens. Enter the reason for the change and then click **Confirm**. For more information, see "Best practices: label management" on page 402.

Clearing an advanced search

- In the advanced search, click the **Clear** link, or
- Apply a different search by entering a basic search.

Closing the advanced search query builder does not clear the search.

Searching for retired devices

By default, retired devices are excluded from search results. To include them, uncheck the Exclude Retired Devices From Search Results check box, located to the left of the Search button in advanced search.

Procedure

1. Uncheck the check box to exclude retired devices
2. Select the following in the advanced search query builder:
   - Field: **Retired**
   - Operator: **Equals**
   - Value: **true**
3. Click **Search**.

The matching records are displayed.

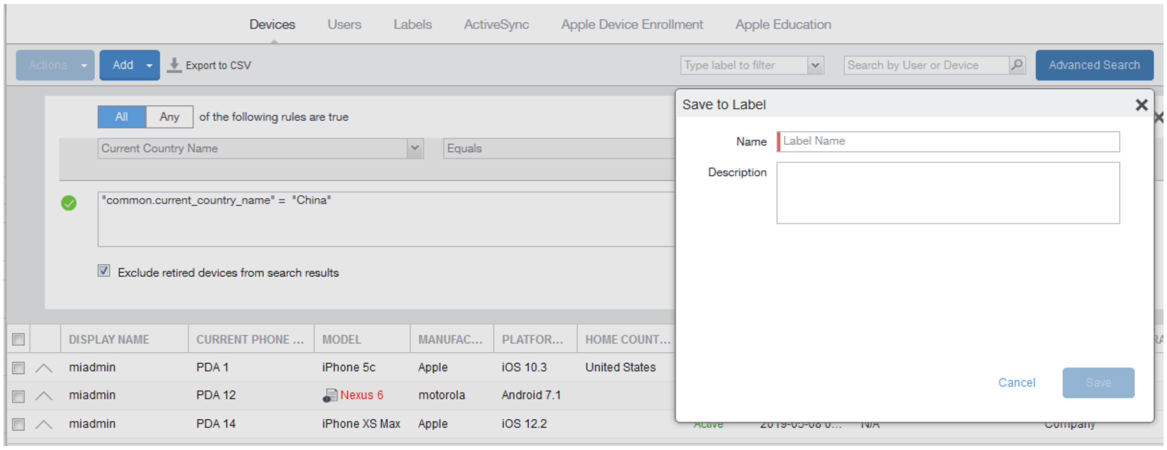
Searching for blocked devices

You can search for devices for which the status field value is **Blocked**, which means that the device is blocked from accessing the ActiveSync server. However, the **Status** column does not show the value **Blocked**. Instead, the ActiveSync Association view shows this information. See “Viewing ActiveSync associations” in the *Sentry Guide for Core.*

Saving a search criterion to a label

Once you create a search criterion, you can save it to a label. Click the **Save To Label** button in advanced search to create a new label using the search criterion. Type a new label name in the **Label** field and type a description. The new filter label is created with the advanced search criterion applied.

FIGURE 1. SAVING A SEARCH CRITERION TO A LABEL



All | Any of the following rules are true

Current Country Name | Equals

"common.current_country_name" = "China"

☑ Exclude retired devices from search results

Name: Label Name

Description:

□		DISPLAY NAME	CURRENT PHONE ...	MODEL	MANUFAC...	PLATFOR...	HOME COUNT...
□	︿	miadmin	PDA 1	iPhone 5c	Apple	iOS 10.3	United States
□	︿	miadmin	PDA 12	Nexus 6	motorola	Android 7.1	
□	︿	miadmin	PDA 14	iPhone XS Max	Apple	iOS 12.2	

If Notes for Audit Logs is enabled, a text dialog box opens. Enter the reason for the change and then click **Confirm**. For more information, see "Best practices: label management" on page 402.

Securing Devices

Securing devices is at the heart of Core. The topics in this chapter include the following advanced topics:

- "Registration-related features and tasks" on the next page
- "Reprovisioning a device" on the next page
- "Retiring a device" on page 65
- Deletion of retired devices
- "Security-related features and tasks" on page 72
- "Lock" on page 74
- "Unlock" on page 74
- "Encryption" on page 74
- "Wipe" on page 75
- "Cancel Wipe" on page 76
- "Selective Wipe" on page 76
- "Block AppTunnels" on page 77

- "Lost" on page 77
- "Found" on page 77
- "Locate" on page 77
- "Reset device PIN" on page 77
- "Force Device Check-In" on page 78
- "Setting up background check-ins with APNs" on page 78
- "Managed iBooks" on page 78
- "Personal hotspot on/off switch" on page 78
- "Custom SyncML" on page 78
- "Reporting on managed devices" on page 80
- "Setting the time zone of a device" on page 83

Refer to the *Getting Started with Core* for the most commonly used topics for managing devices, such as:

- Displaying device assets
- Restricting the number of devices a user registers

Registration-related features and tasks

The following table summarizes features and tasks related to registration.

TABLE 6. REGISTRATION-RELATED TASKS

Feature	Description	Use Case
Reprovisioning a device	This feature is not supported on Windows devices.	
Retire	Ends the registration (and Core management) for a device	Moving devices out of inventory

Reprovisioning a device

This feature is not supported on Windows devices.

Retiring a device

Retiring a device archives the data for that device and removes the configurations and settings applied by Core (no personal information or settings on the device are impacted). The entry for the device no longer appears in the **Device & Users** page (unless you specifically search for retired devices), and the user is notified that the software has been removed.

If the retired device is also in the ActiveSync Association view, it remains there. However, because the device is retired, it can no longer access the ActiveSync server. You can manually remove the device from the ActiveSync Association page. See “Removing ActiveSync phones” in the *Sentry Guide for Core*.

If you have duplicate devices, see "Managing Duplicate Devices" on page 71.

Procedure

1. Go to **Device & Users** > **Devices**.
2. Select the check box for the device.
3. Click **Actions > Retire**.

   The **Retire** dialog appears.
4. In the **Retire** dialog, confirm the user and device information and enter a note.
5. Click **Retire**.

   The user receives notification of the action.

   To see a list of retired devices, see “Searching for retired devices” in the *Getting Started with Core.*

For Windows devices, applying the Retire action to a device removes all Wi-Fi profiles. However, if the device is connected to a Wi-Fi profile pushed from Core, that Wi-Fi profile is not removed immediately, but after the user disconnects from that Wi-Fi.

Retiring and deleting unused and retired devices

As device users leave your enterprise or change to new devices, more and more devices in the Core database are retired or never activated. When you retire a device, Core de-registers it and no longer manages or secures the device. All the configurations and settings that Core had applied to the device are removed. The device can no longer access enterprise data or apps.

However, Core retains retired and unregistered devices in its database. Deleting these devices from the database improves Core performance and frees up disk space. Although Core also provides a web services API and a CLI command to delete these devices, using the Admin Portal display is easier. It also provides an easy way to automatically delete or retire devices on a regular schedule.

With this Admin Portal display, you can:

- Easily navigate to lists of unregistered and retired devices.
- Retire or delete devices that have been retired or not checked in for more than a specified number of days.
- Configure Core to automatically retire or delete devices daily, weekly, or monthly.

You can use this display only if you are assigned to the global space **and** you are assigned the admin role Delete retired device. Otherwise, the actions on this display are disabled.

When Core retires or deletes retired devices due to your actions on this display, it records Delete Retired Device events in the audit log. Personal data related to retired devices can be deleted by deleting the local user. However, LDAP users cannot be permanently deleted unless the LDAP server or group has been deleted, in which case the LDAP users become local users and can be deleted. If a user is deleted on the LDAP server, the user is automatically removed from Core during the next LDAP sync.

Assigning an administrator the role to delete retired devices

If you are a super administrator, you can assign another administrator the capability to delete retired devices. You are a super administrator if you are:

- Assigned to the global space.
- Assigned the role **Manage administrators and device spaces**.

Procedure

1. In the Admin Portal, go to **Admin > Admins**.
2. Select an administrator.
3. Select **Actions > Edit roles**.
4. For **Admin Space**, select **Global**.

5. Select the **Device Management** role **Delete retired device**.

6. Click **Save**.

Creating a schedule to retire or delete devices

You can enable a regular schedule to retire unused devices and delete retired devices. The schedule tool works identically for each task.

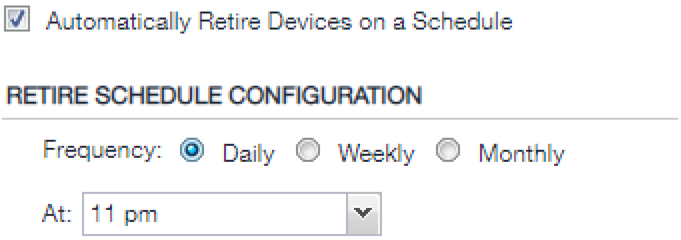
Procedure

1. In the Admin portal, navigate to Settings > System Settings > Users & Devices > Retire and Delete Retired Devices.

2. Click **Automatically Delete Retired Devices on a Schedule**, or **Automatically Retire Devices on a Schedule**. The Schedule Configuration opens.

3. **Frequency**: Select **Daily**, **Weekly**, or **Monthly**.

   a. **Daily**: Select the run time from the **At**: drop-down menu. The default is midnight.



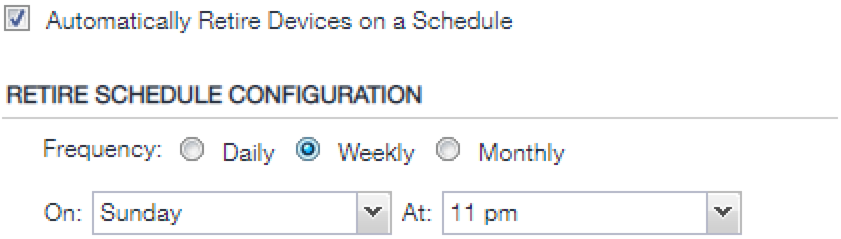
☑ Automatically Retire Devices on a Schedule

RETIRE SCHEDULE CONFIGURATION

Frequency: ● Daily ○ Weekly ○ Monthly

At: 11 pm

   b. **Weekly**: Select the day and time for the clean up. Default value is Sunday at midnight.



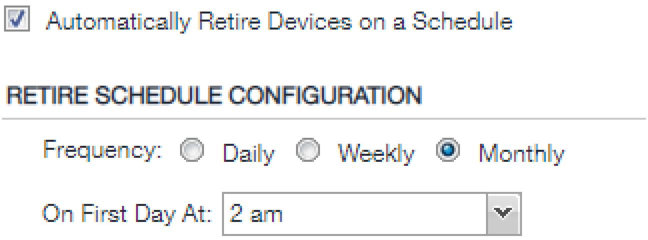
☑ Automatically Retire Devices on a Schedule

RETIRE SCHEDULE CONFIGURATION

Frequency: ○ Daily ● Weekly ○ Monthly

On: Sunday At: 11 pm

   c. **Monthly**: Select the time for a first-day-of-the-month schedule frequency. Default is first day of the month at midnight.



☑ Automatically Retire Devices on a Schedule

RETIRE SCHEDULE CONFIGURATION

Frequency: ○ Daily ○ Weekly ● Monthly

On First Day At: 2 am

4. Click **Save**.

Retiring or deleting retired devices by threshold

A common task, although not necessarily a daily task, is retiring unused or deleting retired devices. You can retire devices that have not checked in or delete retired devices by a threshold amount of time. Deleting these devices from the database improves Core performance and frees up disk space.

Prerequisites

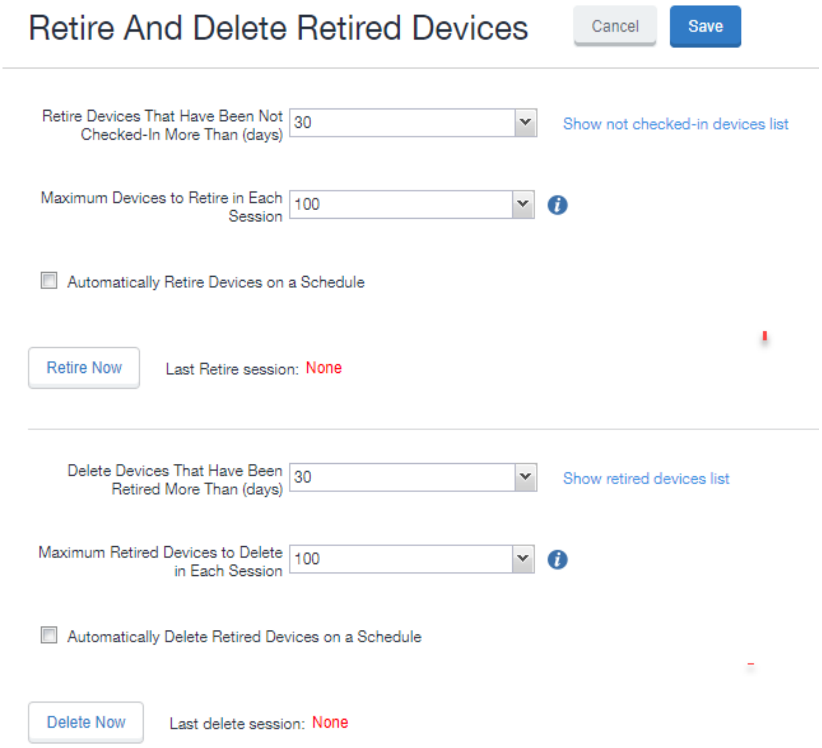
Make sure you are assigned the required admin role. To delete or retire devices, you must be:

- Assigned to the global space
- Assigned the admin role **Delete retired device**

Procedure

1. From the Admin Portal, go to **Settings > System Settings**.
2. Select **Users & Devices > Retire and Delete Retired Devices**. The Retire and Delete Retired Devices configuration page opens.

   The settings to retire unused devices (top half of the page) are identical to the settings to delete retired devices (bottom half of page). The following steps are correct for either task, and all are optional steps, except saving the configuration.



Retire And Delete Retired Devices

Retire Devices That Have Been Not Checked-In More Than (days): 30

Maximum Devices to Retire in Each Session: 100

□ Automatically Retire Devices on a Schedule

Last Retire session: None

Delete Devices That Have Been Retired More Than (days): 30

Maximum Retired Devices to Delete in Each Session: 100

□ Automatically Delete Retired Devices on a Schedule

Last delete session: None

3. Specify the number of days after which devices should be retired/deleted, or accept the default of **30 days**.

4. Specify the maximum number of devices to retire/delete in each session, or accept the default of **100 devices**.

5. To set up a regular schedule for retiring/deleting devices, click **Automatically Retire Devices on a Schedule** or **Automatically Delete Retired Devices on a Schedule** to configure the schedule. See "Creating a schedule to retire or delete devices" on page 67.

6. Click **Retire Now** or **Delete Now** to retire or delete the devices that meet the new criteria.

7. Click **Save** to save the configuration.

If the **Retire Now/Delete Now** button is disabled, only an administrator who is a “super administrator” can assign you to the global space and assign the Delete retired device admin role to you. The procedure for the super administrator and definition of a super administrator are in "Assigning an administrator the role to delete retired devices" on page 66.

Managing Duplicate Devices

This section is applicable to iOS and Windows 8 devices.

Before Core version 10.6, duplicate devices with an "active" state were retired. From Core version 10.6 or supported newer versions, administrators can set duplicate active devices to the “Unknown” status by selecting Enable managing duplicate devices.

Removal of device records from the Core database applies to the following retired device types:

- Active Devices with no device details (iOS and Windows 8 devices)
- Devices with no subject holder (iOS and Windows 8 devices)
- Devices with the below statuses (iOS Only)
  - Enrollment Verified
  - Enrolling
  - Enrolled

Core also supports Daily, Weekly and Monthly options for scheduling this feature.

Procedure

1. In the Admin portal, go to **Settings** > **System Settings**.
2. Expand **Users & Devices** and then click **Manage Duplicate Devices**.

   The Manage Duplicate Devices page displays.
3. Select **Enable managing duplicate devices**.

   The page expands to display more options.

   > To disable this feature, simply deselect this field.
4. Make your settings using the guidelines below.
5. Click **Save**.

TABLE 7. MANAGING DUPLICATE DEVICES SETTINGS

Item	Description
Scan Schedule Frequency	Select the appropriate radio button and make the setting: • **Daily** - Select the time of the scan of the duplicate device. This is the time on the Core server. • **Weekly** - Select the day and time of the of the duplicate device. This is the time on the Core server. • **Monthly** - Select the time of the scan of the duplicate device to occur on the first day of the month. This is the time on the Core server.
Device Action	Select one option: • Retire the old device - (default) • Mark the old device as "Unknown"

Related topics

"Retiring a device" on page 65

Security-related features and tasks

The following table summarizes the features and tasks related to security.

TABLE 8. SECURITY-RELATED FEATURES AND TASKS

Feature	Description	Use Case
Lock	Forces the user to enter a password before accessing the device	Dealing with lost and stolen devices
Unlock	This feature is not supported on Windows devices.	Accessing the device when the passcode has been forgotten or reassigning the device to a different user

TABLE 8. SECURITY-RELATED FEATURES AND TASKS (CONT.)

Feature	Description	Use Case
		ⓘ For security reasons, it is inadvisable to execute this command on lost or stolen devices.
Unlock AppConnect Container	This feature is not supported for Windows devices.	This feature is not supported for Windows devices.
Device Encryption Status	Displays the encryption status of the device in the Device Details tab.	Dealing with lost and stolen devices.
Wipe	Removes content and settings to return the device to factory default settings.	Dealing with lost and stolen devices Preparing a device for a different user
Cancel Wipe	This feature is not supported for Windows devices. Attempts to cancel a wipe action for devices.	This feature is not supported for Windows devices. Reversing an inadvertent Wipe command. ⓘ Wipe cannot be reversed after it completes.
Block AppTunnels	This feature is not supported on Windows devices.	
Lost	This feature is not supported on Windows devices.	
Found	This feature is not supported on Windows devices.	
Locate	This feature is not supported on Windows 8.1 Phone devices.	
Reset PIN	ⓘ This feature is supported on Windows devices. Resets the device PIN.	If a user forgets the device PIN, or you locked the device

Lock

Locking a device forces the user to enter a password to access the device and prevents the user from reversing this restriction. The user is informed of this action via email. If the user has set a password for the device, then that password must be entered.

Procedure

1. Go to **Device & Users** > **Devices**.
2. Select the check box for the device.
3. Select **Lock** from the **Actions** menu.

If the Apps@Work app on the selected device is currently connected, then this action will be applied immediately. If the Apps@Work app is not currently connected, then Core Core attempts to complete the operation by means of the operator's SMTP service. If SMTP is used, it may take more time to execute the operation, and the time required may vary by operator.

Unlock

Unlocking the device passcode is supported as follows:

Procedure

1. Go to **Device & Users** > **Devices**.
2. Select the check box for the device.
3. Click **Actions > Unlock**.

Encryption

The encryption status for a device is now reported on the device details tab.

To check the encryption status of a device:

1. Log into the Admin Portal.
2. Go to **Device & Users** > **Devices > Device Detail.**

   The device encryption status displays as Activating, Active, Active Per User, Active Default Key, Inactive, Unsupported, or None.

Wipe

When wiping a device, Core informs the user of this action via email.

Starting with version 11.1.0.0, administrators can wipe the device in Direct Boot mode in all Android Enterprise modes.

WARNING: Wiping a device returns it to factory defaults, which can result in loss of data.

Required Role: The Device Management: Wipe device role is required to use this feature.

Procedure

1. Go to **Device & Users** > **Devices**.
2. Select the check box for the device to be wiped.
3. Click **Actions > Wipe**.
4. Optionally, select one or more of the following options:
   - **Preserve data plan (iOS 11 and later devices only)** - Select this option to retain the data plan on devices running iOS 11, if one exists.
   - **Skip Proximity Setup (iOS 11.3 and later devices only)** - Select this option to skip the proximity setup pane in the iOS Setup Assistant.
   - **Send Notification of wipe to registered user -** Select (default) to allow an email / notification to be automatically generated when a Wipe command is sent. The Send Notification of wipe to registered user field is useful for users that have multiple devices. An email / notification will be automatically generated when the Wipe command is sent and prevents confusion to device users who may think Core is wiping their current, active device De-select the check box to suppress notification when the Wipe command is used.

     To customize the email notification, go to **System Settings > Settings > Templates > Other**. Select the template type **Action on Device**.
5. Click **Wipe**.

Related topics

- "Cancel Wipe" on the next page

Cancel Wipe

Cancel Wipe attempts to cancel a wipe command for one or more devices. The ability to cancel a device wipe action helps you avoid mistakes that can be difficult and costly to fix.

A device wipe action does not take effect until the device checks in with Core. Using **Cancel Wipe**, you may be able to stop the wipe action.

A successful **Cancel Wipe** action sets the device state to **Active**.

1. In the Admin Portal, go to **Device & Users > Devices**.
2. Check the status of the devices for which you need to cancel the device wipe.
3. Select the devices you do not want to wipe that have status **Wipe pending** or **Wiped**.
4. Click **Actions > Cancel Wipe**.
5. In the Cancel Wipe dialog box, select the **Send Notification of wipe to registered user** check box. The Send Notification of wipe to registered user field is useful for users that have multiple devices. An email / notification will be automatically generated when the Cancel Wipe command is sent and prevents confusion to device users who may think Core is wiping their current, active device. De-select the check box to suppress notification when the Cancel Wipe command is used.

   To customize the email notification, go to **System Settings > Settings > Templates > Other**. Select the template type **Action on Device**.

6. Click **Cancel Wipe**.

   The Cancel Wipe action sets the device state to **Active**.

Related topics

"Wipe" on the previous page

Selective Wipe

The Selective Wipe command is no longer supported, however, the functionality is available using the following methods:

- Selective wipe of email for Windows devices is accomplished through security compliance actions, removing the device from the associated label, or retiring the device.

Block AppTunnels

This feature is not supported on Windows devices.

Lost

This feature is not supported on Windows devices.

Found

This feature is not supported on Windows devices.

Locate

This feature is not supported on Windows devices.

Reset device PIN

If a user forgets the device PIN for a Windows Phone 8.1 managed by Core, or if you locked the device, you can reset the device PIN from the Admin Portal.

To reset the device PIN:

1. In the Admin Portal, go to **Device & Users** > **Devices**.
2. Select the Windows Phone device.
3. Click on **Actions** > **Windows Phone Only** > **Reset PIN**.
4. In the **Reset PIN** pop-up, click **Reset PIN**.

   A new PIN is displayed.

   The device user can unlock the device using the new PIN.

The new PIN is generated by the device and communicated to Core.

Since the new PIN may contain complex characters, we recommend that the user reset the PIN.

Force Device Check-In

You can use the **Force Device Check-in** feature to force the device to connect to the Core. You might use this feature if Mobile@Work has not connected for some time, or you want to override a long sync interval to download updates.

You can use this feature to troubleshoot Core operations.

Procedure

1. Go to **Device & Users > Devices**.
2. Select the check box for the device.
3. Click **Actions > Force Device Check-in**.
4. The **Force Device Check-In** dialog appears.

   In the dialog, confirm the user and device information and enter a note.
5. Click **Force Device Check-in**.

Setting up background check-ins with APNs

This feature is not supported on Windows devices.

Managed iBooks

This feature is not supported on Windows devices.

Personal hotspot on/off switch

This feature is not supported on Windows devices.

Custom SyncML

SyncML is a markup language and the Windows standard of xml. Core allows administrators to upload SyncML files, however, SyncML is not a technology that Ivanti created. For information or support, best practices, and creating customized SyncML, contact Microsoft.

The **Windows Advanced Menu** allows you to enable custom features, including SyncML. Custom SyncML is turned off, by default and you must enable it first before you can upload a SyncML file to apply it to a label.

Enterprises can modify policies outside of Core by enabling and using SyncML that allow administrators the ability to delegate the task to someone who does not have access to Core to create SyncML files or modify scripts.

By using custom SyncML, you understand and assume all associated risks. You should always verify the content of the uploaded file with the latest Microsoft specification. Core does not validate custom SyncML and takes no responsibility for damages to devices, including, but not limited to, lost data or unresponsive devices.

Preparing to use SyncML

Before you try to use SyncML, verify that you have the following details in place:

1. Custom SyncML file to upload that will turn on an action (**Allow Notepad**, as an example call).
2. Custom SyncML file to upload that will turn off the same action (**Deny Notepad**, as an example reversal call for **Allow Notepad**).

In cases where the call will not have a feature to turn off (**Remote Lock**, for example) the device would happen only once and would not need a reversal call.

ⓘ Ivanti recommends that if your custom file turns on a behavior you should have another file that turns off the same behavior. Administrators implement the behavior (turn actions on or off, for example) via labels. However, the labels (and therefore, the behavior) must be managed manually. Core uses only the last setting sent.

How to use SyncML

WARNING: By using custom SyncML, you understand and assume the associated risks. You should always verify the content of the uploaded file with the latest Microsoft specification. Core does not validate custom SyncML and takes no responsibility for damages to devices, including, but not limited to, lost data or unresponsive devices.

This is a three-step process that requires you to:

Step 1: Enable custom SyncML.
Step 2: Upload SyncML files.
Step 3: Apply SyncML settings to labels.

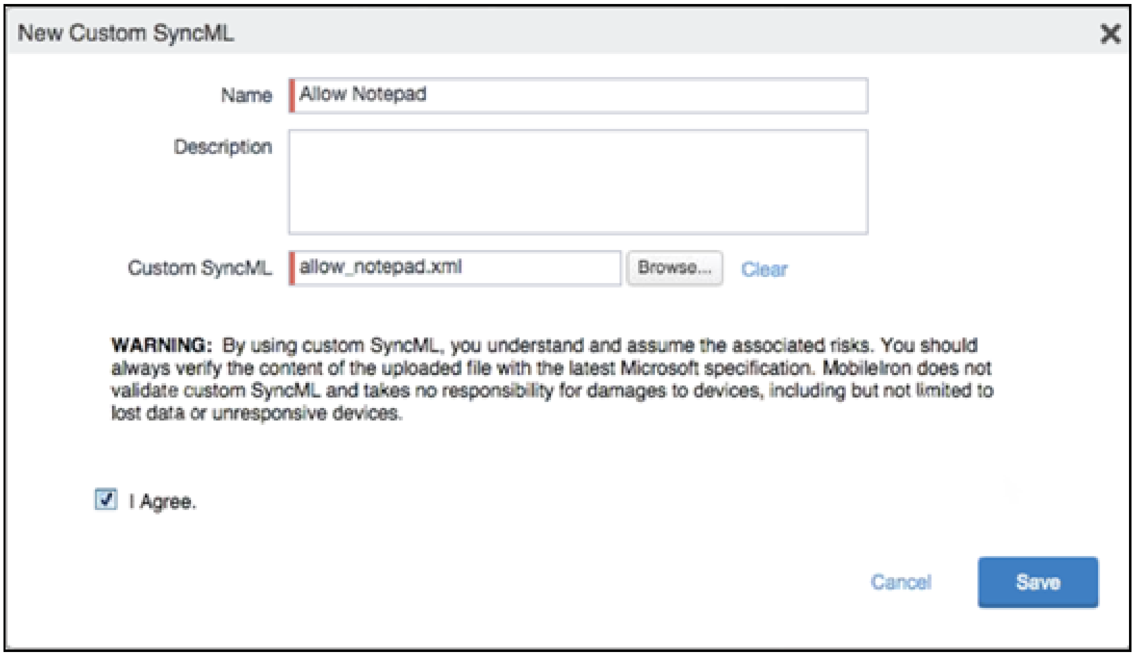
To enable custom SyncML:

1. In Core, go to **Settings > System Settings > Windows > Advanced Menu.**
2. Select **Enable Custom SyncML Menu**.
3. Click **Save** and **OK** after Core successfully enables this feature.

To upload SyncML files:

1. Log into the Admin portal.
2. Go to **Policies & Configs > Add New > Windows > Custom SyncML.**

FIGURE 1. NEW CUSTOM SYNCML



Name: Allow Notepad

Description:

Custom SyncML: allow_notepad.xml

WARNING: By using custom SyncML, you understand and assume the associated risks. You should always verify the content of the uploaded file with the latest Microsoft specification. MobileIron does not validate custom SyncML and takes no responsibility for damages to devices, including but not limited to lost data or unresponsive devices.

☑ I Agree.

3. Enter a name and description for the setting.
4. Click **Browse** to locate and upload the SyncML .xml file.

Custom SyncML files must have an .xml extension.

5. Read the warning.
6. Click **I Agree**.
7. Click **Save**.
8. Repeat these steps for the partner file.

To apply SyncML settings to labels:

1. Go to **Policies & Configs > Configurations.**
2. Select the newly added SyncML setting.
3. Select **Actions > Apply to Label**.
4. Select one or more labels.
5. Click **Apply** then **OK** to apply the setting the next time the device checks in.

Reporting on managed devices

Core provides a Web Services API that enables you to create reports for many aspects of your managed devices. For more information, see the ivanti API documentation on the Ivanti Product Documentation page. You can create reports in the following ways:

- "Exporting records to CSV" below
- Using APIs for reporting
- For details, refer to the **Feature Usage** and **Get Last Sync Time and State of ActiveSync Devices** sections in the *Core V2 API Guide*.

Exporting records to CSV

The enhanced Export to CSV feature provides access to numerous additional device attributes that were previously unavailable. The attributes are organized into platform-specific groups to make it easy to report on the relevant attributes for the devices you're working with.

Procedure

1. In the Admin Portal, go to **Device & Users > Devices**.
2. Use the **Advanced Search** feature or select a label to filter the devices you are interested in. All of the devices in the table will appear in the exported file.
3. Click **Export to CSV** to open the **Export CSV Spreadsheet** dialog.
4. Select the information to export. The exported fields for each selection are listed below.
5. Click **Export**. to export the DeviceSearchResult.csv file is to your computer.

Export to CSV Field Options

Below describes what is contained inside a .CSV file.

TABLE 9. EXPORT TO CSV FIELD OPTIONS

Type	Supported Variables
Selection	**Description**
Include Only Basic Device Information	User ID, Device UUID, Current Country Name, Current Operator Name, Current Phone Number, Device Owner, Display Name, Email Address, Home Country Name, Language, Last Check-In, Manufacturer, Model, Passcode, Passcode Expiration Time, Platform Name, Registration Date, Status
Include all device data, including the following options below.	(Select one or more options below)

TABLE 9. EXPORT TO CSV FIELD OPTIONS (CONT.)

Type	Supported Variables
User Attributes	User ID, Device UUID, account_disabled, Attribute Distinguished Name, custom1, custom2, custom3, custom4, Display Name, Email Address, First Name, Last Admin Portal Login Time, Last Name, LDAP Group Distinguished Name, LDAP User Distinguished Name, LDAP User Locale, locked_out, memberOf, Name, password_expired, Principal, sam_account_name, upn, User UUID ⓘ If defined in LDAP settings, custom attributes appear here also.
Common Device Attributes	User ID, Device UUID, APNS Capable, Background Status, Battery Level, Block Reason, Blocked, Cellular Technology, Client Build Date, Client Id, Client Last Check-in, Client Name, Client Version, Comment, Compliant, Creation Date, Current Country Code, Current Country Name, Current Operator Name, Current Phone Number, Device Admin Enabled, Device Encrypted, Device Is Compromised, Device Locale, Device Owner, Device Space, Display Size, EAS Last Sync Time, Ethernet MAC, Home Country Code, Home Country Name, Home Operator Name, Home Phone Number, IMEI, IMSI, IP Address, Language, Last Check-In, Manufacturer, MDM Managed, Memory Capacity, Memory Free, Model, Model Name, Modified Date, Non-compliance Reason, OS Version, Passcode, Passcode Expiration Time, Platform, Platform Name, Processor Architecture, Quarantined, Quarantined Reason, Registration Date, Registration IMSI, Registration UUID, Retired, Roaming, SD Card Encrypted, Security State, Serial Number, Status, Storage Capacity, Storage Free, Terms of Service Accepted, Terms of Service Accepted Date, Wi-Fi MAC, AzureDeviceId, AzureClientStatusCode, AzureIntuneDeviceStatus, AzureIntuneStatusUpdatedAt, AzureUserUpn

TABLE 9. EXPORT TO CSV FIELD OPTIONS (CONT.)

Type	Supported Variables
Windows Phone Attributes	User ID, Device UUID, AAD Enrolled, Antivirus Signature Status, Antivirus Status, Bitlocker Recovery Password, Bitlocker Startup Password, Bitlocker Startup Pin, DM Client Version, DM Client Version, Exchange ID, Firmware Version, Hardware Version, Health Data: AIK Present, Health Data: Bit locker Status, Health Data: Boot App SVN, Health Data: Boot Debugging Enabled, Health Data: Boot Manager Rev List Version, Health Data: Boot Manager SVN, Health Data: Boot Rev List Info, Health Data: Code Integrity Enabled, Health Data: Code Integrity Rev List Version, Health Data: DEP Policy, Health Data: ELAM Driver Loaded, Health Data: Issued, Health Data: OS Kernel Debugging Enabled, Health Data: OS Rev List Info, Health Data: PCR Hash Algorithm ID, Health Data: PCR0, Health Data: Reset Count, Health Data: Restart Count, Health Data: Safe Mode, Health Data: SBCP Hash, Health Data: Secure Boot Enabled, Health Data: Test Signing Enabled, Health Data: VSM Enabled, Health Data: Win PE, IMEI2, IMSI2, Last Hotfix ID, Last Hotfix Installed On, Local Time, Management Service Address, Network Adapter, OS Edition, Phone, Processor Type, Phone Number2, Processor Type, Roaming 2, Signed DM ID, WNS Channel URL, WP Publisher Device ID, WP Radio SWV

Setting the time zone of a device

This feature is applicable to: iOS 14.0 and tvOS 14.0 devices or supported newer versions. This feature is applicable for supervised devices only and does not require Location Services.

- The time zone device action is also displayed in the Device Details page of a device.
- Time zone changes made in the device will also reflect in the Core server.

> This device action triggers an error if the Force automatic Date & Time restriction is enabled in iOS Restrictions configuration.

- Administrators can search for a time zone. See "Advanced searching" on page 36.

Procedure

1. Go to **Devices & Users > Devices**.
2. Select one or more devices.

3. Click **Actions > iOS Only > Set Time Zone** for the selected device(s).
4. Enter the timezone string in the Olson Time Zone ID format, such as Pacific / Midway.
5. Click **Set Time Zone**.

Managing Custom Attributes

This section addresses all components relating to custom attributes.

Assigning a custom attributes role

An administrator the assigned role of **Manage custom attributes**, can add, view, edit, search, or remove custom user or device attributes. Custom attributes is a role for the global admin space.

Procedure

1. Log into the Admin Portal.

2. Go to **Admin > Admins**.

3. Select an administrator to assign the custom attributes role.

   This role is for the Global admin space.

4. Select one of the following options for the selected administrator:

   - **Actions** > **Assign to Space** > **Global** if the global space has not been assigned
   - **Actions** > **Edit Roles** if the global space has been assigned

5. Scroll down to the **Settings and Services Management** section.

6. Click the **Manage custom attributes** option and click **Save**.

Adding custom attributes to users and/or devices

You can add up to 300 custom attributes for users and 300 custom attributes for devices.

Procedure

1. Log into the Admin Portal.

2. Go to **Settings** > **System Settings** > **Users & Devices** > **Custom Attributes**.

3. In the **Custom Device Attributes** section, click **Add+**.

4. Enter the information for the custom attribute for devices, including:

Field	Description
Attribute Name	Enter a name for the custom attribute.
Attribute Description	Enter a meaningful description for the custom attribute.
Value Type	Select one of three value types: boolean, integer or string.
Variable Name	This field is read-only and displays the machine-generated name of the device that is used as a substitution variable in policies and configurations. For example, the substitution variable $USERNAME$ is replaced with the actual device username.
Actions	Click **Save**. The new custom device attribute is created and displays in the table.

5. (Optional) For Apple School Manager, click **Add+**and create a new Custom Device Attribute for device carts, for example, DeviceCartName, and choose the string value type. Remember this custom attribute name as you will need it when you turn on Apple Education in Core.

6. In the **Custom User Attributes** section, click **Add+**.

7. Referring to the table above, enter the information for the custom user attributes.

8. Click **Save**. The new custom user attribute is created and displays in the table.

9. (Optional) Repeat the steps, as needed.

Viewing custom attributes available for users and/or devices

Procedure

1. Log into the Admin Portal.

2. Go to **Settings > System Settings > Users & Devices > Custom Attributes**.

3. View all available custom attributes for users and/or devices.

   Search for the attribute, if necessary, to see all available attributes.

Viewing custom attributes assigned to users

Procedure

1. Log into the Admin Portal.

2. Go to **Devices & Users > Users**.

3. Locate a single user and expand the details.

4. Click the **Custom Attributes** tab.

Viewing custom attributes assigned to devices

Procedure

1. Log into the Admin Portal.
2. Go to **Devices & Users** > **Devices**.
3. Locate a single device and expand the details.
4. Click the **Custom Attributes** tab.

Editing custom attributes for users and/or devices

Procedure

1. Log into the Admin Portal.
2. Go to **Settings** > **System Settings** > **Users & Devices** > **Custom Attributes**.
3. Locate the attribute you want to edit.

   Search for the attribute, if necessary.
4. Click in the **ATTRIBUTE DESCRIPTION** field and modify the description.

   This field has a 255 characters limit.
5. Click **Save**.

Searching for custom attributes for users and/or devices

Procedure

1. Log into the Admin Portal.
2. Go to **Settings** > **System Settings** > **Users & Devices** > **Custom Attributes**.
3. Enter the search criteria for the name or description.

Exporting a log of the custom attributes for users and/or devices

Procedure

1. Log into the Admin Portal.
2. Go to **Logs**.
3. Scroll down the list of filters to **Custom Attributes**.
4. Click the number link of the custom attributes to display the complete list in the details pane.
5. Click **Export to CSV** to export all records to a single file.

Deleting custom attributes from users and/or devices

You can delete an attribute if it has only been assigned to a user or a device. An attempt to delete a custom attribute assigned to a label will prompt an error message that provides a list of labels to which it has been assigned.

Procedure

1. Log into the Admin Portal.
2. Select **Settings > System Settings > Users & Devices > Custom Attributes**.
3. Locate the attribute you want to remove.

   Search for the attribute, if necessary.
4. Click **Delete**.

Setting custom attribute values for device or users

Setting custom attribute values for device or user requires **Edit custom device attribute values** and **Edit custom user attribute values** roles.

To set custom attributes for devices:

1. Log into Admin Portal.
2. Select **Devices & Users > Devices**.

3. Check the box next to one or more devices.
4. Click **Actions > Set Custom Attributes**.
5. Set the value for attributes and click **Save**.

   You can also clear the value for an attribute by checking the **Clear Value** box and save.

To set custom attributes for users:

1. Log into Admin Portal.
2. Go to **Devices & Users > Users**.
3. Check the box next to one or more users.
4. Click **Actions > Set Custom Attributes**.
5. Set the value for attributes and click **Save**.

   You can also clear the value for an attribute by checking the **Clear Value** box and save.

ⓘ If you choose a single device or user when setting attribute values, the current attribute values are displayed. If you choose multiple devices or users, the current attribute values are not displayed.

Applying custom attributes to labels

Applying custom attributes to labels, requires **Label Management** permissions.

Procedure

1. Log into the Admin Portal.
2. Go to **Devices & Users > Labels**.
3. Click **Add Label > Filter**.

4. Locate the attribute using one of the following options:

    - Search for it in the **Field**, **Operator**, or **Value** fields.
    - Expand **Field** > **Custom Attributes** > **Device Attributes**.
    - Expand **Field** > **Custom Attributes > User Attributes**.

    For more information about field definitions, see "Device field definitions" on page 37.

5. Complete the criteria.
6. Click **Save**.

Pushing label attribute changes to devices and users

Changing attribute values for a user or device label does not trigger an automatic update. If you have changed the attribute values for a label, by default, changes will take effect:

- **For devices**: the next time the device checks in
- **For users**: the next scheduled LDAP sync

If you want the changes to go into effect immediately, take the following action:

- **For devices**: force a device check-in. See "Force Device Check-In" on page 78.
- **For users**: force an LDAP sync. See "Synchronizing with the LDAP server" in *Getting Started with Core*.

Managing Policies

Core uses policies to regulate the behavior of the devices it manages. Each policy consists of a set of rules. You can create multiple policies for each policy type, but only one active policy of each type can be applied to a specific device.

Refer to *Getting Started with Core* for information on the most commonly used policy topics, such as:

- Default policies
- Security policies
- Privacy policies
- Lockdown policies
- Sync policies

The topics in this chapter include the following advanced topics:

- "Working with default policies" on the next page
- "Importing and exporting policies" on the next page
- "Viewing policy status and platform support" on page 96
- "Edge Browser settings" on page 97
- "Sync policies and battery use" on page 98
- "Country changes and alerts" on page 98
- "Working with Windows Update policies" on page 98
- "Notifications of changes to the privacy policy" on page 99
- "Exporting the devices in the WatchList" on page 137

Related topics

For information on Mobile Threat Defense, including the MTD Local Actions policy, see the *Mobile Threat Defense Solution Guide for Core.*

Working with 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.

Unlike configurations, a device can have only one policy of each type.

Core provides defaults for the following policy types:

- Security (Refer to *Getting Started with Core* for details.)
- Privacy (Refer to *Getting Started with Core* for details.)
- Lockdown (Refer to *Getting Started with Core* for details.)
- Sync (Refer to *Getting Started with Core* for details.)
- ActiveSync (See "Working with ActiveSync policies" in the *Sentry Guide for Core*.)
- AppConnect global policy (Refer to the *AppConnect Guide for Core.)*

You cannot delete default policies.

The default settings for each policy type are listed in the section for each type.

Importing and exporting policies

You can import and export policies from one deployment of Core to another. Topics in this section include:

- "Exporting policies or configurations" on the next page
- "Importing policies or configurations" on page 95

ⓘ This feature is supported when importing or exporting policies or configurations between Core instances that are running the same version.

Exporting policies or configurations

Exporting policies and configurations help reduce errors when you have multiple instances of Core. You can export a configuration .json file for an existing policy, modify it, then import it to another policy. The export/import features allow you to do this.

Procedure

1. Select **Policies & Configs** > **Policies** or **Policies & Configs** > **Configurations**.

   All available policies are listed in the policies table.

   All available configurations are listed in the configurations table.

2. Select a single policy or configuration to export.

   You can sort, as necessary, to find the one you want to export.

3. Click **Export** to create an export .json file.

   No application-related information is captured when exporting a policy or configuration.

4. Enter an export password and confirm it in the two password fields.

   This password encrypts sensitive configuration data during export (including passwords and certificates). The same password is required to import the exported data to another Core server.

5. Check **Remember password for this session** if you want to re-use the password during a session.

   A session is defined as the length of a single login. The session ends when you log out or when you have been logged out by the system.

6. Locate the .json file, open, modify, and save it, as necessary.

   Review this file before reusing it as values are not verified before importing them. For instance, If a security policy .json file has a minimum password length of 2000, the imported profile will have a minimum password length of 2000 and, when pushed to devices, it will enforce all the devices to have such a big password. The encrypted hash of the sensitive data is displayed in the .json file, but the sensitive data is not displayed in plain text format in the .json file.

Importing policies or configurations

Importing policies and configurations help reduce errors when you have multiple instances of Core. You can export a configuration .json file for an existing policy, modify it, then import it to another policy. The export/import features allow you to do this.

Procedure

1. Select **Policies & Configs** > **Policies** or **Policies & Configs** > **Configurations**.

2. Click **Import** to locate a saved exported .json file.

3. Enter the name of the file or click **Browse** to locate it.

4. Enter the password created when the file was exported.

   See "Enter an export password and confirm it in the two password fields." on the previous page in "Exporting policies or configurations" on the previous page.

5. Check **Remember password for this session** if you want to re-use the password during a session.

   A session is defined as the length of a single log-in. The session ends when you log out or when you have been logged out by the system.

6. Read the warning message and click the **I Agree** check box.

7. Click **Import** to add the new policy to the policy table.

   If you import a policy that already exists, you can override the policy or cancel the import. If an exported policy has child object/s (such as app control rules and compliance actions), Core creates them during import. If the child objects already exist, they are overridden.

Viewing policy status and platform support

For any given device, you can view the status of a policy you have applied to that device, such as Pending, Sent, or Applied. For any given policy, you can view a list of supported platforms, such as Android, iOS, and Windows.

Topics in this section include:

- "Displaying policy status" below
- "Displaying supported platforms for policies" below

Displaying policy status

The Device Details pane on the **Device & Users > Devices** page displays status for the following tasks:

- apply lockdown policies
- apply security policies

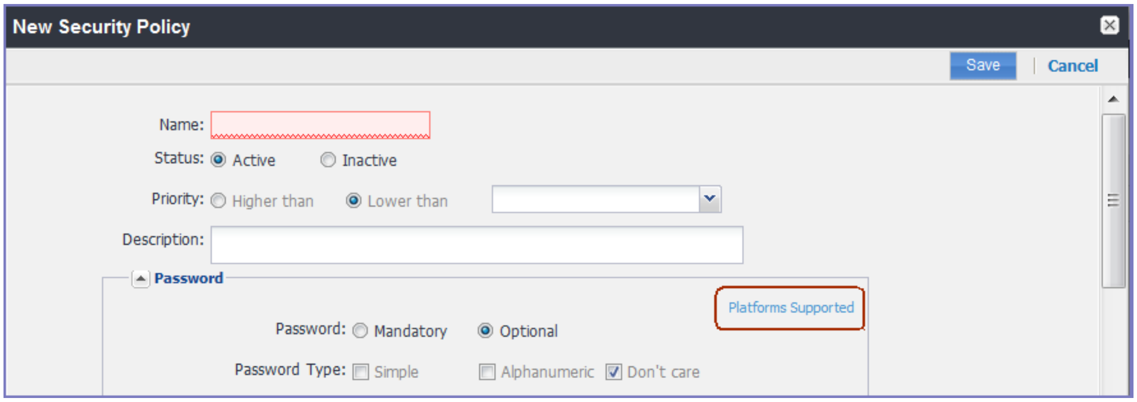
The categories of status you will see in the **Policies** tab are:

- **Pending**: The process of applying the policy has been started.
- **Sent**: The policy has been successfully sent to the device.
- **Applied**: Core has confirmed that the verifiable settings appear to have been applied to the device.
- **Partially Applied**: One or more settings may have been rejected by the device. This can mean that the feature is not supported by the device.

Displaying supported platforms for policies

To clarify which policies are supported on specific platforms, “Platforms Supported” links are included in the policy dialogs. For example:

FIGURE 1. PLATFORMS SUPPORTED LINK



Name:

Status: ● Active ○ Inactive

Priority: ○ Higher than ● Lower than

Description:

Password: ○ Mandatory ● Optional

Password Type: □ Simple □ Alphanumeric ☑ Don't care

Each link displays a table outlining the platform support for each policy feature.

Edge Browser settings

Edge Browser was introduced with Windows 10 and therefore, this feature is not supported on Windows Phone 8.1 devices. Disabling pop-ups and saved passwords for Edge browsers helps administrators prevent hackers from creating pop ups on end user desktop and mobile devices.

In previous releases, administrators could not disable these features. Starting with Core 9.0, these features are allowed by default. If administrators make no changes, device users will not see any changes, but hacker risks continue. However, if you disable these actions, end users might notice the features no longer work the same and request help.

Core 9.0 adds the capability for administrators to disable the following actions for Edge browsers on mobile devices:

- pop-ups (Windows 10 Desktop devices only)
- saved passwords

How to disable Edge browser settings

To disable pop-ups and password manager for Edge browsers on mobile devices:

1. In Core, go to **Policies & Configs** > **Policies**.
2. Select the **Default Lockdown Policy** and click **Edit**.
3. Scroll down to the **Windows** group.

4. Click **Disable** for one or both Edge browser settings:
   - Block Browser Popups
   - Browser Password Manager
5. Click **Save**.

Sync policies and battery use

If users note significant battery impact on their devices after installing the client (Apps@Work), consider reviewing and optimizing your sync policies.

Country changes and alerts

Country changes are monitored by the Mobile@Work client. Assuming that the **Sync While Roaming** option is not set to **No Sync**, each country change causes Apps@Work to send the change to Core. If Apps@Work can connect, then the **Event Center** generates the configured alerts, regardless of the sync interval. If connectivity is not established, then Apps@Work generates a local alert, if configured.

Working with Windows Update policies

To set up the Windows update policies:

1. Go to the Admin Portal.
2. Select **Policies & Configs** > **Policies** > **Add New** > **Windows** > **Windows Update**.
3. Use the following guidelines to complete this form:

Use the following guidelines to create or edit Windows update policies for Windows 10 devices:

Item	Description
Name	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. **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.
Description	Enter an explanation of the purpose of this policy.
Auto Update Strategy	The options are:

Item	Description
	• Notify user before downloading. • Auto install and notify for restart. • Auto install and restart (default). • Auto install at scheduled time. • Auto install at scheduled time without notifying user.
Scheduled Install Day	The options are: • Everyday (default) • Monday-Sunday
Scheduled Install Time	Every hour on the hour. The default is 3:00 AM
Update Sources	The options are: • Enterprise WSUS • Enterprise WSUS and Microsoft Update
URL to Enterprise WSUS Server	The URL for the instance of your enterprise Windows Server Update Services server.
Defer non-security Upgrades	In order to defer non-security upgrades, pause updates or upgrades, defer updates, or upgrades, administrators must: • Make sure that the URL to Enterprise WSUS Server is left blank (in **Policies & Configs** > **Policies** > **Windows** > **Windows Update**). • MS Error Reporting is Enabled (in **Policies & Configs** > **Policies** > **Lockdown**).
Pause Updates/Upgrades	Check this box to pause the update or upgrades based on the time period specified in the following options.
Defer Updates	The options are 0-4 weeks. The default is 0 weeks.
Defer Upgrades	The options are 0-8 months. The default is 0 months.

Use the Windows update policy to defer Microsoft upgrades and updates on Windows 10 devices using TH2 builds and above. Once the time frame of the deferment is up you cannot defer that update again on that device.

Notifications of changes to the privacy policy

This feature is not available on Windows devices.

Exporting the devices in the WatchList

The number in the **WatchList** field indicates the number of devices for which the configuration is still in queue.

Procedure

1. In the Core Admin Portal, go to **Policies & Configs** > **Configurations**.
2. Click the number in the WatchList field for the configuration for which you want to export the WatchList.

   The Pending Devices window appears. The window displays a list of devices for which the configuration is queued.
3. Click Export to export the list of devices.
4. The list is downloaded as .CSV file.

Managing Compliance

Core uses compliance policies to ensure that managed devices comply with security and administrator-defined compliance policies. Actions you define in policies, such as placing a device in quarantine, take effect when a device is non-compliant.

Refer to the following Knowledge Base articles for more information on compliance:

- How to determine why devices are out of compliance
- How to block compromised iOS and Android devices managed by MobileIron Core

The topics in this chapter include the following advanced topics:

- "Managing device compliance checks" below
- "Tiered compliance" on page 110
- "Compliance actions policy violations" on page 111
- "Viewing quarantine information" on page 115
- "Viewing configurations removed due to quarantine" on page 116
- "Custom compliance policies" on page 116

Managing device compliance checks

Devices are checked for compliance with assigned policies each time they check in with Core. In addition, Core checks all devices for compliance at regular intervals to detect out-of-compliance devices that have not checked in with Core.

Using Core, you can:

- Update device compliance status at any time
- Set the timing for device compliance checks
- Update the device last check-in and policy update time

Core receives information regarding device compliance status and last check-in only after devices actually check-in with Core. While you can request a device check-in using the Admin Portal, many factors can affect whether a device actually checks in, such as network connectivity, or whether a device is switched on or off.

Setting the device compliance check interval

By default, all devices are checked for policy compliance every 24 hours. You can change the time between compliance checks. The Compliance Check Interval setting applies to compliance checks by the server only. Out of compliance conditions include:

- Device is out of contact for the time limit you set.
- Device's root detection logic has found an issue.
- Device Admin privileges have been lost.
- Device has been decrypted.
- Device OS version is below the expected version.

It is best to run LDAP Sync and the compliance check at different times to avoid any potential Core performance problems.

Procedure

1. In the Admin Portal, go to **Policies & Configs > Compliance Actions**.
2. Click **Preferences**.
3. In **Edit Compliance Preferences**, select one of the timings for **Compliance Check Interval** (2, 4, 8, 12 or 24 hours).

Checking the compliance status of all devices every two or four hours may impact Core performance.

4. Click **Save**.

Updating device compliance status

You can manually request a device check-in to update device compliance status for one device, several devices, or all the devices registered to Core. Updating device compliance status enables:

- Administrators to update the compliance status of any device without waiting for the scheduled compliance check to run.
- Users to return to productive work when a compliance check is resolved, rather than wait for the next scheduled compliance check.
- Administrators to update the following information about a device:
  - Last check-in, updated when the device checks in
  - Policy update time

Without the ability to update device status, the device in the following example could be locked for almost 24 hours after complying with the defined security policy:

- A device status is jailbreak when Monday’s daily compliance check is done (the compliance check is set for 24 hours).
- The device is blocked when this status is detected, due to the defined security policy.
- The device is brought back into compliance two hours after Monday’s compliance check.
- The user cannot use the device until the Tuesday daily compliance check is run 22 hours from the time the device is back in compliance.

Procedure

1. In the Admin Portal, go to **Device & Users > Devices**.
2. Select one or more devices to update.
3. Select **Actions > Check Compliance**.
4. A message is displayed, letting you know that the compliance check has begun.

ⓘ The compliance status of the chosen devices may not change for one to two minutes after selecting **Check Compliance**.

To update device compliance information for all devices:

1. In the Admin Portal, go to **Policies & Configs** > **Compliance Actions**.
2. Click **Check Compliance** to display a message asking if you want to update compliance status for all devices.
3. Click **Yes** to check compliance status for all devices or click **No** to cancel the action.

The compliance status of the devices may not change for one to two minutes after selecting **Check Compliance**.

Compliance triggers and actions

Compliance actions, configured by the administrator, may be implemented locally on the device by Mobile@Work when certain system events have occurred that cause a compliance verification check, and only when the Enforce Compliance Actions Locally on Devices check box is selected for compliance action. Compliance verification checks also occur at the device check-in interval. Out of compliance conditions include:

- Out of Contact: the device has had no communication with the Core server for greater than the time period selected which is specified in days.
- Compromised: the device is suspected to be rooted or an app has been installed for rooted devices.
- Device Admin lost: the device administration privileges have been revoked.
- Decrypted: it has been detected that the device is no longer encrypted
- OS Version: the version of the operating system on the device is below the expected version.

Server compliance conditions and actions

Server compliance actions resulting from compliance conditions are listed in the table below.

TABLE 1. SERVER COMPLIANCE CONDITIONS AND ACTIONS

Action and OS	Out of Contact	Compromised	Device Admin lost	Decrypted	OS Version
Wipe (Android only, when enabling Android custom ROM)	Wipe the device when it has been out of contact.	Wipe the device when the device has been compromised.	The device cannot be wiped when the administrator privileges have been removed.	Wipe the device when it has been detected that the device has been decrypted.	Wipe the device when the OS version is less than expected.
Alert • Android • iOS	Send an alert when the device is out of contact. You can send alerts to device users, admins, or both users and admins, using SMS, push notifications, or email.	Send an alert when the device has been compromised. You can send alerts to device users, admins, or both users and admins, using SMS, push notifications, or email.	Send an alert when administrator privileges have been removed. You can send alerts to device users, admins, or both users and admins, using SMS, push notifications, or email.	Send an alert when it has been detected that the device as been decrypted. You can send alerts to device users, admins, or both users and admins, using SMS, push notifications, or email.	Send an alert when the OS version is less than expected. You can send alerts to device users, admins, or both users and admins, using SMS, push notifications, or email.
Remove Apps • Android • iOS Removal of apps is only possible if the MDM profile is sent by Core and is present on the device OR if the app settings have	Remove managed apps when the device is out of contact.	Remove managed apps when the device has been compromised.	Managed apps cannot be removed when administrator privileges have been removed.	Remove managed apps when the device has been decrypted.	Remove managed apps when the OS version is less than expected.

Action and OS	Out of Contact	Compromised	Device Admin lost	Decrypted	OS Version
the "Remove app when device is quarantined of signed-out" check box selected.					
Quarantine All - Android - iOS All Android Enterprise apps and functionality are hidden, except Downloads, Google Play Store, and Mobile@Work. (Applicable only if the "Quarantine app when device is quarantined" check box is selected.)	Remove all configurations when the device is out of contact.	Remove All configurations when the device has been compromised.	Remove All configurations when administrator privileges have been removed.	Remove All configurations when the device has been decrypted.	Remove All configurations when the OS version is less than expected.
Quarantine All Except Wi-Fi - Android - iOS	Remove all configurations except for Wi-Fi.	Remove all configurations except for Wi-Fi when compromised.	Remove all configurations except for Wi-Fi when administrator privileges have been removed.	Remove all configurations except for Wi-Fi when the device has been decrypted.	Remove all configurations except for Wi-Fi when the OS version is less than expected.

Action and OS	Out of Contact	Compromised	Device Admin lost	Decrypted	OS Version
• macOS (For Android Enterprise apps, this is applicable only if the "Quarantine app when device is quarantined" check box is selected.)					
Quarantine All Except Wi-Fi on Wi-Fi Only • Android • iOS • macOS (Applicable only if the "Quarantine app when device is quarantined" check box is selected.)	Remove all configurations except for Wi-Fi on Wi-Fi only devices.	Remove all configurations except for Wi-Fi on Wi-Fi only devices when compromised.	Remove all configurations except for Wi-Fi on Wi-Fi only devices when administrator privileges have been removed.	Remove all configurations except for Wi-Fi on Wi-Fi only devices when the device has been decrypted.	Remove all configurations except for Wi-Fi on Wi-Fi only devices when the OS version is less than expected.
Block or retire AppConnect apps • iOS	not applicable	Block (unauthorized) or retire (unauthorize and wipe) AppConnect apps	not applicable	not applicable	not applicable

Action and OS	Out of Contact	Compromised	Device Admin lost	Decrypted	OS Version
"Block" means blocking access to AppConnect apps.					

Local compliance conditions and actions

Local compliance actions do not apply to Mobile Threat Defense functionality included with Mobile@Work clients. There are also no local compliance actions for Mobile@Work for macOS devices.

Local compliance enforcement actions resulting from compliance conditions are listed in the table below.

TABLE 2. LOCAL COMPLIANCE CONDITIONS AND ACTIONS

Situation	OS	Action
When the device can communicate with Core to perform a Compliance Check	**Alert** • Android • iOS	Send an alert when the device is out of contact. Alerts are sent to device users, admins, or both users and admins, using SMS, push notifications, or email.
	Block AppConnect apps • Android • iOS	Blocks access to AppConnect apps.
	Quarantine • iOS (Applicable only if the "Quarantine app when device is quarantined" check box is selected.)	When the device is out of contact, all configurations, managed apps and iBooks content are removed. New app downloads are disallowed.
	Quarantine • Android	When the device is out of contact, all configurations and managed apps are removed. New app downloads are disallowed.

Situation	OS	Action
	(Applicable only if the "Quarantine app when device is quarantined" check box is selected.)	
	Quarantine • Android Enterprise	All Android Enterprise apps and functionality are hidden, except Downloads, Google Play Store, and Mobile@Work.
When the device can NOT communicate with Core to perform a Compliance check	**Alert** • Android • iOS	Send an alert when the device is out of contact. Alerts are sent to device users, admins, or both users and admins, using SMS, push notifications, or email.
	Block AppConnect apps • Android • iOS	Blocks access to AppConnect apps.
	Quarantine • iOS (Applicable only if the "Quarantine app when device is quarantined" check box is selected.)	When the device is out of contact, all configurations, managed apps and iBooks content are removed. New app downloads are disallowed. Quarantine action requires all appConnect apps to be re-installed after the device is back in compliance.
	Quarantine • Android (Applicable only if the "Quarantine app when device is quarantined" check box is selected.)	When the device is out of contact, all configurations and managed apps are removed. New app downloads are disallowed.
	Quarantine • Android Enterprise	All Android Enterprise apps and functionality are hidden, except Downloads, Google settings, Google Play Store, and Mobile@Work.

Situation	OS	Action
	Retire • Android Enterprise	The work profile is deleted or the managed device will be factory reset. This action is not reversible.

Tiered compliance

Administrators can apply multiple compliance actions over time on violating devices using tiered compliance. The following example describes a possible 3-tiered compliance action:

1. Send device users a warning message that their device is out of compliance, and give them time to fix the violation.
2. If the device is violating the same policy 24 hours later, Core sends users a second message and blocks the device.
3. If the device continues to violate the same policy another 24 hours later, Core sends users a third message and quarantines the device.

The increasing penalties over time allow a user that is unintentionally violating a policy to get back under compliance before punitive measures are taken, rather than immediately pulling email configurations, for example, off the device and interrupting normal work flow.

Tiers beyond the first one are only used by compliance policy rules, and are not used for security policies.

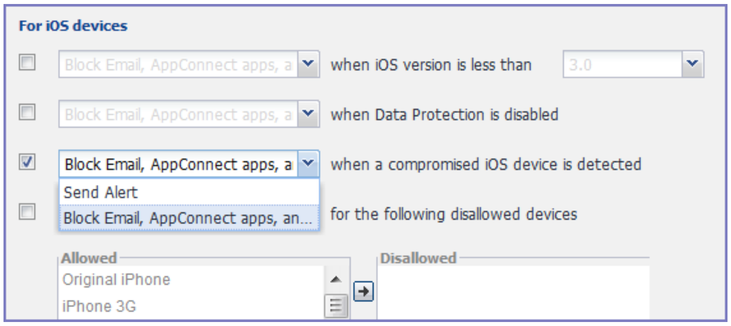
Tiered compliance behavior

- Tiered compliance checks do not run based on delay times. For example, if the delay time is 4 hours, Core does not automatically run a tiered compliance check after 4 hours. Instead, the next compliance check will occur in one of the following cases:
    - Device Check-in
    - Compliance check from the Devices page
    - Periodic compliance check (if the device has not checked in since the last periodic compliance check)
- If a device check-in or compliance check occurs during the interval between two tiers, Core will not take action based on the next tier. Core will only take action for the next tier after the delay time between tiers has elapsed.
- Delays between tiers are cumulative. For example, if the delay for tier 2 is 4 hours, and 8 hours for tier 3, then Core takes tier 3 action after 12 hours.

Compliance actions policy violations

You can assign compliance actions for security policy violations and for compliance policy violations. When you configure access control in either type of policy, you can select default compliance actions that are provided with Core. You can also select custom compliance actions that you create.

FIGURE 1. COMPLIANCE ACTIONS POLICY VIOLATIONS



For iOS devices

□ Block Email, AppConnect apps, a ▾ when iOS version is less than 3.0 ▾

□ Block Email, AppConnect apps, a ▾ when Data Protection is disabled

☑ Block Email, AppConnect apps, a ▾ when a compromised iOS device is detected

Send Alert
Block Email, AppConnect apps, an...

□ for the following disallowed devices

Allowed: Original iPhone, iPhone 3G

Disallowed

To create the custom compliance actions, see "Custom compliance actions" on the next page.

Default compliance actions

The following table describes the default compliance actions:

TABLE 10. DEFAULT COMPLIANCE ACTIONS TABLE

Default compliance action	Description
Send Alert	Sends alert that you configured for the policy violation. To configure the alert, see "Policy violations event settings" on page 375.
Block Email, AppConnect Apps And Send Alert	This feature is not supported on Windows devices.
Customized compliance actions	These actions can contain 4 tiers of actions. Tiers 2-4 are only used in compliance policies; they are not used by legacy security policies. Security policies only perform the action defined in tier 1.

Custom compliance actions

You can customize the compliance actions that you want to take for the settings on the Compliance Actions page under Policies & Configs. After you create your customized compliance actions, the actions you created appear in a drop-down list in the **Access Control** section of your security policies.

Custom compliance actions enable you to specify combinations of the following actions:

- Send alert
- Block email access and AppConnect apps (includes blocking app tunnels)
- Quarantine: block email access, block app tunnels, block AppConnect apps, and wipe AppConnect app data
- Remove configurations (i.e., profiles)
- Specify exceptions for Wi-Fi-only devices

Once you create a set of these actions, you can select that set from the drop downs in the **Access Control** section of security policies.

Creating a compliance action

With custom compliance actions, you can create actions to better manage access control. With tiered compliance actions, you can customize them to include up to 4 levels of action to better manage compliance actions.

Procedure

1. Log into the Admin Portal.
2. Go to **Policies & Configs > Compliance Actions**.
3. Click **Add+** to open the **Add Compliance Action** dialog box.
4. Select the appropriate fields as described in the "Add Compliance Action table" below.
5. If you want to add another set of actions, click the plus (+) button and select the fields, as necessary, to complete the second compliance action.
6. If you want to add another set of actions, click the plus (+) button and select the fields, as necessary, to complete the third compliance action.
7. Click **Save** to add the new compliance action for access control and compliance actions.
8. You can select them by going to:
   - **Policies & Configs > Policies >** policy > **Edit > Access Control** section (1 tier only).
   - **Policies & Configs > Compliance Policies > Add+ > Compliance Policy Rule > Compliance Actions** drop-down (1-4 tiers).

Add Compliance Action table

The following table describes the Add Compliance Actions options:

TABLE 1. ADD COMPLIANCE ACTION FIELDS

Item	Description
Name	Enter an identifier for this set of compliance actions. Consider specifying the resulting action so that the action will be apparent when you are editing a security policy.
Enforce Compliance Actions Locally on Devices	This feature is not supported on Windows devices.
ALERT: Send a compliance notification or alert to the user	Select if you want to trigger a message indicating that the violation has occurred. Core sends alerts to users, administrators, or both. To configure the alert, see "Policy violations event settings" on page 375.

Item	Description
BLOCK ACCESS: Block email access and AppConnect apps	This feature is not supported on Windows devices.
QUARANTINE: Quarantine the device (Select this check box to display the other Quarantine options.)	This feature is not supported on Windows devices. •
QUARANTINE: Remove All Configurations and SaaS Sign-on Policy	This feature is not supported on Windows devices.
QUARANTINE: Do not remove Wi-Fi settings for Wi-Fi only devices	This feature is not supported on Windows devices.
QUARANTINE: Do not remove Wi-Fi settings for all devices (iOS and Android only)	This feature is not supported on Windows devices.
QUARANTINE: Remove iBooks content, managed apps, and block new app downloads	This feature is not supported on Windows devices.
Retire: Retire the Work profile or factory reset the managed device	This feature is not supported on Windows devices.

When the compliance action takes effect

When you first apply a security policy, several factors affect the amount of time required to communicate the changes to targeted devices:

- sync interval
- time the device last checked in

- battery level
- number of changes already queued
- whether **Enforce Compliance Actions Locally on Devices** is selected.

Once the change reaches the device, Core checks the device for compliance. If the device is out of compliance, then the action is performed.

If the action for a security violation can be enforced locally on the device, and that option is selected in the Compliance Action dialog, then Apps@Work initiates the compliance action without requiring contact with Core.

Viewing quarantine information

Devices that have had configurations removed due to policy violations are considered quarantined. You can view quarantine information in the following places:

- **Device & Users** > **Devices** page
- **Policies & Configs** > **Configurations** page
- **Dashboard** page

Procedure

1. Go to **Device & Users** > **Devices**.
2. Click **Advanced Search**
3. Enter the search phrase: “common.quarantined” = true
4. Click **Search**.

To view information about an individual quarantined device:

1. Go to **Device & Users** > **Devices**.
2. Note devices that have been highlighted and appear with a quarantine icon.
3. Expand the device details for a quarantined device.
4. Click the **Configurations** tab in the device details panel to see which configurations have been removed due to quarantine.

Viewing configurations removed due to quarantine

You can view the configurations that Core has removed due to quarantine on the Configurations page.

1. Go to **Policies & Configs** > **Configurations**.
2. Click a number link in the **Quarantined** column to display a list of devices that have had the configuration removed.

Dashboard page: Device by Compliance chart

To see how many devices are quarantined:

1. Go to **Dashboard**.
2. View the **Device by Compliance** chart. (If the chart is not visible, click **Add** to add it.)
3. To see a list of all quarantined devices, click the quarantined category.

Custom compliance policies

Core provides security policies for 10 static definitions to mark a device as non-compliant. These policies have limited customization options, but are a quick and easy way to begin to set up compliance policy rules. The Compliance Policies feature allows administrators to define their own criteria for marking devices non-compliant. They can combine dozens of device and user fields to create non-compliant matching criteria.

Compliance policy rules use the **Advanced Search** filter criteria to define non-compliant devices. Each compliance policy rule has a filter criteria and an associated compliance action object. Access compliance policies by selecting **Policies & Configs > Compliance Policies** from the Admin Portal.

Core uses custom device and user attributes to set up compliance policy rule conditions. These settings, listed under **Devices & Users > Devices > Advanced Search > User Fields > LDAP > User Account Control** in the Admin Portal, are:

- Account Disabled
- Locked Out
- Password Expired

Compliance policies are enforced by Core during device check-in.

The work flow to set up and use compliance policies is:

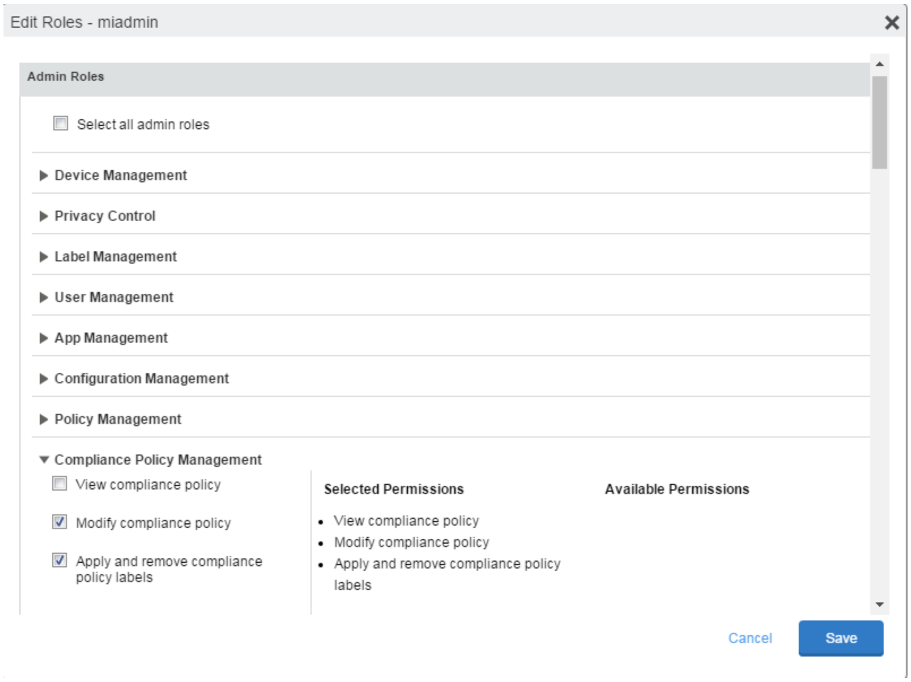
- "Assigning compliance roles" below
- "Managing compliance policy rules" on the next page
- "Managing compliance policy groups" on page 124
- "Device search fields for compliance rules" on page 128

Assigning compliance roles

The following describes how to assign compliance roles.

Procedure

1. Log into the Admin Portal.
2. Go to **Admin > Admins**.
3. Select a user then click **Actions > Edit Roles**.
4. Select an Admin Space.
5. Scroll down the window to the **Compliance Policy Management** section.



Edit Roles - miadmin

Admin Roles

□ Select all admin roles

▶ Device Management
▶ Privacy Control
▶ Label Management
▶ User Management
▶ App Management
▶ Configuration Management
▶ Policy Management
▼ Compliance Policy Management

□ View compliance policy
☑ Modify compliance policy
☑ Apply and remove compliance policy labels

Selected Permissions
- View compliance policy
- Modify compliance policy
- Apply and remove compliance policy labels

Available Permissions

6. Select one or more of the roles:

   - **View compliance policy**: Allows the selected user to view rules, groups, lists, and configuration.
   - **Modify compliance policy**: Allows the selected user to create, edit, and delete rules and groups.
   - **Apply and remove compliance policy labels**: Allows the selected user to add or remove groups from labels.

7. Scroll to the **Settings and Services Management** section.
8. Select **View settings and services**.
9. Click **Save**.

Managing compliance policy rules

Compliance policy rules are the building blocks in compliance policy groups used to manage device compliance. Administrators create compliance policy groups, add compliance policy rules to the groups, apply the groups to labels pushed to devices. Administrators can create a group with no rules or add compliance policy rules while creating the compliance policy group, if rules have already been created. They can also modify the group, including the name, description, and selected rules. This section describes:

- "Creating compliance policy rules" below
- "Substitution variables for compliance policy rules" on page 120
- "Viewing and modifying compliance policy rules" on page 122
- "Deleting compliance policy rules" on page 123
- "Searching for compliance policy rules" on page 123

Creating compliance policy rules

A single rule can be in multiple compliance policy groups.

Procedure

1. Go to the Admin Portal.
2. Select **Policies & Configs > Compliance Policies**.
3. Click **Compliance Policy Rule** tab and then click **Add+**.
4. Add a unique name in the **Rule Name** field.
5. Select the **Status** to **Enabled** or **Disable**.
6. Enter a description of the rule if desired.
7. Build a **Condition** using **Advance Search** to define non-compliance. For a list of definitions / values of the items to search on, see "Advanced searching" on page 36.

   It is recommended to have one Condition set to include when Mobile@Work last checked in within the last 30 days. See the TIP below.

8. In the **Compliance Actions** field, select from the drop-down to use on devices matching the condition.
9. (Optional) In the **Message** field, enter text for alerts generated by violations of the policy rule. When configuring the message accompanying the compliance action, custom attributes (see "Adding custom attributes to users and/or devices" on page 86) and substitution variables can be inserted into the text. To do this, copy the appropriate variable (see the "Substitution variable" on page 121 table) located to the right of the Message field and paste it into the text box. Before sending the message to the device, Core will replace the substitution variable to the actual value of the custom attribute for that device. For example, $FIRST_NAME$ would insert the first name of the target user into the message.
10. If you don't want the search results to include retired devices, select the **Exclude retired devices from search results** check box.
11. Click **Save**.

TIP - It is recommended to have a Compliance Policy Rule with one condition set to include when Mobile@Work last checked in with Core. This is helpful if you need assurance that Mobile@Work is running on devices (for example, for use in Mobile Threat Defense).

Procedure

1. Go to the Admin Portal.
2. Select **Policies & Configs** > **Compliance Policies**.
3. Click **Compliance Policy Rule** tab and then click **Add+**.
4. Enter *ClientLastCheckIn* in the **Rule Name** field.
5. Enter **Condition** > **All.**
6. Go to **Field** and type in "Client Last Check-In" or select **Common Fields > Client Last Check-In**.

   The regular expression is listed below; green check mark indicates regular expression is accepted.
7. Select **within the last** in the **Value** field; enter **30 days** in the remaining two fields.
8. Keep the default setting of **Exclude retired devices from search results.**
9. In the **Compliance Actions** field, select **Send Alert** from the drop-down.
10. Click **Save**.

Substitution variables for compliance policy rules

The following table lists the substitution variables for compliance policy rules.

TABLE 11. SUBSTITUTION VARIABLES FOR COMPLIANCE POLICY RULES

Category	Substitution variable
Compliance policy rule customized message	The substitution variables are available for use in compliance policy rules for all devices. To use in a compliance action message, copy/paste the variable into the Message field. • $MANAGED_APPLE_ID$ • CN • $CONFIG_UUID$ • $DEVICE_CLIENT_ID$ • $DEVICE_ID$ • $DEVICE_IMEI$ • $DEVICE_IMSI$ • $DEVICE_MAC$ • $DEVICE_PIVD_ACTIVATION_LINK$ • $DEVICE_SN$ • $DEVICE_UDID$ • $DEVICE_UUID$ • $DEVICE_UUID_NO_DASHES$ • $DISPLAY_NAME$ • $EMAIL$ • $EMAIL_DOMAIN$ • $EMAIL_LOCAL$ • $FIRST_NAME$ • $GOOGLE_AUTOGEN_PASSWORD$ • $ICCID$ • $LAST_NAME$ ⓘ For Shared iPad devices and User Enrolled devices only. • $MI_APPSTORE_URL$ • $MODEL$ • $NULL$

TABLE 11. SUBSTITUTION VARIABLES FOR COMPLIANCE POLICY RULES (CONT.)

Category	Substitution variable
	• OU • $PASSWORD$ • $PHONE_NUMBER$ • $RANDOM_16$ • $RANDOM_32$ • $RANDOM_64$ • $REALM$ • $SAM_ACCOUNT_NAME$ • $TIMESTAMP_MS$ • $USERID$ • $USER_CUSTOM1$ • $USER_CUSTOM2$ • $USER_CUSTOM3$ • $USER_CUSTOM4$ • $USER_DN$ • $USER_LOCALE$ • $USER_UPN$

Viewing and modifying compliance policy rules

You can view or modify a compliance policy rule. Viewing a rule requires the View role and modifying a rule requires the Modify role.

You can modify a rule without removing it from an assigned group. For instance, you can change its status from Enabled to Disabled to troubleshoot it. When you modify a rule, the change is applied to all the groups that use the rule.

Procedure

1. Go to the Admin Portal.
2. Select **Policies & Configs** > **Compliance Policies** > **Compliance Policy Rule**.
3. Select the name of the rule you want to modify and click **Edit**.
4. Modify details, as necessary, including disabling the rule.
5. Click **Save**.

Deleting compliance policy rules

Procedure

1. Go to the Admin Portal.
2. Select **Policies & Configs** > **Compliance Policies** > **Compliance Policy Rule**.
3. Select the name of one or more rules to delete.
4. Click **Actions** > **Delete**.

Searching for compliance policy rules

Procedure

1. Go to the Admin Portal.
2. Select **Policies & Configs** > **Compliance Policies** > **Compliance Policy Rule**.
3. Enter a name in the search field.

4. Use one of the following filters:
   - All
   - Enabled
   - Disabled
5. Click **Search**.

Managing compliance policy groups

Compliance policy groups are applied to devices to manage device compliance. Administrators create compliance policy groups, add compliance policy rules to the groups, apply the group's rules to devices matching the label criteria.

Administrators can create a group with no rules or add compliance policy rules while creating the compliance policy group, if rules have already been created. They can also modify the group, including the name, description, and selected rules. This section describes:

- "Creating compliance policy groups" below
- "Modifying compliance policy groups" on the next page
- "Adding compliance policy rules to a group" on the next page
- "Applying compliance policy groups to labels" on page 126
- "Removing compliance policy groups from labels" on page 127
- "Deleting compliance policy groups" on page 127
- "Searching for compliance policy groups" on page 127

Creating compliance policy groups

You can create a group without adding rules, which can be added later. One rule can be member of multiple groups.The following provides the steps to add one or more compliance policy rules to a compliance policy group.

Procedure

1. Go to the Admin Portal.
2. Select **Policies & Configs** > **Compliance Policies**.
3. Click **Compliance Policy Group** tab.
4. Click **Add+**. The Add Compliance Policy Group page displays.
5. Enter a unique name in the **Group Name** field.
6. Select Enabled in the **Status** field.
7. Move one or more rules from **Available Rules** to the **Selected Rules** list.
8. Click **Save**.

Modifying compliance policy groups

The following provides the steps to modify compliance policy groups.

Procedure

1. Go to the Admin Portal.
2. Select **Policies & Configs** > **Compliance Policies** > **Compliance Policy Group**.
3. Select the name of the group you want to modify.
4. Modify details, as necessary, including the name, description, or to enable or disable the group.
5. Click **Save** in the **Details** section.
6. Click **Edit** in the Rules section.
7. Modify rules, as necessary, by adding or removing rules.
8. Click **Save** in the **Rules** section.

Adding compliance policy rules to a group

One rule can be a member of multiple groups. This procedure requires that you have already created one or more rule. See "Creating compliance policy rules" on page 118 for details.

Procedure

1. Go to the Admin Portal.
2. Select **Policies & Configs** > **Compliance Policies** > **Compliance Policy Group**.
3. Double-click the name of the group to which you want to add one or more rules.
4. Go to the **Rules** section and click **Edit**.
5. Move one or more rules from the **Available Rules** list to the **Selected Rules** list.
6. Click **Save** in the **Rules** section.

Applying compliance policy groups to labels

Once a group (and its underlying rules) is assigned to devices, status of the devices are evaluated based on the conditions in the rules for compliance. Compliance Policy rules are evaluated against each device in the following ways:

- During device check-in
- Periodically, during the compliance policy check interval. This is set at **Policies & Configs** > **Compliance Actions** > **Preferences**.
- When a manual Check Compliance is initiated by the administrator. This can be set at **Policies & Configs** > **Compliance Actions** > **Check Compliance** or on the **Devices** page under **Actions**.

Procedure

1. Go to the Admin Portal.
2. Select **Policies & Configs** > **Compliance Policies** > **Compliance Policy Group**.
3. Select the name of the compliance policy group you want to apply to label.
4. Click **Actions** > **Apply to Labels**.
5. Select one or more of the labels.
6. Click **Apply**.

Removing compliance policy groups from labels

Once a group (and its underlying rules) is assigned to devices, status of the devices are evaluated based on the conditions in the rules for compliance. The following describes the steps to apply a compliance policy groups to one or more labels.

Procedure

1. Go to the Admin Portal.
2. Select **Policies & Configs** > **Compliance Policies** > **Compliance Policy Group**.
3. Select the name of the compliance policy group you want to remove from a label.
4. Click **Actions** > **Remove from Labels**.
5. De-select one or more of the labels.
6. Click **Apply**.
   After the next device check in, these changes will apply.

Deleting compliance policy groups

The following provides the steps to delete one or more compliance policy groups.

Procedure

1. Go to the Admin Portal.
2. Select **Policies & Configs** > **Compliance Policies** > **Compliance Policy Group**.
3. Select the name of one or more groups to delete.
4. Click **Actions** > **Delete**.

Searching for compliance policy groups

The following provides the steps to search for compliance policy group.

Procedure

1. Go to the Admin Portal.
2. Select **Policies & Configs** > **Compliance Policies** > **Compliance Policy Group**.

3. Enter a name in the search field.
4. Use one of the following filters:
   - All
   - Enabled
   - Disabled
5. Click **Search**.

Device search fields for compliance rules

This section includes the compliance action objects the compliance policy rules use for device search fields. In addition to the fields listed in the below table, any Custom Device Attributes or Custom User Attributes that were added in **Settings > System Settings > Users & Devices > Custom Attributes** will also be available for searching.

The following table lists the available objects, including:

- Common fields
- Custom fields
- Android devices
- iOS devices
- Windows devices
- User fields (including LDAP fields)

TABLE 12. DEVICE SEARCH FIELDS FOR COMPLIANCE RULES

Category	Compliance policy objects
Common	The following search fields are available for use in compliance rules for all devices: cellular_technology, client_name, client_build_date, client_version, creation_date, current_country_code, current_country_name, country_name, current_operator_name, carrier_short_name, current_phone_number, current_phone_number, data_protection_enabled, data_protection_reasons, device_admin_enabled, device_encrypted, device_is_compromised, eas_last_sync_time, ethernet_mac, home_country_code, home_country_name, home_operatory_name, home_phone_number, imei, imsi, language, last_connected _at, locale, location_last_captured_at, manufacturer, mdm_managed, mdm_tos_accepted, mdm_tos_accepted_date, model, model_name, os_version, owner, pending_device_passcode, pending_device_passcode_expiration_time, platform_name, platform, registration_date, registration_imsi, retired, roaming, security_state, status, uuid, wifi_mac_address
Android	The following search fields are available for use in compliance rules for all Android devices: admin_activated, attestation, afw_capable, brand, Client_version_code, device_roaming_flag, knox_version, manufacturer_os_version, mdm_enabled, multi-mdm, os_build_number, os_update_status, registration_status, samsung_dm, secure_apps_encryption_enabled, secure_apps_encryption_mode, security_detail, security_patch, usb_debugging, dpm_encryption_status
iOS	The following search fields are available for use in compliance rules for all iOS devices: BluetoothMAC, BuildVersion, CarrierSettingsVersion, Current MCC, Current MNC, DataRoamingEnabled, data_protection, forceEncryptedBackup, iCloud Backup Is Enabled, iOSBackgroundStatus, iPhone PRODUCT, iPhone VERSION, IsDeviceLocatorServiceEnabled, IsDEPEnrolledDevice, IsDoNotDisturbInEffect, IsMDMLostModeEnabled, IsMDMServiceEnrolledDevice, iTunesStoreAccountIsActive, ProductName, PasscodePresent, PasscodeIsCompliantWithProfiles, PasscodeIsCompliant, Personal Hotspot Enabled, SerialNumber, Supervised, SIM MCC, SIM MNC, Subscriber Carrier Network, Voice Roaming Enabled, osUpdateStatus,
Windows	The following search fields are available for use in compliance rules for all Windows devices: dm_client_version, wp_firmware_version, wp_hardware_version, wp_os_edition, health_data_issued, health_data_aik_present, health_data_dep_policy, health_data_bit_locker_status, health_data_boot_manager_rev_list_version, health_data_code_integrity_rev_list_version, health_data_secure_boot_enabled, health_data_boot_debugging_enabled, health_data_os_kernel_debugging_enabled, health_data_code_integrity_enabled, health_data_test_signing_enabled, health_data_safe_mode, health_data_win_pe, health_data_elam_driver_loaded, health_data_vsm_enabled, health_data_pcr0, health_data_sbcp_hash,

TABLE 12. DEVICE SEARCH FIELDS FOR COMPLIANCE RULES (CONT.)

Category	Compliance policy objects
User	The following search fields are available for use in compliance rules user-related fields, including LDAP: email_address, user_id, attr_dn, dn, name, locale, principal, upn, account-disabled, locked_out, password_expired, custom1, custom2, custom3, custom4, <dynamically created custom user-attribute field name #1>, <dynamically created custom user-attribute field name #2>, <dynamically created custom user-attribute field name #3>, <dynamically created custom user-attribute field name #4>, <dynamically created user-attribute field names>

Managing Device Settings with Configurations

This section addresses the automation of major settings via configurations that can then be applied to a large inventory of different devices.

Management of device settings with configurations

Configuring major settings across a large inventory of different devices can mean a major daily time investment for IT personnel. You can automate this process by specifying and distributing configurations, previously called app settings. A configuration is a group of settings to be applied to devices.

The following table summarizes the device settings managed by Core. Configurations are found on the **Policies & Configs > Configurations** page.

TABLE 13. DEVICE SETTINGS

Category	Configuration Type
Infrastructure	• Exchange • Email • Wi-Fi • VPN • Certificates • Certificate Enrollment
AppConnect	• App Configuration • Container Policy
Features	• Docs@Work • Web@Work
Windows	• Enrollment Token (AET) (Windows Phone only) • Sideloading Key (Windows 8.1 only)

Configurations page

A configuration (previously called app settings) is a group of settings that are applied to devices. Go to the **Policies & Configs > Configurations** page to create and manage configurations. It displays the following information for each configuration.

TABLE 14. CONFIGURATIONS PAGE OPTIONS

Field	Description
Name	Indicates a name for this group of settings.
Configuration Type	Indicates the kind of configuration.
Bundle/Package ID	If this configuration is links to a App Catalog entry, the Bundle/Package ID will display here.
Description	Displays additional information about this group of settings.

TABLE 14. CONFIGURATIONS PAGE OPTIONS (CONT.)

Field	Description
# Phones	Indicates the number of phones to which this group of settings has been applied. Click the link to display a list of the devices.
Labels	Lists the labels to which this group of settings has been applied.
WatchList	Displays the number of devices for which this group of settings is queued. Click the link to display a list of the devices.
Quarantined	Displays the number of devices that have had configurations removed due to policy violations. Click the link to display a list of the devices. See "Creating a compliance action" on page 112 for information on quarantining devices.

Required role: Administrator must have the **View configuration** role to access the Configurations page.

Default configurations

Core provides the following default configurations. The names of these default configurations start with "System - ".

TABLE 15. DEFAULT CONFIGURATIONS

Configuration Name	Type	Description
Windows Cert Auth Root CA Certificate	CERTIFICATE	This setting is used for (non-enrollment) server authentication by Windows devices.
Windows Computer-level Cert Auth CE Setting	CERTIFICATE	This setting is used for computer-level certificate authentication by Windows clients.
Windows Phone Enrollment SCEP	CERTIFICATE	This setting is an auto-created SCEP setting for the Windows Phone Enrollment CA.
Windows User-level Cert Auth CE Setting	CERTIFICATE	This setting is used for user-level certificate authentication by Windows clients.

Displaying configurations status

To see the status of configurations for each device:

1. Go to **Device & Users > Devices**
2. Select a device, and click the caret to open the device details

3. Click the **Configurations** tab.

The statuses you will see are:

- **Pending**: The process of applying the settings has been started.
- **Sent**: The settings have been successfully sent to the device.
- **Applied**: Core has confirmed that the verifiable settings appear to have been applied to the device.
- **Partially Applied**: One or more settings may have been rejected by the device. This can mean that the feature is not supported by the device.
- **Update Pending**: The administrator has edited the setting in the Admin Portal. The process of applying the updated setting has begun.

Adding new configurations

ⓘ Add new configurations for Windows devices through Exchange and Certificates only. Add new configurations for Windows 8.1 devices through Wi-Fi and VPN only.

To add new configurations:

1. Go to **Policies & Configs > Configurations**.
2. Click **Add New**.
3. Select the type of configuration you want to create.
4. Complete the displayed form for the configuration.
5. Click **Save**.
6. To push the configuration to devices, apply it to the appropriate labels. Select **Actions > Apply to Label**.

Editing configurations

ⓘ Add new configurations for Windows devices through Exchange and Certificates only. Add new configurations for Windows 8.1 devices through Wi-Fi and VPN only.

To edit configurations:

1. In the Configurations screen, select the configuration you want to edit.
2. Click **Edit**.
3. Make your changes.
4. Click **Save**.

   A pop-up displays.
5. Click **Yes** to continue.

   The configuration will be re-pushed to matching devices even you made no changes. However, if the only change made is to the description, the configuration will **not** be re-pushed to the devices.

Deleting configurations

Add new configurations for Windows devices through Exchange and Certificates only. Add new configurations for Windows 8.1 devices through Wi-Fi and VPN only.

To delete configurations:

1. In the Configurations screen, select the settings you want to delete.
2. Click **Delete**.

Exporting configurations

Export and importing setting configurations helps reduce errors when you have multiple instances of Core. You can export a configuration .json file for an existing setting, modify it, then import it to another configuration.

To export a configuration:

1. Select **Policies & Configs** > **Configurations**.

   All available configurations are listed in the table.

2. Select a single configuration to export.

   You can sort, as necessary, to find the configuration you want to export.

3. Click **Export** to create an export configuration .json file.

   No application-related information is captured when exporting a configuration.

4. Locate the .json file, open, modify, and save it, as necessary.

> Review this file before reusing it as values are not verified before importing them.

Importing configurations

To import a configuration:

1. Log into Core.
2. Select **Policies & Configs** > **Configurations**.
3. Click **Import** to locate a saved exported configuration .json file.
4. Enter the name of the file or click **Browse** to locate it.
5. Read the warning message and click in the **I Agree** check box.
6. Click **Import** to add the new configuration to the configuration table.

   If you import a configuration that already exists, you can override the file or cancel the import.

Applying configurations to labels

Use labels to apply configurations to devices. Refer to the “Using labels to establish groups” section in the*Getting Started with Core* for more information.

To apply a configuration to a label:

1. Select **Policies & Configs > Configurations** to display the configurations table with all available settings configurations.

2. Select the check box next to a configuration you want to apply to a label.

   Search for a configuration by entering the configuration name or description in the search box.

3. Click **Actions > Apply To Label**.

   Select the label.

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

5. Click **Apply**.

Exporting the devices in the WatchList

The number in the **WatchList** field indicates the number of devices for which the configuration is still in queue.

Procedure

1. In the Core Admin Portal, go to **Policies & Configs** > **Configurations**.

2. Click the number in the WatchList field for the configuration for which you want to export the WatchList.

   The Pending Devices window appears. The window displays a list of devices for which the configuration is queued.

3. Click Export to export the list of devices.

4. The list is downloaded as .CSV file.

Impact of changing LDAP server variables

A change to a LDAP server variable (such as $EMAIL$, $FIRST_NAME$, $LAST_NAME$, $DISPLAY_NAME$, $USER_UPN$, $USER_CUSTOM1, $USER_CUSTOM2, $USER_CUSTOM3$, or $USER_CUSTOM4$) now causes a setting that uses the variable to be re-pushed to the device. The impacted settings are:

- Exchange setting
- Email setting
- Wi-Fi setting

- VPN setting
- CalDAV setting
- CardDAV setting
- Subscribed calendar setting
- AppConnect app configuration
- Docs@Work setting

Configuring Email

This section addresses email account configuration, enabling S/MIME encryption and synchronizing account data.

- "Exchange settings" below
- "Synchronizing Google account data" on page 146

Exchange settings

To specify the settings for the ActiveSync server that devices use, go to **Policies & Configs > Configurations**, then click **Add New > Exchange**. The ActiveSync server can be a Microsoft Exchange server, an IBM® Lotus® Notes Traveler server, Microsoft Office 365, or another server.

The following table describes the Exchange settings you can specify.

TABLE 16. EXCHANGE SETTINGS

Section	Field Name	Description
General	Name	Enter brief text that identifies this group of Exchange settings.
	Description	Enter additional text that clarifies the purpose of this group of Exchange settings.
	Server Address	Enter the address of the ActiveSync server. If you are using Standalone Sentry, do the following: • Enter the Standalone Sentry's address. • If you are using Lotus Domino server 8.5.3.1 Upgrade Pack 1 for your ActiveSync server, set the server address to <***Standalone Sentry's fully qualified domain name***>/traveler.

TABLE 16. EXCHANGE SETTINGS (CONT.)

Section	Field Name	Description
		• If you are using a Lotus Domino server earlier than 8.5.3.1 Upgrade Pack 1, set the address to <***Standalone Sentry fully qualified domain name***>/servlet/traveler. • If you are using load balancers, contact Ivanti. Professional Services. When using Integrated Sentry, set the server address to Microsoft Exchange Server's address. ⓘ When using Sentry, you can do preliminary verification of your Exchange configuration choices for the ActiveSync User Name, ActiveSync User Email, and ActiveSync Password fields. To do so, first set the server address to the ActiveSync server. After you have verified that users can access their email using this Exchange configuration, change the server address to the appropriate Sentry address. For more information about configuring Sentry, see the Sentry Guide for Core.
	Use SSL	Select to use secure connections.
	Use alternate device handling	Replaces the **Use Standalone Sentry** option. Use this option only under the direction of Ivanti Technical Support.
	Domain	Specify the domain configured for the server.
	Google Apps Password	This check box only appears if you have configured a Google account with Core. When linking to Google Apps, select this option to use the Google Apps password to log in to the Google account you have configured to work with Core. This password allows device users to access their Email, Contacts, and Calendar data on their managed devices.

TABLE 16. EXCHANGE SETTINGS (CONT.)

Section	Field Name	Description
		When selected, Core grays out the **ActiveSync User Name** and **ActiveSync User Password**. This check box only appears if you have configured a Google account with Core, as described in "Synchronizing Google account data" on page 146.
	ActiveSync User Name	Specify the variable for the user name to be used with this Exchange configuration. You can specify any or all of the following variables $EMAIL$, $USERID$, $PASSWORD$. $MANAGED_APPLE_ID$ can be used for Shared iPad devices and User Enrolled devices only. You can also specify custom formats, such as $USERID$_US. Custom attribute variable substitutions are supported. Typically, you use $USERID$ if your ActiveSync server is a Microsoft Exchange Server, and you use $EMAIL$ if your ActiveSync server is an IBM Lotus Notes Traveler server. You cannot use $NULL$ for this field.
	ActiveSync User Email	Specify the variable for the email address to be used with this Exchange configuration. You can specify any or all of the following variables $USERID$, $EMAIL$,$SAM_ACCOUNT_NAME$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$, $CUSTOM_DEVICE_Attributename$, CUSTOM_USER_Attributename$, or $NULL$. $MANAGED_APPLE_ID$ can be used for Shared iPad devices and User Enrolled devices only. You can also specify custom formats, such as $USERID$_US. Custom attribute variable substitutions are supported. Typically, you use $EMAIL$ in this field; you cannot use $NULL$. **For Windows 10 devices: Use only $EMAIL$.**

TABLE 16. EXCHANGE SETTINGS (CONT.)

Section	Field Name	Description
	ActiveSync User Password	Specify the variable for the password to be used with this Exchange configuration. You can specify any or all of the following variables: $USERID$, $EMAIL$, $PASSWORD$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$, $CUSTOM_DEVICE_Attributename$, CUSTOM_USER_Attributename$, or $NULL$. You can also specify custom formats, such as $USERID$_US. Custom attribute variable substitutions are supported. Enter additional variables or text in the text box adjacent to the **Password** field. Entries in this text box are kept hidden and will not be visible to any Core administrator. ⓘ All variables and text up to the last valid variable will be visible. Anything after the last valid variable will not be visible. The valid variable may appear in either of the password fields. Valid variables are variables in the drop-down list.
	Identity Certificate	Select the Certificate Enrollment entry you created for supporting Exchange ActiveSync, if you are implementing certificate-based authentication.

TABLE 16. EXCHANGE SETTINGS (CONT.)

Section	Field Name	Description
		ⓘ When setting up email for devices with multi-user sign-in, the exchange profile must always use a user-based certificate. The user-based certificate will ensure secure access to email for all users. Using a device-based certificate can result in one user sending or receiving emails for another user. When configuring the user-based certificate, select the **Proxy enabled** and **Store certificate keys on MobileIron Core** options. This allows the user certificate and private key to be delivered each time they log in on the shared device.
	Password is also required	Specify whether to prompt device users for a password when certificate authentication is implemented. The password prompt is turned off by default. Once you specify an Identify Certificate, this option is enabled. Select the option if you want to retain the password prompt.
	Items to Synchronize (Android, Windows)	Select the Outlook items to be synchronized (Contacts, Calendar, Email, Tasks).
	Items to Synchronize (iOS)	This feature is not supported on Windows devices.
	Past Days of Email to Sync	Specify the maximum amount of email to synchronize each time by selecting an option from the drop-down list. The 1 Day option maps to the All option.
	Move/Forward Messages to Other Email Accounts	This feature is not supported for Windows devices.
S/MIME	Enable for Android and iOS 9.3.3 (or earlier)	Select to enable S/MIME signing and encryption on devices running Android or iOS 9.3.3 or earlier.

TABLE 16. EXCHANGE SETTINGS (CONT.)

Section	Field Name	Description
S/MIME Signing		
	S/MIME Signing: Enable	This feature is not supported for Windows devices.
	S/MIME Signing identity	This feature is not supported for Windows devices.
	Signing Identity: User Overrideable	This feature is not supported for Windows devices.
	S/MIME Signing: User Overrideable	This feature is not supported for Windows devices.
S/MIME Encryption		
	Encryption by Default	This feature is not supported for Windows devices.
	Encryption Identity	This feature is not supported for Windows devices.
	Encryption Identity: User Overrideable	This feature is not supported for Windows devices.
	Encryption by Default: User Overrideable	This feature is not supported for Windows devices.
	Per-Message Encryption Switch	This feature is not supported for Windows devices.
ActiveSync		
	Sync during	
	Peak Time	Select the preferred synchronization approach for peak times.
	Off-peak Time	Select the preferred synchronization approach for off-peak times.
	Use above settings when roaming	Specify whether to apply synchronization preferences while roaming.
	Send/receive when send	Specify whether queued messages should be sent and received whenever the user sends a message.

TABLE 16. EXCHANGE SETTINGS (CONT.)

Section	Field Name	Description
	Peak Time	
	Peak Days	Specify which days should be considered peak days.
	Start Time	Specify the beginning of the peak period for all peak days.
	End Time	Specify the end of the peak period for all peak days.
iOS 5 and Later Settings		These features are not supported for Windows devices.
Android		These features are not supported for Windows devices.
	Windows 10 Desktop	This feature is only supported for Windows 10 Desktop devices.
Windows 10 Desktop	Configure Outlook	Select this option to configure an email profile with the use of Microsoft's Outlook client, versions of 2010 or 2013. Outlook uses the Name, Server Address, Domain, ActiveSync User Name, ActiveSync User Email, and ActiveSync Password. All other settings are ignored. This is supported only on Outlook 2010 and 2013. Outlook 2016 and future versions require that Auto Discovery is configured on the Exchange server and does not need this configuration. ⓘ This feature requires Bridge. See "Setting up Bridge" on page 332 for details.

Configuring POP and IMAP email settings

This feature is not supported for Windows devices.

Synchronizing Google account data

You can synchronize email, contacts, calendar, and tasks with mail apps on devices managed by Core. To enable synchronization, you need to authorize apps to use Google APIs for communication between servers without accessing user information. This requires a service account that makes API calls on behalf of an app, as well as credentials that authenticate the identity of the app.

You create these credentials in the Google Developers Console, and then upload the credentials both to the Google Admin Console and Core. You can then configure an Exchange setting to synchronize Google email data (including email, contacts, calendar, and tasks) with managed devices. You can alternatively choose to synchronize only some email data, such as calendar and contacts only, or email alone.

The Exchange setting also allows you to control the Google Apps password through Core.

Main steps

Synchronizing Google Apps data involves the following main steps:

- "Using OAuth to enable access to Google APIs" on the next page
- "Uploading OAuth credentials to the Google Admin Console" on page 148
- "Linking Google Apps credentials with Core" on page 148
- "Setting up your Exchange setting for access to Google Apps data" on page 150
- "Renewing the Google Apps password for a given set of users" on page 152 (optional)

Before you begin

You need a Google administrator account.

Review the following Google documentation:

- Develop Admin Console solutions
- Credentials, access, security, and identity - API Console Help
- API Console Help > Service Accounts

Using OAuth to enable access to Google APIs

You must login to the Google Developers Console to enable access to Google APIs from clients using OAuth.

For detailed information, see the Google documentation here:

- Using OAuth 2.0 to Access Google APIs
- Using OAuth 2.0 for Server to Server Applications

Procedure

1. Login to https://console.developers.google.com
2. In the Google Developers Console, create a new project.
3. Enable the Admin SDK and/or APIs.
4. Create credentials for the OAuth 2.0 client.
5. Create a consent form.
6. Enter the relevant information, as shown in the following table.

Item	Description
Application type	Select web application.
Name	Enter the name of the iOS app.
Authorized JavaScript origins	Enter JavaScript origins here or redirect URIs below (or both). Cannot contain a wildcard (http://*.example.com) or a path (http://example.com/subdir).
Authorized redirect URIs	Must have a protocol. Cannot contain URL fragments or relative paths. Cannot be a public IP address.

7. Download the credentials in the form of a JSON file for the web client.

Uploading OAuth credentials to the Google Admin Console

You must now upload to the Google Admin Console the JSON file you created in "Using OAuth to enable access to Google APIs" on the previous page. The JSON files contains the credentials you created for client access.

For detailed information, see the Google documentation here:

- Using OAuth 2.0 to Access Google APIs
- Using OAuth 2.0 for Server to Server Applications

Procedure

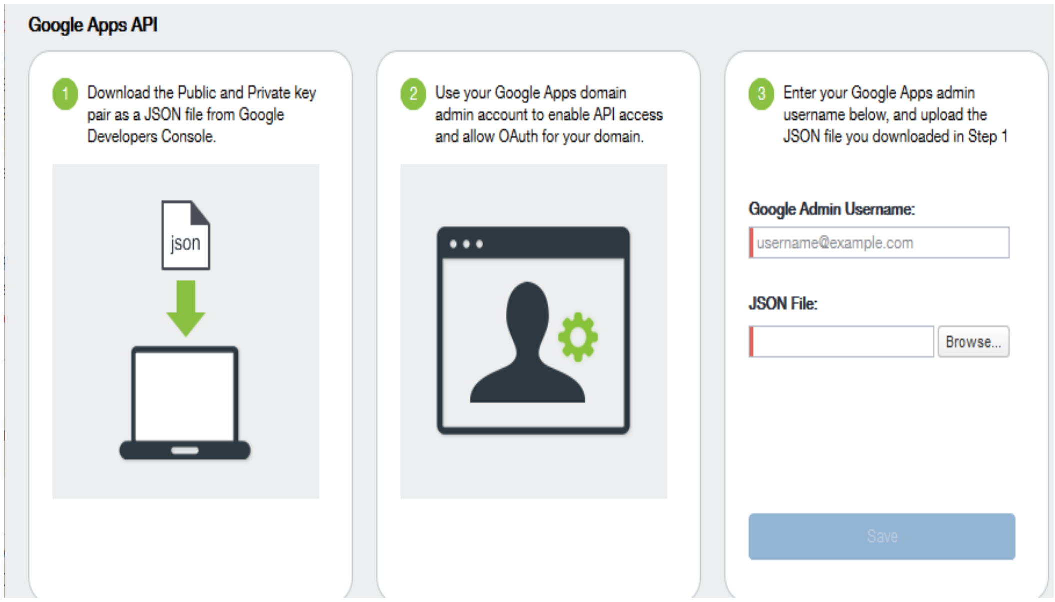
1. Go to https://admin.google.com and login with your administrator ID.
2. Enable API access.
3. Enter the client name and API scope.
4. Authorize the JSON file so that clients may access it.

Linking Google Apps credentials with Core

You must upload the JSON credentials file you downloaded from the Google Developers console to link your Google credentials with Core. For more information, see "Using OAuth to enable access to Google APIs" on the previous page.

Procedure

1. In the Admin Portal, go to **Services** > **Google**.
2. In the **Google Admin Username** field, enter your Google administrator email address.
3. Next to the **JSON File** field, click **Browse**.



Google Apps API

1 Download the Public and Private key pair as a JSON file from Google Developers Console.

2 Use your Google Apps domain admin account to enable API access and allow OAuth for your domain.

3 Enter your Google Apps admin username below, and upload the JSON file you downloaded in Step 1

4. Select the JSON file you downloaded from the Google Developers Console.

   a. Click **Save**.

      The results are displayed in the lower left of the page.

5. Go to **Settings** > **Preferences**.

6. Scroll down to the **Google Apps API** section.

7. Click **Password Settings**.

8. Configure password settings as follows:

   - Password length must be: Enter the minimum password length.

   - Require a password change every: Check the box and enter the number of days after which device users must change their password.

   > Password expiration and password length values should match whatever is configured in Google. For example, if you configured a 90 day expiration period in Google with a password length of 8 to 90, then you would configure the same expiration and password length values in Core.

9. Click **Save**.

10. Optionally, view the Google Apps account status by clicking **View Account**.

Setting up your Exchange setting for access to Google Apps data

Create an Exchange setting to connect Core to Google servers, such that device users will be able to access their email, calendar, and contacts. Apply the Exchange setting to the relevant labels, such that Core pushes the new setting to the correct devices. The Exchange setting must include the Google Apps Password flag, which tells Core to generate a Google Apps password and send it to Google servers.

When sending an event to a device, Core checks whether the Google Apps Password flag is toggled on or off. If a Google Apps password is required, but the password has not yet been generated and sent to Google, then Core sends the password to Google first before sending the Exchange setting to the device.

If Core cannot find a user on Google, Core logs an error, and does not push the Exchange setting again.

Under some circumstances, you may need to renew the Google Apps password. For more information, see "Renewing the Google Apps password for a given set of users" on page 152.

Note the following:

- If you intend to distribute an AppConnect email app to devices, such as Email+ for iOS, you must add the key email_password with a value of $GOOGLE_AUTOGEN_PASSWORD$ to the AppConnect app configuration for the email app. For more information, see "Configuring an AppConnect app configuration" in the *AppConnect Guide for Core*.

- Set the Exchange Username field to $EMAIL$ when using $GOOGLE_AUTOGEN_PASSWORD$ in the Password field and when using Android Enterprise managed configurations or AppConnect KVPs.

Procedure

1. In the Admin Portal go to **Policies & Configs > Configurations**.

2. Click **Add New > Exchange**.

3. In the Exchange Setting dialog box, enter the following:

Item	Description
General	
Name	Enter brief text that identifies this group of Exchange settings.
Description	Enter additional text that clarifies the purpose of this group of Exchange settings.
Server Address	Enter the address of the mail server, such as **m.google.com**. If you are using Standalone Sentry, do the following: • Enter the address of Standalone Sentry. • Go to **Services > Sentry** and edit your Standalone Sentry. In the **ActiveSync Server** field, enter **m.google.com**. • If you are using load balancers, contact Ivanti Professional Services. For more information about configuring Sentry, see the *Sentry Guide for Core*.
Use SSL	Select to use secure connections. ⓘ You must use SSL to link to Google Apps.
Google Apps Password	When linking to Google Apps, select this option to use the Google Apps password to log in to the Google account you have configured to work with Core. This password allows device users to access their mail, contacts, and calendar data on their managed devices. When selected, Core grays out the **ActiveSync User Name** and **ActiveSync User Password**. This check box only appears if you have configured a Google account with Core, as described in "Synchronizing Google account data" on page 146.

Item	Description
ActiveSync User Email	Specify the variable for the email address to be used with this Exchange configuration. You can specify any or all of the following variables $EMAIL$, $USERID$, $PASSWORD$. $MANAGED_APPLE_ID$ can be used for Shared iPad devices and User Enrolled devices only. You can also specify custom formats, such as $USERID$_US. Custom attribute variable substitutions are supported. Typically, you use $EMAIL$ in this field.
Items to Synchronize	Select the items you want to synchronize with Google Apps: Contacts, Calendar, Email, Tasks.

4. Click **Save**.

5. Check the box next to the Exchange setting you created, and select **Actions** > **Apply To Label**.

6. Select the labels to which you want to apply the Exchange setting and click **Apply**.

Renewing the Google Apps password for a given set of users

If there is a communication error when sending a Google Apps password to Google, Core. Core tracks the number of attempts to send updated passwords to Google. If it reaches the preset maximum number of attempts to contact Google servers, Core stops trying and the password is set to failure state. At this point, you must manually renew the Google Apps password.

You can renew the Google password for an individual user or a set of users on the Users page in the Core Admin Portal. After you generate it, Core pushes the new password to Google when the device checks in.

Procedure

1. Go to **Devices & Users** > **Users**.

2. Select the user or users whose Google password you want to renew.

3. Select **Actions > Renew Google Apps Password**.

   The Admin Portal shows a dialog that lists the users whose Google Apps password you want to renew.

4. Click **Renew Google Apps Password**.

   The Admin Portal sends the request to renew the Google Apps password for the selected users.

5. Click **Close**.

Managing Wi-Fi Settings

This section addresses the Wi-Fi settings.

- "Wi-Fi settings" below
- "Wi-Fi profiles and password caching" below
- "Wi-Fi authentication types" below

Wi-Fi settings

To configure wireless network access, in the Admin Console, go to **Policies & Configs > Configurations.** Click **Add New > Wi-Fi** to create a new configuration.

Do not assign multiple Wi-Fi profiles to a device if the Network Name SSID (Service Set Identifier) differs only by case. For example, if one profile has an SSID value of "yourco" and another has an SSID of "YourCo," those two must not be assigned to the same device. Doing so will cause check-in problems, and full device details will not be properly recorded.

Wi-Fi profiles and password caching

To make deployments easier, Core offers the option of caching a user’s Wi-Fi password. This option is turned off by default. Cached passwords are encrypted, stored on Core, and used only for authentication. Note that the password must match the LDAP password in order for this feature to be of use.

Wi-Fi authentication types

The fields that appear in the **New Wi-Fi Setting** dialog change based on values selected. The following tables describe the fields required **for each selection in the Authentication field**:

- "Open authentication" on the next page

- "Shared authentication" on page 158
- "WPA Enterprise authentication" on page 162
- "WPA2 / WPA3 Enterprise authentication" on page 164
- "WPA Personal authentication" on page 167
- "WPA2 / WPA3 Personal authentication" on page 170
- "Supported variables for Wi-Fi authentication" on page 171

Open authentication

Open authentication allows any device to authenticate and then attempt to communicate with the access point. Using open authentication, any wireless device can authenticate with the access point, but the device can communicate only if its Wired Equivalent Privacy (WEP) keys match the access point's WEP keys.

Use the following guidelines to set up Open authentication.

TABLE 17. WI-FI OPEN AUTHENTICATION FIELD DESCRIPTIONS

Item	Description
Name	Enter the name to use to reference this configuration in Core.
Network Name (SSID)	Enter the name (i.e., service set identifier) of the Wi-Fi network these settings apply to. This field is case sensitive. If the profile name and SSID are different, Windows devices will not connect to Wi-Fi.
Description	Enter additional text to clarify the purpose of this group of Wi-Fi settings.
Hidden Network	Select this option if the SSID is not broadcast.
Authentication	Select Open.
Data Encryption	Select the data encryption method associated with the selected authentication type. The selection affects which of the following fields are displayed. For Open authentication, the following encryption options are available: • Disabled

TABLE 17. WI-FI OPEN AUTHENTICATION FIELD DESCRIPTIONS (CONT.)

Item	Description
	• WEP • WEP Enterprise
Network Key	WEP encryption Enter the network key necessary for accessing this network. The network key should be 5 or 13 ASCII characters or 10 or 26 hexadecimal digits.
Key Index	WEP encryption If using multiple network keys, select a number indicating the memory position of the correct encryption key.
Confirm Network Key	Re-enter the network key to confirm.
User Name	WEP Enterprise encryption Specify the variable to use as the user name when establishing the Wi-Fi connection. See "Supported variables for Wi-Fi authentication" on page 171
Password	WEP Enterprise encryption Specify the variable to use and any necessary custom formatting for the Wi-Fi password. The default variable selected is $PASSWORD$. Enter additional variables or text in the text box adjacent to the Password field. Entries in this text box are kept hidden and will not be visible to any Core administrator. Note the following: • If you specify $PASSWORD$, also enable **Save User Password** under **Settings > System Settings > Users & Devices > Registration**. • All variables and text up to the last valid variable will be visible. Anything after the last valid variable will not be visible. The valid variable may appear in either of the password fields. See "Supported variables for Wi-Fi authentication" on page 171.

TABLE 17. WI-FI OPEN AUTHENTICATION FIELD DESCRIPTIONS (CONT.)

Item	Description
Apply to Certificates	WEP Enterprise encryption Configure this field with the CA certificate needed to validate the Identity Certificate presented by the Wi-Fi Access Point. It is not the CA certificate needed to validate the Identity Certificate sent to the device in the Wi-Fi config.
Trusted Certificate Names	WEP Enterprise encryption. If you did not specify trusted certificates in the Apply to Certificates list, then enter the names of the authentication servers to be trusted. You can specify a particular server, such as server.mycompany.com or a partial name such as *.mycompany.com.
Allow Trust Exceptions	WEP Enterprise encryption. Select this option to let users decide to trust a server when the chain of trust can’t be established. To avoid these prompts, and to permit connections only to trusted services, turn off this option and upload all necessary certificates.
Use Per-connection Password	WEP Enterprise encryption. Select this option to prompt the user to enter a password each time the device connects to the Wi-Fi network.
EAP Type	Select the authentication protocol used: • EAP-FAST • EAP-SIM • LEAP • PEAP • TLS • TTLS **If you select EAP-FAST,** then you also need to specify the Protected Access Credential (PAC). **If you select TLS,** then you must specify an Identity Certificate. **If you select TTLS,** then you must also specify the Inner Identity Authentication Protocol. You may optionally specify an Outer Identity

TABLE 17. WI-FI OPEN AUTHENTICATION FIELD DESCRIPTIONS (CONT.)

Item	Description
Connects To	Select Internet or Work.
Apple Settings	These features are not supported on Windows devices.
Windows Settings	These features are not supported on Windows devices.
Proxy Type	Specifies whether a proxy is configured and which type is configured. Available types are **Manual** and **Auto**. ⓘ The **Auto** type is only available for Windows 10 Mobile devices.
PAC URL	Specifies the URL for the proxy auto-configuration (PAC) file. This option is only available after selecting **Auto**.
Proxy Host	Specifies the proxy host. This option is only available after selecting **Manual**.
Proxy Port	Specifies the proxy port. This option is only available after selecting **Manual**.

Related topics

- "Shared authentication" below
- "WPA Enterprise authentication" on page 162
- "WPA2 / WPA3 Enterprise authentication" on page 164
- "WPA Personal authentication" on page 167
- "WPA2 / WPA3 Personal authentication" on page 170
- "Supported variables for Wi-Fi authentication" on page 171

Shared authentication

Shared Key Authentication (SKA) is a process by which a computer can gain access to a wireless network that uses the Wired Equivalent Privacy (WEP) protocol. With SKA, a computer equipped with a wireless modem can fully access any WEP network and exchange encrypted or unencrypted data.

Use the following guidelines to set up shared authentication:

TABLE 18. WI-FI SHARED AUTHENTICATION FIELD DESCRIPTIONS

Item	Description
Name	Enter the name to use to reference this configuration in Core.
Network Name (SSID)	Enter the name (i.e., service set identifier) of the Wi-Fi network these settings apply to. This field is case sensitive. If the profile name and SSID are different, Windows devices will not connect to Wi-Fi.
Description	Enter additional text to clarify the purpose of this group of Wi-Fi settings.
Hidden Network	Select this option if the SSID is not broadcast.
Authentication	Select Shared.
Data Encryption	Select the data encryption method associated with the selected authentication type. The selection affects which of the following fields are displayed. For Shared authentication, the following encryption options are available: • Disabled • WEP • WEP Enterprise
Network Key	WEP encryption Enter the network key necessary for accessing this network. The network key should be 5 or 13 ASCII characters or 10 or 26 hexadecimal digits.
Key Index	WEP encryption If using multiple network keys, select a number indicating the memory position of the correct encryption key.
Confirm Network Key	Re-enter the network key to confirm.
User Name	WEP Enterprise encryption Specify the variable to use as the user name when establishing the Wi-Fi connection. See "Supported variables for Wi-Fi authentication" on page 171.

TABLE 18. WI-FI SHARED AUTHENTICATION FIELD DESCRIPTIONS (CONT.)

Item	Description
Password	WEP Enterprise encryption Specify the variable to use and any necessary custom formatting for the Wi-Fi password. The default variable selected is $PASSWORD$. Enter additional variables or text in the text box adjacent to the Password field. Entries in this text box are kept hidden and will not be visible to any Core administrator. Note the following: • If you specify $PASSWORD$, also enable **Save User Password** under **Settings > System Settings > Users & Devices > Registration**. • All variables and text up to the last valid variable will be visible. Anything after the last valid variable will not be visible. The valid variable may appear in either of the password fields. See "Supported variables for Wi-Fi authentication" on page 171.
Apply to Certificates	WEP Enterprise encryption Configure this field with the CA certificate needed to validate the Identity Certificate presented by the Wi-Fi Access Point. It is **not** the CA certificate needed to validate the Identity Certificate sent to the device in the Wi-Fi config.
Trusted Certificate Names	WEP Enterprise encryption. If you did not specify trusted certificates in the Apply to Certificates list, then enter the names of the authentication servers to be trusted. You can specify a particular server, such as server.mycompany.com or a partial name such as *.mycompany.com.
Allow Trust Exceptions	WEP Enterprise encryption. Select this option to let users decide to trust a server when the chain of trust can’t be established. To avoid these prompts, and to permit connections only to trusted services, turn off this option and upload all necessary certificates.
Use Per-connection Password	WEP Enterprise encryption. Select this option to prompt the user to enter a password each time the device connects to the Wi-Fi network.

TABLE 18. WI-FI SHARED AUTHENTICATION FIELD DESCRIPTIONS (CONT.)

Item	Description
EAP Type	Select the authentication protocol used: • EAP-FAST • EAP-SIM • LEAP • PEAP • TLS • TTLS **If you select EAP-FAST,** then you also need to specify the Protected Access Credential (PAC). **If you select TLS,** then you must specify an Identity Certificate. **If you select TTLS,** then you must also specify the Inner Identity Authentication Protocol. You may optionally specify an Outer Identity.
Connects To	Select Internet or Work.
Apple Settings	These features are not supported on Windows devices.

Related topics

- "Open authentication" on page 155
- "WPA Enterprise authentication" on the next page
- "WPA2 / WPA3 Enterprise authentication" on page 164
- "WPA Personal authentication" on page 167
- "WPA2 / WPA3 Personal authentication" on page 170
- "Supported variables for Wi-Fi authentication" on page 171

WPA Enterprise authentication

Wi-Fi Protected Access-Enterprise (WPA-Enterprise) is a wireless security mechanism designed for small to large enterprise wireless networks. It is an enhancement to the WPA security protocol with advanced authentication and encryption.

Use the following guidelines to set up WPA Enterprise authentication:

TABLE 19. WI-FI WPA ENTERPRISE AUTHENTICATION FIELD DESCRIPTIONS

Item	Description
Name	Enter the name to use to reference this configuration in Core.
Network Name (SSID)	Enter the name (i.e., service set identifier) of the Wi-Fi network these settings apply to. This field is case sensitive. If the profile name and SSID are different, Windows devices will not connect to Wi-Fi.
Description	Enter additional text to clarify the purpose of this group of Wi-Fi settings.
Hidden Network	Select this option if the SSID is not broadcast.
Authentication	Select WPA Enterprise.
Data Encryption	Select the data encryption method associated with the selected authentication type. For WPA Enterprise authentication, the following encryption options are available: • AES • TKIP
User Name	Specify the variable to use as the user name when establishing the Wi-Fi connection. See "Supported variables for Wi-Fi authentication" on page 171
Password	Specify the variable to use and any necessary custom formatting for the Wi-Fi password. The default variable selected is $PASSWORD$. Enter additional variables or text in the text box adjacent to the Password field. Entries in this text box are kept hidden and will not be visible to any Core administrator.

TABLE 19. WI-FI WPA ENTERPRISE AUTHENTICATION FIELD DESCRIPTIONS (CONT.)

Item	Description
	ⓘ If you specify $PASSWORD$, also enable Save User Password under **Settings > System Settings > Users & Devices > Registration**. ⓘ All variables and text up to the last valid variable will be visible. Anything after the last valid variable will not be visible. The valid variable may appear in either of the password fields. See "Supported variables for Wi-Fi authentication" on page 171
Apply to Certificates	Configure this field with the CA certificate needed to validate the Identity Certificate presented by the Wi-Fi Access Point. It is **not** the CA certificate needed to validate the Identity Certificate sent to the device in the Wi-Fi configuration.
Trusted Certificate Names	If you did not specify trusted certificates in the Apply to Certificates list, then enter the names of the authentication servers to be trusted. You can specify a particular server, such as server.mycompany.com or a partial name such as *.mycompany.com.
Allow Trust Exceptions	Select this option to let users decide to trust a server when the chain of trust can't be established. To avoid these prompts, and to permit connections only to trusted services, turn off this option and upload all necessary certificates.
Use Per-connection Password	Select this option to prompt the user to enter a password each time the device connects to the Wi-Fi network.
EAP Type	Select the authentication protocol used: • EAP-FAST • EAP-SIM • LEAP • PEAP • TLS • TTLS

TABLE 19. WI-FI WPA ENTERPRISE AUTHENTICATION FIELD DESCRIPTIONS (CONT.)

Item	Description
	If you select EAP-FAST, then you also need to specify the Protected Access Credential (PAC). **If you select TLS,** then you must specify an Identity Certificate. **If you select TTLS,** then you must also specify the Inner Identity Authentication Protocol. You may optionally specify an Outer Identity.
Connects To	Select Internet or Work.
Apple Settings	These features are not supported on Windows devices.

Related topics

- "Open authentication" on page 155
- "Shared authentication" on page 158
- "WPA2 / WPA3 Enterprise authentication" below
- "WPA Personal authentication" on page 167
- "WPA2 / WPA3 Personal authentication" on page 170
- "Supported variables for Wi-Fi authentication" on page 171

WPA2 / WPA3 Enterprise authentication

WPA-Enterprise uses TKIP with RC4 encryption, while WPA2-Enterprise adds AES encryption. WPA3 uses Simultaneous Authentication of Equals (SAE) to provide stronger defenses against password guessing. SAE is a secure key establishment protocol. WPA3-Enterprise provides additional protections for networks transmitting sensitive data by offering the equivalent of 192-bit cryptographic strength.

Use the following guidelines to configure WPA2 or WPA3 Enterprise authentication.

Except for Apple TV, WPA2 Enterprise is applicable to iOS 8.0 or supported newer versions.

WPA3 Enterprise is applicable to iOS 13.0 or supported newer versions.

TABLE 20. WI-FI WPA2 / WPA3 ENTERPRISE AUTHENTICATION FIELD DESCRIPTION

Item	Description
Network Name (SSID)	Enter the name (i.e., service set identifier) of the Wi-Fi network these settings apply to. This field is case sensitive. If the profile name and SSID are different, Windows devices will not connect to Wi-Fi.
Description	Enter additional text to clarify the purpose of this group of Wi-Fi settings.
Hidden Network	Select this option if the SSID is not broadcast.
Authentication	Select one: • WPA2 Enterprise • WPA2 Enterprise (iOS 8 or later except Apple TV) • WPA3 Enterprise (iOS 13 or later)
Data Encryption	Select the data encryption method associated with the selected authentication type. For WPA2 Enterprise authentication, the following encryption options are available: • AES • TKIP
User Name	Specify the variable to use as the user name when establishing the Wi-Fi connection. See "WPA2 / WPA3 Enterprise authentication" on the previous page.
Password	Specify the variable to use and any necessary custom formatting for the Wi-Fi password. The default variable selected is $PASSWORD$. Enter additional variables or text in the text box adjacent to the Password field. Entries in this text box are kept hidden and will not be visible to any Core administrator. If you specify $PASSWORD$, also enable **Save User Password** under **Settings > System Settings > Users & Devices > Registration**.

TABLE 20. WI-FI WPA2 / WPA3 ENTERPRISE AUTHENTICATION FIELD DESCRIPTION (CONT.)

Item	Description
	All variables and text up to the last valid variable will be visible. Anything after the last valid variable will not be visible. The valid variable may appear in either of the password fields. Valid variables are variables in the drop-down list.
Apply to Certificates	Configure this field with the CA certificate needed to validate the Identity Certificate presented by the Wi-Fi Access Point. It is **not** the CA certificate needed to validate the Identity Certificate sent to the device in the Wi-Fi configuration.
Trusted Certificate Names	If you did not specify trusted certificates in the Apply to Certificates list, then enter the names of the authentication servers to be trusted. You can specify a particular server, such as server.mycompany.com or a partial name such as *.mycompany.com.
Allow Trust Exceptions	Select this option to let users decide to trust a server when the chain of trust can’t be established. To avoid these prompts, and to permit connections only to trusted services, turn off this option and upload all necessary certificates.
Use Per-connection Password	Select this option to prompt the user to enter a password each time the device connects to the Wi-Fi network.
EAP Type	Select the authentication protocol used: • EAP-FAST • EAP-SIM • LEAP • PEAP • TLS • TTLS **If you select EAP-FAST,** then you also need to specify the Protected Access Credential (PAC). **If you select TLS,** then you must specify an Identity Certificate.

TABLE 20. WI-FI WPA2 / WPA3 ENTERPRISE AUTHENTICATION FIELD DESCRIPTION (CONT.)

Item	Description
	If you select TTLS, then you must also specify the Inner Identity Authentication Protocol. You may optionally specify an Outer Identity.
Connects To	Select Internet or Work.
Apple Settings	These features are not supported on Windows devices.

Related topics

- "Open authentication" on page 155
- "Shared authentication" on page 158
- "WPA Enterprise authentication" on page 162
- "WPA Personal authentication" below
- "WPA2 / WPA3 Personal authentication" on page 170
- "Supported variables for Wi-Fi authentication" on page 171

WPA Personal authentication

WPA-Personal, also referred to as WPA-PSK (pre-shared key) mode, is designed for home and small office networks and doesn't require an authentication server. Each wireless network device encrypts the network traffic by deriving its 128-bit encryption key from a 256-bit shared key.

Use the following guidelines to configure WPA Personal authentication.

TABLE 21. WI-FI WPA PERSONAL AUTHENTICATION FIELD DESCRIPTIONS

Item	Description
Name	Enter the name to use to reference this configuration in Core.
Network Name (SSID)	Enter the name (i.e., service set identifier) of the Wi-Fi network these settings apply to. This field is case sensitive. If the profile name and SSID are different, Windows devices will not connect to Wi-Fi.

TABLE 21. WI-FI WPA PERSONAL AUTHENTICATION FIELD DESCRIPTIONS (CONT.)

Item	Description
Description	Enter additional text to clarify the purpose of this group of Wi-Fi settings.
Hidden Network	Select this option if the SSID is not broadcast.
Authentication	Select WPA Personal.
Data Encryption	Select the data encryption method associated with the selected authentication type. For WPA Personal authentication, the following encryption options are available: • AES • TKIP
Network Key	Enter the network key necessary for accessing this network. The key should be at least 8 characters long.
Confirm Network Key	Re-enter the network key to confirm.
EAP Type	Not applicable.
Connects To	Select Internet or Work.
Apple Settings	These features are not supported on Windows devices.

WPA2 Personal authentication

Use the following guidelines to configure WPA2 Personal authentication.

TABLE 22. WI-FI WPA2 PERSONAL AUTHENTICATION FIELD DESCRIPTIONS

Item	Description
Name	Enter the name to use to reference this configuration in Core.
Network Name (SSID)	Enter the name (i.e., service set identifier) of the Wi-Fi network these settings apply to. This field is case sensitive. If the profile name and SSID are different, Windows devices will not connect to Wi-Fi.

TABLE 22. WI-FI WPA2 PERSONAL AUTHENTICATION FIELD DESCRIPTIONS (CONT.)

Item	Description
Description	Enter additional text to clarify the purpose of this group of Wi-Fi settings.
Hidden Network	Select this option if the SSID is not broadcast.
Authentication	Select WPA2 Personal.
Data Encryption	Select the data encryption method associated with the selected authentication type. For WPA Personal authentication, the following encryption options are available: • AES • TKIP
Network Key	Enter the network key necessary for accessing this network. The key should be at least 8 characters long.
Confirm Network Key	Re-enter the network key to confirm.
EAP Type	Not applicable.
Connects To	Select Internet or Work.
iOS Settings	These features are not supported on Windows devices.

Related topics

- "Open authentication" on page 155
- "Shared authentication" on page 158
- "WPA Enterprise authentication" on page 162
- "WPA2 / WPA3 Enterprise authentication" on page 164
- "WPA2 / WPA3 Personal authentication" on the next page
- "Supported variables for Wi-Fi authentication" on page 171

WPA2 / WPA3 Personal authentication

WPA2 is currently the most secure standard utilizing AES (Advanced Encryption Standard) and a pre-shared key for authentication. WPA2 is backwards compatible with TKIP to allow interoperability with legacy devices. WPA3 Personal is available as a setting in the local browser user interface (UI). This personal authentication option is a more secure option than WPA2.

Use the following guidelines to configure WPA2 or WPA3 Personal authentication.

WPA3 Personal is applicable to iOS 13.0 or supported newer versions.

TABLE 23. WI-FI WPA2 / WPA3 PERSONAL AUTHENTICATION FIELD DESCRIPTIONS

Item	Description
Name	Enter the name to use to reference this configuration in Core.
Network Name (SSID)	Enter the name (i.e., service set identifier) of the Wi-Fi network these settings apply to. This field is case sensitive. If the profile name and SSID are different, Windows devices will not connect to Wi-Fi.
Description	Enter additional text to clarify the purpose of this group of Wi-Fi settings.
Hidden Network	Select this option if the SSID is not broadcast.
Authentication	Select one: • WPA2 Personal • WPA3 Personal (iOS 13 or later)
Data Encryption	Select the data encryption method associated with the selected authentication type. For WPA Personal authentication, the following encryption options are available: • AES • TKIP
Network Key	Enter the network key necessary for accessing this network. The key should be at least 8 characters long.

TABLE 23. WI-FI WPA2 / WPA3 PERSONAL AUTHENTICATION FIELD DESCRIPTIONS (CONT.)

Item	Description
Confirm Network Key	Re-enter the network key to confirm.
EAP Type	Not applicable.
Connects To	Select Internet or Work.
Apple Settings	These features are not supported on Windows devices.

Related topics

- "Open authentication" on page 155
- "Shared authentication" on page 158
- "WPA Enterprise authentication" on page 162
- "WPA2 / WPA3 Enterprise authentication" on page 164
- "WPA Personal authentication" on page 167
- "Supported variables for Wi-Fi authentication" below

Supported variables for Wi-Fi authentication

You can use the following variables in fields that support variables.

- $PASSWORD$ (only supported in the password field)
- $EMAIL$
- $USERID$
- $DEVICE_MAC$
- $NULL$
- $USER_CUSTOM1$... $USER_CUSTOM4$ (custom fields defined for LDAP)

Custom attribute variable substitutions are supported.

Related topics

- "Open authentication" on page 155
- "Shared authentication" on page 158
- "WPA Personal authentication" on page 167
- "WPA2 / WPA3 Personal authentication" on page 170
- "WPA Enterprise authentication" on page 162
- "WPA2 / WPA3 Enterprise authentication" on page 164

Managing VPN Settings

This section addresses the VPN settings. If you do not see information for the relevant VPN setting, check the *Core Device Management Guide* of the relevant OS.

- "Palo Alto Networks GlobalProtect" on page 220
- "PPTP" on page 220
- "Pulse Secure SSL" on page 226
- "Samsung Knox IPsec" on page 233
- "SonicWall Mobile Connect" on page 233
- "Custom SSL" on page 243
- "Application-triggered VPN for Windows devices" on page 243

VPN settings overview

This feature is supported for Cisco’s AnyConnect VPN client on Windows devices.

VPN is a technology that creates a secure network connection over a public network. A mobile device uses a VPN client to securely access protected corporate networks.

To use VPN:

- On the device, the user installs a VPN client app.
- Define a VPN setting in Core.
- Apply labels to the VPN setting so that the VPN setting is sent to the appropriate devices.
- Depending on the type of VPN, additional set up steps may be required to complete the VPN configuration.

Apps@Work uses the VPN client and the VPN setting, based on defined VPN rules, to enable access to corporate networks.

Configuring new VPN settings

In the Admin Portal, go to **Policies & Configs > Configurations** and click **Add New > VPN** to configure VPN access.

For macOS only, select one of the following Channel options:

- **Device channel** - the configuration is effective for all users on a device. This is the typical option.
- **User channel** - the configuration is effective only for the currently registered user on a device.

The following sections describe the fields required for each selection in the Connect Type field. For Tunnel support for Android, select Tunnel (Android) in the Connection Type field.

About VPN settings for Windows devices

- The following VPN settings are supported for Windows devices:
  - Cisco Legacy AnyConnect
  - IKEv2
  - Juniper SSL
  - PPTP
  - Pulse Secure SSL
- The following VPN settings are expected to work, but are not included in product warranty as they have been tested for provisioning only, but not tested for connectivity with Windows devices:
  - F5 SSL
  - SonicWALL
- If you change the name of a VPN profile, it is pushed as a new profile to the device.
- Identity certificates with Microsoft SCEP are supported. A root or intermediate certificate from a trusted certificate authority (CA) is required, and you must set up Core to act as a SCEP reverse proxy.

Check Point Capsule

This VPN connection type is supported on iOS, macOS, and Windows devices only. It is not supported on Android devices

Use the following guidelines to configure the Check Point Capsule VPN connection type:

- "Proxy - None (default)" below
- "Proxy - Manual " on page 178
- "Proxy - Automatic" on page 180

Within these selections, you may make settings for:

- "Windows Configuration" on page 182
- "Custom Data" on page 183

Proxy - None (default)

Use the following guidelines to configure a Check Point Capsule VPN without a proxy.

TABLE 24. PROXY - NONE SETTINGS

Item	Description
Name	Enter a short phrase that identifies this VPN setting.
Description	Provide a description that clarifies the purpose of these settings.
Channel	For macOS only. Select one of the following distribution options: • Device channel - the configuration is effective for all users on a device. This is the typical option. • User channel - the configuration is effective only for the currently registered user on a device.
Connection Type	Select **Check Point Capsule**.
Server	Enter the IP address, hostname, or URL for the VPN server.
Proxy	**None** is the default setting. To configure a **Manual** or **Automatic** proxy, go to "Proxy - Manual " on page 178 or "Proxy - Automatic" on page 180.
Username	Specify the user name to use. The default value is $USERID$. Use this field to specify an alternate format, such as: $USERID$, $EMAIL$, $SAM_ACCOUNT_NAME$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$, $CUSTOM_DEVICE_Attributename$, $CUSTOM_USER_Attributename$, $NULL$ You can use combinations such as the following:

TABLE 24. PROXY - NONE SETTINGS (CONT.)

Item	Description
	- $USERID$:$EMAIL$ - $USERID$_$EMAIL$ Enter $NULL$ if you want the field presented to the user to be blank. Users will need to fill in the relevant username. ⓘ Some enterprises have a strong preference concerning which identifier is exposed.
User Authentication	Select the user authentication to use: - Password - see next row for information. - Certificate - If you select Certificate, select the identity certificate to be used as the account credential. If you select Certificate, and extended authentication (EAP) is not used, this certificate will be sent out for IKE client authentication. If extended authentication is used, this certificate can be used for EAP-TLS.
Password	Specify the password to use (required.) The default value is $PASSWORD$. Include at least one of the following variables: $USERID$, $EMAIL$, $PASSWORD$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$, $CUSTOM_DEVICE_Attributename$, $CUSTOM_USER_Attributename$, $NULL$ You can use combinations such as $EMAIL$:$PASSWORD$ Enter $NULL$ if you want the field presented to the user to be blank. Users will need to fill in the relevant password.
Send All Traffic	Select to send all traffic from the Windows device through the VPN gateway. When *Send All Traffic* is checked, all traffic is sent through the VPN gateway with the exception of traffic from the resources you enter in this table. When *Send All Traffic* is unchecked, only traffic from the resources you enter in this table is sent through the VPN gateway.

Continue to "Windows Configuration" on page 182.

Continue to "Custom Data" on page 183.

Proxy - Manual

If you select **Manual**, you must specify the proxy server, port number. and proxy domain information.

TABLE 25. PROXY - MANUAL SETTINGS

Item	Description
Name	Enter a short phrase that identifies this VPN setting.
Description	Provide a description that clarifies the purpose of these settings.
Channel	For macOS only. Select one of the following distribution options: • Device channel - the configuration is effective for all users on a device. This is the typical option. • User channel - the configuration is effective only for the currently registered user on a device.
Connection Type	Select **Check Point Capsule**.
Server	Enter the IP address, hostname, or URL for the VPN server.
Proxy	Select **Manual**. For an Automatic proxy, see "Proxy - Automatic" on page 180.
Proxy Server	Enter the name for the proxy server.
Proxy Server Port	Enter the port number for the proxy server. Type - Select **Static** or **Variable** for the type of authentication to be used for the proxy server.
Type	*Select Manual proxy to see this option.* Select **Static** or **Variable**.
Proxy Server User Name	If the authentication type is **Static**, enter the user name for the proxy server. If the authentication type is **Variable**, the default variable selected is $USERID$.
Proxy Server Password	If the authentication type is **Static**, enter the password for the proxy server. Confirm the password in the field below. If the authentication type is **Variable**, the default variable selected is $PASSWORD$.

TABLE 25. PROXY - MANUAL SETTINGS (CONT.)

Item	Description
Proxy Domains (iOS only)	This setting applies to iOS and macOS devices only.
Username	Specify the user name to use. The default value is $USERID$. Use this field to specify an alternate format, such as: $USERID$, $EMAIL$, $SAM_ACCOUNT_NAME$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$, $CUSTOM_DEVICE_Attributename$, $CUSTOM_USER_Attributename$, $NULL$ You can use combinations such as the following: • $USERID$:$EMAIL$ • $USERID$_$EMAIL$ Enter $NULL$ if you want the field presented to the user to be blank. Users will need to fill in the relevant username. ⓘ Some enterprises have a strong preference concerning which identifier is exposed.
User Authentication	Select the user authentication to use: • Password - see next row for information. • Certificate - If you select Certificate, select the identity certificate to be used as the account credential. If you select Certificate, and extended authentication (EAP) is not used, this certificate will be sent out for IKE client authentication. If extended authentication is used, this certificate can be used for EAP-TLS.
Password	Specify the password to use (required.) The default value is $PASSWORD$. Include at least one of the following variables: $USERID$, $EMAIL$, $PASSWORD$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$, $CUSTOM_DEVICE_Attributename$, $CUSTOM_USER_Attributename$, $NULL$ You can use combinations such as $EMAIL$:$PASSWORD$ Enter $NULL$ if you want the field presented to the user to be blank. Users will need to fill in the relevant password.

TABLE 25. PROXY - MANUAL SETTINGS (CONT.)

Item	Description
Send All Traffic	Select to send all traffic from the Windows device through the VPN gateway. When *Send All Traffic* is checked, all traffic is sent through the VPN gateway with the exception of traffic from the resources you enter in this table. When *Send All Traffic* is unchecked, only traffic from the resources you enter in this table is sent through the VPN gateway.

Continue to "Windows Configuration" on page 182.

Continue to "Custom Data" on page 183.

Proxy - Automatic

If you selected an Automatic proxy, you must specify the proxy server URL and proxy domain(s).

WARNING: For Windows 10 devices, please add the configuration and value for automatic proxy in the Custom Data Grid. Automatic proxy is not supported in Windows 8.1.

TABLE 26. PROXY - AUTOMATIC SETTINGS

Item	Description
Name	Enter a short phrase that identifies this VPN setting.
Description	Provide a description that clarifies the purpose of these settings.
Channel	For macOS only. Select one of the following distribution options: • Device channel - the configuration is effective for all users on a device. This is the typical option. • User channel - the configuration is effective only for the currently registered user on a device.
Connection Type	Select **Check Point Capsule**.
Server	Enter the IP address, hostname, or URL for the VPN server.
Proxy	Select **Automatic**. For a manual proxy, see "Proxy - Manual " on page 178

TABLE 26. PROXY - AUTOMATIC SETTINGS (CONT.)

Item	Description
Proxy Server URL	Enter the URL for the proxy server. Enter the URL of the location of the proxy auto-configuration file.
Proxy Domains (iOS only)	This setting applies to iOS and macOS devices only.
Username	Specify the user name to use (required.) The default value is $USERID$. Include at least one of the following variables: $USERID$, $EMAIL$, $SAM_ACCOUNT_NAME$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$, $CUSTOM_DEVICE_Attributename$, $CUSTOM_USER_Attributename$, $NULL$ You can use combinations such as the following: • $USERID$:$EMAIL$ • $USERID$_$EMAIL$ Enter $NULL$ if you want the field presented to the user to be blank. Users will need to fill in the relevant username.
User Authentication	Select the user authentication to use: • Password - see next row for information. • Certificate - If you select Certificate, select the identity certificate to be used as the account credential. If you select Certificate, and extended authentication (EAP) is not used, this certificate will be sent out for IKE client authentication. If extended authentication is used, this certificate can be used for EAP-TLS.
Password	Specify the password to use (required.) The default value is $PASSWORD$. Include at least one of the following variables: $USERID$, $EMAIL$, $PASSWORD$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$, $CUSTOM_DEVICE_Attributename$, $CUSTOM_USER_Attributename$, $NULL$ You can use combinations such as $EMAIL$:$PASSWORD$

TABLE 26. PROXY - AUTOMATIC SETTINGS (CONT.)

Item	Description
	Enter $NULL$ if you want the field presented to the user to be blank. Users will need to fill in the relevant password.
Send All Traffic	Select to send all traffic from the Windows device through the VPN gateway. When *Send All Traffic* is checked, all traffic is sent through the VPN gateway with the exception of traffic from the resources you enter in this table. When *Send All Traffic* is unchecked, only traffic from the resources you enter in this table is sent through the VPN gateway.

Continue to "Windows Configuration" below.

Continue to "Custom Data" on the next page.

Windows Configuration

Allowed Secured Resources (Windows Phone only)
Excluded Secured Resources (Windows Phone only)

See "Application-triggered VPN for Windows devices" on page 243 for information on how to configure these settings to set up application-triggered VPN for 8.0.1 devices.

TABLE 27. WINDOWS CONFIGURATIONS

Item	Description
Windows Configuration	Enter the secured resources (domains, IP ranges, or apps) used by the **Send All Traffic** option.
Always On	Select this option to keep the VPN on. **Lock Down** supersedes this option for Windows devices.
Lock Down	You cannot change the assigned settings unless 1) the **Lock Down** setting is removed from the profile and the new profile is pushed to the device or 2) the device is un-enrolled from Core. This option supersedes the **Always On** option.

Custom Data

- **Add+** - Click to add a new key / value pair.
- **Key / Value** - Enter the Key / value pairs necessary to configure the VPN setting. The app creator should provide the necessary key / value pairs.

Cisco AnyConnect (iOS only)

This VPN connection type is supported on iOS devices only. It is not supported on Android, macOS, and Windows devices.

Cisco Legacy AnyConnect

This VPN connection type is supported on iOS devices (up to version 12.0), macOS, Android, and Windows devices.

Cisco Legacy AnyConnect is a universal app that can be used with Samsung Knox or with any Android device. This app can be used for all VPN modes:

- per-app inside the Knox container
- per-app outside the Knox container
- per-container (Knox)
- per-device (Knox)
- per-device (Android)

Use the following guidelines to configure Cisco Legacy AnyConnect VPN.

- "Proxy - None (default)" on the next page
- "Proxy - Manual " on page 185
- "Proxy - Automatic" on page 188

Within these selections, you may make settings for:

- "Windows Configuration" on page 190
- "Custom Data" on page 190 (does not apply to Android devices)

Proxy - None (default)

Use the following guidelines to configure a Cisco Legacy AnyConnect VPN without a proxy.

TABLE 28. PROXY - NONE SETTINGS

Item	Description
Name	Enter a short phrase that identifies this VPN setting.
Description	Provide a description that clarifies the purpose of these settings.
Channel	For macOS only. Select one of the following distribution options: • Device channel - the configuration is effective for all users on a device. This is the typical option. • User channel - the configuration is effective only for the currently registered user on a device.
Connection Type	Select **Cisco Legacy AnyConnect**.
Samsung Knox	This setting applies to Android devices only.
Deploy inside Knox Workspace	This setting applies to Android devices only.
Server	Enter the IP address, hostname, or URL for the VPN server.
Proxy	**None** is the default setting. To configure a **Manual** or **Automatic** proxy, go to "Proxy - Manual " on the next page or "Proxy - Automatic" on page 188.
Username	Specify the user name to use. The default value is $USERID$. Use this field to specify an alternate format, such as: $USERID$, $EMAIL$, $SAM_ACCOUNT_NAME$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$, $CUSTOM_DEVICE_Attributename$, $CUSTOM_USER_Attributename$, $NULL$ You can use combinations such as the following: • $USERID$:$EMAIL$ • $USERID$_$EMAIL$ Enter $NULL$ if you want the field presented to the user to be blank. Users will need to fill in the relevant username.

TABLE 28. PROXY - NONE SETTINGS (CONT.)

Item	Description
	ⓘ Some enterprises have a strong preference concerning which identifier is exposed.
User Authentication	Select the user authentication to use: • Password - see next row for information. • Certificate - If you select Certificate, select the identity certificate to be used as the account credential. If you select Certificate, and extended authentication (EAP) is not used, this certificate will be sent out for IKE client authentication. If extended authentication is used, this certificate can be used for EAP-TLS.
Password	Specify the password to use (required.) The default value is $PASSWORD$. Include at least one of the following variables: $USERID$, $EMAIL$, $PASSWORD$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$, $CUSTOM_DEVICE_Attributename$, $CUSTOM_USER_Attributename$, $NULL$ You can use combinations such as $EMAIL$:$PASSWORD$ Enter $NULL$ if you want the field presented to the user to be blank. Users will need to fill in the relevant password.
Group Name	Specify the name of the group to use.
VPN On Demand	This setting does not apply to Windows devices.
Per-App VPN	This setting applies to iOS and macOS devices only.
Provider Type	This setting applies to iOS and macOS devices only.

Continue to "Windows Configuration" on page 190.

Continue to "Custom Data" on page 190.

Proxy - Manual

If you select **Manual**, you must specify the proxy server, port number, and proxy domain information.

TABLE 29. PROXY - MANUAL SETTINGS

Item	Description
Name	Enter a short phrase that identifies this VPN setting.
Description	Provide a description that clarifies the purpose of these settings.
Channel	For macOS only. Select one of the following distribution options: • Device channel - the configuration is effective for all users on a device. This is the typical option. • User channel - the configuration is effective only for the currently registered user on a device.
Connection Type	Select **Cisco Legacy AnyConnect**.
Samsung Knox	This setting applies to Android devices only.
Deploy inside Knox Workspace	This setting applies to Android devices only.
Server	Enter the IP address, hostname, or URL for the VPN server.
Proxy Server	Enter the name for the proxy server.
Proxy Server Port	Enter the port number for the proxy server. Type - Select **Static** or **Variable** for the type of authentication to be used for the proxy server.
Proxy Server User Name	If the authentication type is **Static**, enter the user name for the proxy server. If the authentication type is **Variable**, the default variable selected is $USERID$.
Proxy Server Password	If the authentication type is **Static**, enter the password for the proxy server. Confirm the password in the field below. If the authentication type is **Variable**, the default variable selected is $PASSWORD$.
Proxy Domains (iOS only)	This setting applies to iOS and macOS devices only.
Username	Specify the user name to use. The default value is $USERID$. Use this field to specify an alternate format, such as:

TABLE 29. PROXY - MANUAL SETTINGS (CONT.)

Item	Description
	$USERID$, $EMAIL$, $SAM_ACCOUNT_NAME$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$, $CUSTOM_DEVICE_Attributename$, $CUSTOM_USER_Attributename$, $NULL$ You can use combinations such as the following: • $USERID$:$EMAIL$ • $USERID$_$EMAIL$ Enter $NULL$ if you want the field presented to the user to be blank. Users will need to fill in the relevant username. ⓘ Some enterprises have a strong preference concerning which identifier is exposed.
User Authentication	Select the user authentication to use: • Password - see next row for information. • Certificate - If you select Certificate, select the identity certificate to be used as the account credential. If you select Certificate, and extended authentication (EAP) is not used, this certificate will be sent out for IKE client authentication. If extended authentication is used, this certificate can be used for EAP-TLS.
Password	Specify the password to use (required.) The default value is $PASSWORD$. Include at least one of the following variables: $USERID$, $EMAIL$, $PASSWORD$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$, $CUSTOM_DEVICE_Attributename$, $CUSTOM_USER_Attributename$, $NULL$ You can use combinations such as $EMAIL$:$PASSWORD$ Enter $NULL$ if you want the field presented to the user to be blank. Users will need to fill in the relevant password.
Group Name	Specify the name of the group to use.
VPN on Demand	This setting does not apply to Windows devices.

TABLE 29. PROXY - MANUAL SETTINGS (CONT.)

Item	Description
Per-App VPN	This setting applies to iOS and macOS devices only.
Provider Type	This setting applies to iOS and macOS devices only.

Continue to "Windows Configuration" on page 190.

Continue to "Custom Data" on page 190.

Proxy - Automatic

If you selected an Automatic proxy, you must specify the proxy server URL and proxy domain(s).

TABLE 30. PROXY - AUTOMATIC SETTINGS

Item	Description
Name	Enter a short phrase that identifies this VPN setting.
Description	Provide a description that clarifies the purpose of these settings.
Channel	For macOS only. Select one of the following distribution options: • Device channel - the configuration is effective for all users on a device. This is the typical option. • User channel - the configuration is effective only for the currently registered user on a device.
Connection Type	Select **Cisco Legacy AnyConnect**.
Samsung Knox	This setting applies to Android devices only.
Deploy inside Knox Workspace	This setting applies to Android devices only.
Server	Enter the IP address, hostname, or URL for the VPN server.
Proxy Server URL	Enter the URL for the proxy server. Enter the URL of the location of the proxy auto-configuration file.
Proxy Domains (iOS only)	This setting applies to iOS and macOS devices only.
Username	Specify the user name to use (required.) The default value is $USERID$. Include at least one of the following variables:

TABLE 30. PROXY - AUTOMATIC SETTINGS (CONT.)

Item	Description
	$USERID$, $EMAIL$, $SAM_ACCOUNT_NAME$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$, $CUSTOM_DEVICE_Attributename$, $CUSTOM_USER_Attributename$, $NULL$ You can use combinations such as the following: • $USERID$:$EMAIL$ • $USERID$_$EMAIL$ Enter $NULL$ if you want the field presented to the user to be blank. Users will need to fill in the relevant username.
User Authentication	Select the user authentication to use: • Password - see next row for information. • Certificate - If you select Certificate, select the identity certificate to be used as the account credential. If you select Certificate, and extended authentication (EAP) is not used, this certificate will be sent out for IKE client authentication. If extended authentication is used, this certificate can be used for EAP-TLS.
Password	Specify the password to use (required.) The default value is $PASSWORD$. Include at least one of the following variables: $USERID$, $EMAIL$, $PASSWORD$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$, $CUSTOM_DEVICE_Attributename$, $CUSTOM_USER_Attributename$, $NULL$ You can use combinations such as $EMAIL$:$PASSWORD$ Enter $NULL$ if you want the field presented to the user to be blank. Users will need to fill in the relevant password.
Group Name	Specify the name of the group to use.
VPN On Demand	This setting does not apply to Windows devices.
Per-App VPN	This setting applies to iOS and macOS devices only.
Provider Type	This setting applies to iOS and macOS devices only.

Continue to "Windows Configuration" on the next page.

Continue to "Custom Data" below.

Windows Configuration

Allowed Secured Resources (Windows Phone only)
Excluded Secured Resources (Windows Phone only)

See "Application-triggered VPN for Windows devices" on page 243 for information on how to configure these settings to set up application-triggered VPN for 8.0.1 devices.

TABLE 31. WINDOWS CONFIGURATIONS

Item	Description
Windows Configuration	Enter the secured resources (domains, IP ranges, or apps) used by the **Send All Traffic** option.
Always On	Select this option to keep the VPN on. **Lock Down** supersedes this option for Windows devices.
Lock Down	You cannot change the assigned settings unless 1) the **Lock Down** setting is removed from the profile and the new profile is pushed to the device or 2) the device is un-enrolled from Core. This option supersedes the **Always On** option.

Custom Data

Custom Data does not apply to Android devices.

- **Add+** - Click to add a new key / value pair.
- **Key / Value** - Enter the Key / value pairs necessary to configure the VPN setting. The app creator should provide the necessary key / value pairs.

F5 SSL

This VPN connection type is supported on iOS, macOS, Windows devices. F5 SSL supports Android devices that have Samsung Knox enabled and on Android devices without Samsung Knox.

Use the following guidelines to configure the F5 SSL VPN connection type:

- "Proxy - None (default)" on the next page
- "Proxy - Manual " on page 193

- "Proxy - Automatic" on page 195

Within these selections, you may make settings for:

- "Windows Configuration" on page 197
- "Custom Data" on page 197

Proxy - None (default)

Use the following guidelines to configure a F5 SSL VPN without a proxy.

TABLE 32. PROXY - NONE SETTINGS

Item	Description
Name	Enter a short phrase that identifies this VPN setting.
Description	Provide a description that clarifies the purpose of these settings.
Channel	For macOS only. Select one of the following distribution options: • Device channel - the configuration is effective for all users on a device. This is the typical option. • User channel - the configuration is effective only for the currently registered user on a device.
Connection Type	This setting is not supported on Windows devices.Select **F5 SSL**.
Samsung Knox	This setting is only supported on Android devices.
Deploy inside Knox Workspace	This setting is only supported on Android devices.
Server	Enter the IP address, hostname, or URL for the VPN server.
Proxy	**None** is the default setting. To configure a **Manual** or **Automatic** proxy, go to "Proxy - Manual " on page 193 or "Proxy - Automatic" on page 195.
Username	Specify the user name to use. The default value is $USERID$. Use this field to specify an alternate format, such as: $USERID$, $EMAIL$, $SAM_ACCOUNT_NAME$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$, $CUSTOM_DEVICE_Attributename$, $CUSTOM_USER_Attributename$, $NULL$

TABLE 32. PROXY - NONE SETTINGS (CONT.)

Item	Description
	You can use combinations such as the following: • $USERID$:$EMAIL$ • $USERID$_$EMAIL$ Enter $NULL$ if you want the field presented to the user to be blank. Users will need to fill in the relevant username. ⓘ Some enterprises have a strong preference concerning which identifier is exposed.
User Authentication	Select the user authentication to use: • Password - see next row for information. • Certificate - If you select Certificate, select the identity certificate to be used as the account credential. If you select Certificate, and extended authentication (EAP) is not used, this certificate will be sent out for IKE client authentication. If extended authentication is used, this certificate can be used for EAP-TLS.
Password	Specify the password to use (required.) The default value is $PASSWORD$. Include at least one of the following variables: $USERID$, $EMAIL$, $PASSWORD$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$, $CUSTOM_DEVICE_Attributename$, $CUSTOM_USER_ Attributename$, $NULL$ You can use combinations such as $EMAIL$:$PASSWORD$ Enter $NULL$ if you want the field presented to the user to be blank. Users will need to fill in the relevant password.
VPN On Demand	This setting applies to Windows devices only.
Per-App VPN	This setting does not apply to Windows devices.
Provider Type	This setting applies to iOS and macOS devices only.

Continue to "Windows Configuration" on page 197.

Continue to "Custom Data" on page 197.

Proxy - Manual

If you select **Manual**, you must specify the proxy server, port number. and proxy domain information.

TABLE 33. PROXY - MANUAL SETTINGS

Item	Description
Name	Enter a short phrase that identifies this VPN setting.
Description	Provide a description that clarifies the purpose of these settings.
Channel	For macOS only. Select one of the following distribution options: • Device channel - the configuration is effective for all users on a device. This is the typical option. • User channel - the configuration is effective only for the currently registered user on a device.
Connection Type	This setting is not supported on Windows devices.Select **F5 SSL**.
Samsung Knox	This setting is only supported on Android devices.
Deploy inside Knox Workspace	This setting is only supported on Android devices.
Server	Enter the IP address, hostname, or URL for the VPN server.
Proxy	Select **Manual**. For an Automatic proxy, see "Proxy - Automatic" on page 195.
Proxy Server	Enter the name for the proxy server.
Proxy Server Port	Enter the port number for the proxy server. Type - Select **Static** or **Variable** for the type of authentication to be used for the proxy server.
Proxy Server User Name	If the authentication type is **Static**, enter the user name for the proxy server. If the authentication type is **Variable**, the default variable selected is $USERID$.
Proxy Server Password	If the authentication type is **Static**, enter the password for the proxy server. Confirm the password in the field below. If the authentication type is **Variable**, the default variable selected is $PASSWORD$.
Proxy Domains (iOS only)	This setting applies to iOS and macOS devices only.

Table 33. Proxy - Manual settings (Cont.)

Item	Description
Username	Specify the user name to use. The default value is $USERID$. Use this field to specify an alternate format, such as: $USERID$, $EMAIL$, $SAM_ACCOUNT_NAME$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$, $CUSTOM_DEVICE_Attributename$, $CUSTOM_USER_Attributename$, $NULL$ You can use combinations such as the following: • $USERID$:$EMAIL$ • $USERID$_$EMAIL$ Enter $NULL$ if you want the field presented to the user to be blank. Users will need to fill in the relevant username. ℹ Some enterprises have a strong preference concerning which identifier is exposed.
User Authentication	Select the user authentication to use: • Password - see next row for information. • Certificate - If you select Certificate, select the identity certificate to be used as the account credential. If you select Certificate, and extended authentication (EAP) is not used, this certificate will be sent out for IKE client authentication. If extended authentication is used, this certificate can be used for EAP-TLS.
Password	Specify the password to use (required.) The default value is $PASSWORD$. Include at least one of the following variables: $USERID$, $EMAIL$, $PASSWORD$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$, $CUSTOM_DEVICE_Attributename$, $CUSTOM_USER_Attributename$, $NULL$ You can use combinations such as $EMAIL$:$PASSWORD$ Enter $NULL$ if you want the field presented to the user to be blank. Users will need to fill in the relevant password.

TABLE 33. PROXY - MANUAL SETTINGS (CONT.)

Item	Description
Per-App VPN	This setting does not apply to Windows devices.
Provider Type	This setting applies to iOS and macOS devices only.

Continue to "Windows Configuration" on page 197.

Continue to "Custom Data" on page 197.

Proxy - Automatic

If you selected an Automatic proxy, you must specify the proxy server URL and proxy domain(s).

For Windows 10 devices, please add the configuration and value for automatic proxy in the Custom Data Grid. Automatic proxy is not supported in Windows 8.1.

TABLE 34. PROXY - AUTOMATIC SETTINGS

Item	Description
Name	Enter a short phrase that identifies this VPN setting.
Description	Provide a description that clarifies the purpose of these settings.
Channel	For macOS only. Select one of the following distribution options: • Device channel - the configuration is effective for all users on a device. This is the typical option. • User channel - the configuration is effective only for the currently registered user on a device.
Connection Type	This setting is not supported on Windows devices.Select **F5 SSL**.
Samsung Knox	This setting is only supported on Android devices.
Deploy inside Knox Workspace	This setting is only supported on Android devices.
Server	Enter the IP address, hostname, or URL for the VPN server.
Proxy	Select **Automatic**. For a manual proxy, see "Proxy - Manual " on page 193
Proxy Server URL	Enter the URL for the proxy server.

TABLE 34. PROXY - AUTOMATIC SETTINGS (CONT.)

Item	Description
	Enter the URL of the location of the proxy auto-configuration file.
Proxy Domains (iOS only)	This setting applies to iOS and macOS devices only.
Username	Specify the user name to use (required.) The default value is $USERID$. Include at least one of the following variables: $USERID$, $EMAIL$, $SAM_ACCOUNT_NAME$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$, $CUSTOM_DEVICE_Attributename$, $CUSTOM_USER_Attributename$, $NULL$ You can use combinations such as the following: • $USERID$:$EMAIL$ • $USERID$_$EMAIL$ Enter $NULL$ if you want the field presented to the user to be blank. Users will need to fill in the relevant username.
User Authentication	Select the user authentication to use: • Password - see next row for information. • Certificate - If you select Certificate, select the identity certificate to be used as the account credential. If you select Certificate, and extended authentication (EAP) is not used, this certificate will be sent out for IKE client authentication. If extended authentication is used, this certificate can be used for EAP-TLS.
Password	Specify the password to use (required.) The default value is $PASSWORD$. Include at least one of the following variables: $USERID$, $EMAIL$, $PASSWORD$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$, $CUSTOM_DEVICE_Attributename$, $CUSTOM_USER_Attributename$, $NULL$ You can use combinations such as $EMAIL$:$PASSWORD$ Enter $NULL$ if you want the field presented to the user to be blank. Users will need to fill in the relevant password.

TABLE 34. PROXY - AUTOMATIC SETTINGS (CONT.)

Item	Description
VPN On Demand	This setting does not apply to Windows devices.
Per-App VPN	This setting does not apply to Windows devices.
Provider Type	This setting applies to iOS and macOS devices only.

Continue to "Windows Configuration" below.

Continue to "Custom Data" below.

Windows Configuration

Allowed Secured Resources (Windows Phone only)
Excluded Secured Resources (Windows Phone only)

See "Application-triggered VPN for Windows devices" on page 243 for information on how to configure these settings to set up application-triggered VPN for 8.0.1 devices.

TABLE 35. WINDOWS CONFIGURATIONS

Item	Description
Windows Configuration	Enter the secured resources (domains, IP ranges, or apps) used by the **Send All Traffic** option.
Always On	Select this option to keep the VPN on. **Lock Down** supersedes this option for Windows devices.
Lock Down	You cannot change the assigned settings unless 1) the **Lock Down** setting is removed from the profile and the new profile is pushed to the device or 2) the device is un-enrolled from Core. This option supersedes the **Always On** option.

Custom Data

- **Add+** - Click to add a new key / value pair.
- **Key / Value** - Enter the Key / value pairs necessary to configure the VPN setting. The app creator should provide the necessary key / value pairs.

IKEv2 (iOS Only)

This VPN connection type is supported on iOS devices. It is not supported on Android, macOS, and Windows devices.

iOS VPN configurations using IKEv2 need to include a selected value from the following list of certificate types:

- RSA
- ECDSA256
- ECDSA384
- ECDSA512

The ED25519 certificate type is not supported.

IKEv2 (Windows)

This VPN connection type is supported on Windows devices. It is not supported on Android, iOS, and macOS devices.

ⓘ For Windows 10 devices, please add the configuration and value for auto proxy in the Custom Data Grid. Please note that the Automatic proxy is not supported in Windows 8.1.

Note the following:

- Windows devices do not support pushing $USERID$ and $PASSWORD$ to the device in VPN settings. The device user must enter user name and password to connect to VPN.
- For certificate authentication, Windows devices only support identity certificates using SCEP reverse proxy.

Use the following guidelines to configure a IKEv2 (Windows) VPN.

- "Proxy - None (default)" on the next page
- "Proxy - Manual " on page 201
- "Proxy - Automatic" on page 203

Within these selections, you may make settings for:

- "Windows Configuration" on page 205
- "Custom Data" on page 205

Proxy - None (default)

Use the following guidelines to configure a IKEv2 (Windows) VPN connection without a proxy.

TABLE 36. PROXY - NONE SETTINGS

Item	Description
Name	Enter a short phrase that identifies this VPN setting.
Description	Provide a description that clarifies the purpose of these settings.
Channel	For macOS only. Select one of the following distribution options: • Device channel - the configuration is effective for all users on a device. This is the typical option. • User channel - the configuration is effective only for the currently registered user on a device.
Connection Type	Select **IKEv2 (Windows)**.
Server	Enter the IP address, hostname, or URL for the VPN server.
Proxy	**None** is the default setting. To configure a Manual or Automatic proxy, go to "Proxy - Manual " on page 201 or "Proxy - Automatic" on page 203. ⓘ Windows 8.1 devices do not currently support *Automatic* Proxy.
Proxy Server	*Select Manual proxy to see this option.* Enter the name for the proxy server.
Username	Specify the user name to use (required.) The default value is $USERID$. Use this field to specify an alternate format, such as: $USERID$, $EMAIL$, $SAM_ACCOUNT_NAME$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$, $CUSTOM_DEVICE_Attributename$, $CUSTOM_USER_Attributename$, $NULL$ You can use combinations such as the following:

TABLE 36. PROXY - NONE SETTINGS (CONT.)

Item	Description
	• $USERID$:$EMAIL$ • $USERID$_$EMAIL$ Enter $NULL$ if you want the field presented to the user to be blank. Users will need to fill in the relevant username. ℹ Some enterprises have a strong preference concerning which identifier is exposed.
User Authentication	Select the user authentication to use: • Password - see next row for information. • Certificate - If you select Certificate, select the identity certificate to be used as the account credential.
Password	Specify the password to use (required.) The default value is $PASSWORD$. Include at least one of the following variables: $USERID$, $EMAIL$, $PASSWORD$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$, $CUSTOM_DEVICE_Attributename$, $CUSTOM_USER_Attributename$, $NULL$ You can use combinations such as $EMAIL$:$PASSWORD$ Enter $NULL$ if you want the field presented to the user to be blank. Users will need to fill in the relevant password.
Send All Traffic	Select to send all traffic from the Windows device through the VPN gateway. When *Send All Traffic* is checked, all traffic is sent through the VPN gateway with the exception of traffic from the resources you enter in this table. When *Send All Traffic* is unchecked, only traffic from the resources you enter in this table is sent through the VPN gateway.

Continue to "Windows Configuration" on page 205.

Continue to "Custom Data" on page 205.

Proxy - Manual

Use the following guidelines to configure a IKEv2 (Windows) VPN connection with a manual proxy.

TABLE 37. PROXY - MANUAL SETTINGS

Item	Description
Name	Enter a short phrase that identifies this VPN setting.
Description	Provide a description that clarifies the purpose of these settings.
Channel	For macOS only. Select one of the following distribution options: • Device channel - the configuration is effective for all users on a device. This is the typical option. • User channel - the configuration is effective only for the currently registered user on a device.
Connection Type	Select **IKEv2 (Windows)**.
Server	Enter the IP address, hostname, or URL for the VPN server.
Proxy	Select **Manual**. To configure an Automatic proxy, go to "Proxy - Automatic" on page 203. ℹ Windows 8.1 devices do not currently support *Automatic* Proxy.
Proxy Server	*Select Manual proxy to see this option.* Enter the name for the proxy server.
Proxy Server Port	*Select Manual proxy to see this option.* Enter the port for the proxy server.
Type	*Select Manual proxy to see this option.* Select **Static** or **Variable**.
Proxy Server User Name	*Select Manual proxy to see this option.* If the type is Static, enter the username for the proxy server If the type is Variable, the default variable selected is $USERID$. ℹ Windows devices do not support Proxy Server User Name.
Proxy Server Password	*Select Manual proxy to see this option.* If the type is Static, enter the password for the proxy server If the type is Variable, the default variable selected is $PASSWORD$.

TABLE 37. PROXY - MANUAL SETTINGS (CONT.)

Item	Description
	ⓘ Windows devices do not support Proxy Server Password.
Username	Specify the user name to use (required.) The default value is $USERID$. Use this field to specify an alternate format, such as: $USERID$, $EMAIL$, $SAM_ACCOUNT_NAME$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$, $CUSTOM_DEVICE_Attributename$, $CUSTOM_USER_Attributename$, $NULL$ You can use combinations such as the following: • $USERID$:$EMAIL$ • $USERID$_$EMAIL$ Enter $NULL$ if you want the field presented to the user to be blank. Users will need to fill in the relevant username. ⓘ Some enterprises have a strong preference concerning which identifier is exposed.
User Authentication	Select the user authentication to use: • Password - see next row for information. • Certificate - If you select Certificate, select the identity certificate to be used as the account credential.
Password	Specify the password to use (required.) The default value is $PASSWORD$. Include at least one of the following variables: $USERID$, $EMAIL$, $PASSWORD$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$, $CUSTOM_DEVICE_Attributename$, $CUSTOM_USER_Attributename$, $NULL$ You can use combinations such as $EMAIL$:$PASSWORD$ Enter $NULL$ if you want the field presented to the user to be blank. Users will need to fill in the relevant password.
Send All Traffic	Select to send all traffic from the Windows device through the VPN gateway.

TABLE 37. PROXY - MANUAL SETTINGS (CONT.)

Item	Description
	When *Send All Traffic* is checked, all traffic is sent through the VPN gateway with the exception of traffic from the resources you enter in this table. When *Send All Traffic* is unchecked, only traffic from the resources you enter in this table is sent through the VPN gateway.

Continue to "Windows Configuration" on page 205.

Continue to "Custom Data" on page 205.

Proxy - Automatic

Use the following guidelines to configure a IKEv2 (Windows) VPN connection with an automatic proxy.

For Windows 10 devices, please add the configuration and value for auto proxy in the Custom Data Grid. Please note that the Automatic proxy is not supported in Windows 8.1.

TABLE 38. PROXY - AUTOMATIC SETTINGS

Item	Description
Name	Enter a short phrase that identifies this VPN setting.
Description	Provide a description that clarifies the purpose of these settings.
Channel	For macOS only. Select one of the following distribution options: • Device channel - the configuration is effective for all users on a device. This is the typical option. • User channel - the configuration is effective only for the currently registered user on a device.
Connection Type	Select **IKEv2 (Windows)**.
Server	Enter the IP address, hostname, or URL for the VPN server.
Proxy	Select **Automatic**. To configure an Manual proxy, go to "Proxy - Manual " on page 201.

TABLE 38. PROXY - AUTOMATIC SETTINGS (CONT.)

Item	Description
	ⓘ Windows 8.1 devices do not currently support *Automatic* Proxy.
Proxy Server URL	*Select Automatic proxy to see this option.* Enter the URL for the proxy server.
Username	Specify the user name to use (required.) The default value is $USERID$. Use this field to specify an alternate format, such as: $USERID$, $EMAIL$, $SAM_ACCOUNT_NAME$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$, $CUSTOM_DEVICE_Attributename$, $CUSTOM_USER_Attributename$, $NULL$ You can use combinations such as the following: • $USERID$:$EMAIL$ • $USERID$_$EMAIL$ Enter $NULL$ if you want the field presented to the user to be blank. Users will need to fill in the relevant username. ⓘ Some enterprises have a strong preference concerning which identifier is exposed.
User Authentication	Select the user authentication to use: • Password - see next row for information. • Certificate - If you select Certificate, select the identity certificate to be used as the account credential.
Password	Specify the password to use (required.) The default value is $PASSWORD$. Include at least one of the following variables: $USERID$, $EMAIL$, $PASSWORD$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$, $CUSTOM_DEVICE_Attributename$, $CUSTOM_USER_Attributename$, $NULL$ You can use combinations such as $EMAIL$:$PASSWORD$ Enter $NULL$ if you want the field presented to the user to be blank. Users will need to fill in the relevant password.

TABLE 38. PROXY - AUTOMATIC SETTINGS (CONT.)

Item	Description
Send All Traffic	Select to send all traffic from the Windows device through the VPN gateway. When *Send All Traffic* is checked, all traffic is sent through the VPN gateway with the exception of traffic from the resources you enter in this table. When *Send All Traffic* is unchecked, only traffic from the resources you enter in this table is sent through the VPN gateway.

Continue to "Windows Configuration" below.

Continue to "Custom Data" below.

Windows Configuration

Allowed Secured Resources (Windows Phone only)
Excluded Secured Resources (Windows Phone only)

See "Application-triggered VPN for Windows devices" on page 243 for information on how to configure these settings to set up application-triggered VPN for 8.0.1 devices.

TABLE 39. WINDOWS CONFIGURATIONS

Item	Description
Windows Configuration	Enter the secured resources (domains, IP ranges, or apps) used by the **Send All Traffic** option.
Always On	Select this option to keep the VPN on. **Lock Down** supersedes this option for Windows devices.
Lock Down	You cannot change the assigned settings unless 1) the **Lock Down** setting is removed from the profile and the new profile is pushed to the device or 2) the device is un-enrolled from Core. This option supersedes the **Always On** option.

Custom Data

- **Add+** - Click to add a new key / value pair.
- **Key / Value** - Enter the Key / value pairs necessary to configure the VPN setting. The app creator should provide the necessary key / value pairs.

IPSec (Blue Coat)

This VPN connection type is supported on iOS devices. It is not supported on Android, macOS, and Windows devices.

IPSec (Cisco)

This VPN connection type is supported on iOS and macOS devices. It is not supported on Android and Windows devices.

Juniper SSL

This VPN connection type is supported on iOS, macOS, Android and Windows devices.

Ivanti recommends that you use Pulse Secure SSL instead of Juniper SSL.

Use the following guidelines to configure Juniper SSL VPN.

- "Proxy - None (default)" below
- "Proxy - Manual " on page 208
- "Proxy - Automatic" on page 210

Within these selections, you may make settings for:

- "Windows Configuration" on page 212
- "Custom Data" on page 213

Proxy - None (default)

Use the following guidelines to configure a Juniper SSL VPN without a proxy.

TABLE 40. PROXY - NONE SETTINGS

Item	Description
Name	Enter a short phrase that identifies this VPN setting.
Description	Provide a description that clarifies the purpose of these settings.
Channel	For macOS only. Select one of the following distribution options:

TABLE 40. PROXY - NONE SETTINGS (CONT.)

Item	Description
	- Device channel - the configuration is effective for all users on a device. This is the typical option. - User channel - the configuration is effective only for the currently registered user on a device.
Connection Type	Select **Juniper SSL**.
Samsung Knox	This setting applies to Android devices only.
Deploy inside Knox Workspace	This setting applies to Android devices only.
Server	Enter the IP address, hostname, or URL for the VPN server.
Proxy	**None** is the default setting. To configure a Manual or Automatic proxy, go to "Proxy - Manual " on the next page or "Proxy - Automatic" on page 210.
Username	Specify the user name to use (required.) The default value is $USERID$. Use this field to specify an alternate format, such as: $USERID$, $EMAIL$, $SAM_ACCOUNT_NAME$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$, $CUSTOM_DEVICE_Attributename$, $CUSTOM_USER_Attributename$, $NULL$ You can use combinations such as the following: - $USERID$:$EMAIL$ - $USERID$_$EMAIL$ Enter $NULL$ if you want the field presented to the user to be blank. Users will need to fill in the relevant username. ⓘ Some enterprises have a strong preference concerning which identifier is exposed.
User Authentication	Select the user authentication to use: - Password - see next row for information. - Certificate - If you select Certificate, select the identity certificate to be used as the account credential.

TABLE 40. PROXY - NONE SETTINGS (CONT.)

Item	Description
Password	Specify the password to use (required.) The default value is $PASSWORD$. Include at least one of the following variables: $USERID$, $EMAIL$, $PASSWORD$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$, $CUSTOM_DEVICE_Attributename$, $CUSTOM_USER_Attributename$, $NULL$ You can use combinations such as $EMAIL$:$PASSWORD$ Enter $NULL$ if you want the field presented to the user to be blank. Users will need to fill in the relevant password.
Role	Specify the Juniper user role to use as a restriction.
Realm	Specify the Juniper realm to use as a restriction.
VPN On Demand	This setting does not apply to Windows devices.
Per-app VPN	This setting does not apply to Windows devices.
Provider Type	This setting applies to iOS and macOS devices only.

Continue to "Windows Configuration" on page 212.

Continue to "Custom Data" on page 213.

Proxy - Manual

Use the following guidelines to configure a Juniper SSL VPN with a manual proxy.

TABLE 41. PROXY - MANUAL SETTINGS

Item	Description
Name	Enter a short phrase that identifies this VPN setting.
Description	Provide a description that clarifies the purpose of these settings.
Channel	For macOS only. Select one of the following distribution options: • Device channel - the configuration is effective for all users on a device. This is the typical option. • User channel - the configuration is effective only for the currently registered user on a device.

TABLE 41. PROXY - MANUAL SETTINGS (CONT.)

Item	Description
Connection Type	Select **Juniper SSL**.
Samsung Knox	This setting applies to Android devices only.
Deploy inside Knox Workspace	This setting applies to Android devices only.
Server	Enter the IP address, hostname, or URL for the VPN server.
Proxy	Select **Manual**. To configure an Automatic proxy, go to "Proxy - Automatic" on the next page.
Proxy Server	Enter the name for the proxy server.
Proxy Server Port	Enter the port number for the proxy server.
Type	Select **Static** or **Variable** for the type of authentication to be used for the proxy server.
Proxy Server User Name	If the authentication type is **Static**, enter the username for the proxy server. If the authentication type is **Variable**, the default variable selected is $USERID$.
Proxy Server Password	If the authentication type is **Static**, enter the password for the proxy server. Confirm the password in the field below. If the authentication type is **Variable**, the default variable selected is $PASSWORD$.
Proxy Domains (iOS only)	This setting applies to iOS and macOS devices only.
Username	Specify the user name to use (required.) The default value is $USERID$. Use this field to specify an alternate format, such as: $USERID$, $EMAIL$, $SAM_ACCOUNT_NAME$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$, $CUSTOM_DEVICE_Attributename$, $CUSTOM_USER_Attributename$, $NULL$ You can use combinations such as the following: • $USERID$:$EMAIL$ • $USERID$_$EMAIL$ Enter $NULL$ if you want the field presented to the user to be blank. Users will need to fill in the relevant username.

TABLE 41. PROXY - MANUAL SETTINGS (CONT.)

Item	Description
	ⓘ Some enterprises have a strong preference concerning which identifier is exposed.
User Authentication	Select the user authentication to use: - Password - see next row for information. - Certificate - If you select Certificate, select the identity certificate to be used as the account credential.
Password	Specify the password to use (required.) The default value is $PASSWORD$. Include at least one of the following variables: $USERID$, $EMAIL$, $PASSWORD$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$, $CUSTOM_DEVICE_Attributename$, $CUSTOM_USER_ Attributename$, $NULL$ You can use combinations such as $EMAIL$:$PASSWORD$ Enter $NULL$ if you want the field presented to the user to be blank. Users will need to fill in the relevant password.
Role	Specify the Juniper user role to use as a restriction.
Realm	Specify the Juniper realm to use as a restriction.
VPN On Demand	This setting does not apply to Windows devices.
Per-app VPN	This setting does not apply to Windows devices.
Provider Type	This setting applies to iOS and macOS devices only.

Continue to "Windows Configuration" on page 212

Continue to "Custom Data" on page 213.

Proxy - Automatic

Use the following guidelines to configure a Juniper SSL VPN with an automatic proxy.

TABLE 42. PROXY - AUTOMATIC SETTINGS

Item	Description
Name	Enter a short phrase that identifies this VPN setting.
Description	Provide a description that clarifies the purpose of these settings.
Channel	For macOS only. Select one of the following distribution options: • Device channel - the configuration is effective for all users on a device. This is the typical option. • User channel - the configuration is effective only for the currently registered user on a device.
Connection Type	Select **Juniper SSL**.
Samsung Knox	This setting applies to Android devices only.
Deploy inside Knox Workspace	This setting applies to Android devices only.
Server	Enter the IP address, hostname, or URL for the VPN server.
Proxy	Select **Automatic**. To configure a manual proxy, go to "Proxy - Manual " on page 208.
Proxy Server URL	Enter the URL for the proxy server. Enter the URL of the location of the proxy auto-configuration file.
Proxy Domains (iOS only)	This setting applies to iOS and macOS devices only.
Username	Specify the user name to use (required.) The default value is $USERID$. Use this field to specify an alternate format, such as: $USERID$, $EMAIL$, $SAM_ACCOUNT_NAME$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$, $CUSTOM_DEVICE_Attributename$, $CUSTOM_USER_Attributename$, $NULL$ You can use combinations such as the following: • $USERID$:$EMAIL$ • $USERID$_$EMAIL$ Enter $NULL$ if you want the field presented to the user to be blank. Users will need to fill in the relevant username.

TABLE 42. PROXY - AUTOMATIC SETTINGS (CONT.)

Item	Description
	ⓘ Some enterprises have a strong preference concerning which identifier is exposed.
User Authentication	Select the user authentication to use: • Password - see next row for information. • Certificate - If you select Certificate, select the identity certificate to be used as the account credential.
Password	Specify the password to use (required.) The default value is $PASSWORD$. Include at least one of the following variables: $USERID$, $EMAIL$, $PASSWORD$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$, $CUSTOM_DEVICE_Attributename$, $CUSTOM_USER_Attributename$, $NULL$ You can use combinations such as $EMAIL$:$PASSWORD$ Enter $NULL$ if you want the field presented to the user to be blank. Users will need to fill in the relevant password.
Role	Specify the Juniper user role to use as a restriction.
Realm	Specify the Juniper realm to use as a restriction.
VPN On Demand	This setting does not apply to Windows devices.
Per-app VPN	This setting does not apply to Windows devices.
Provider Type	This setting applies to iOS and macOS devices only.

Continue to "Windows Configuration" below.

Continue to "Custom Data" on the next page.

Windows Configuration

Allowed Secured Resources (Windows Phone only)
Excluded Secured Resources (Windows Phone only)

See "Application-triggered VPN for Windows devices" on page 243 for information on how to configure these settings to set up application-triggered VPN for 8.0.1 devices.

TABLE 43. WINDOWS CONFIGURATIONS

Item	Description
Windows Configuration	Enter the secured resources (domains, IP ranges, or apps) used by the **Send All Traffic** option.
Always On	Select this option to keep the VPN on. **Lock Down** supersedes this option for Windows devices.
Lock Down	You cannot change the assigned settings unless 1) the **Lock Down** setting is removed from the profile and the new profile is pushed to the device or 2) the device is un-enrolled from Core. This option supersedes the **Always On** option.

Custom Data

- **Add+** - Click to add a new key / value pair.
- **Key / Value** - Enter the Key / value pairs necessary to configure the VPN setting. The app creator should provide the necessary key / value pairs.

L2TP

This VPN connection type is supported on iOS, macOS, and Windows devices. It is not supported on Android devices.

This section covers how to configure L2TP VPN.

- "Proxy - None (default)" below
- "Proxy - Manual" on page 215
- "Proxy - Automatic" on page 217

Proxy - None (default)

Use the following guidelines to configure a L2TP VPN without a proxy.

TABLE 44. PROXY - NONE SETTINGS

Item	Description
Name	Enter a short phrase that identifies this VPN setting.

TABLE 44. PROXY - NONE SETTINGS (CONT.)

Item	Description
Description	Provide a description that clarifies the purpose of these settings.
Channel	For macOS only. Select one of the following distribution options: • Device channel - the configuration is effective for all users on a device. This is the typical option. • User channel - the configuration is effective only for the currently registered user on a device.
Connection Type	Select **L2TP**.
Server	Enter the IP address, hostname, or URL for the VPN server.
Proxy	**None** is the default setting. To configure a Manual or Automatic proxy, go to "Proxy - Manual" on the next page or "Proxy - Automatic" on page 217.
Shared Secret	The shared secret passcode. This is not the user’s password; the shared secret must be specified to initiate a connection.
Confirm Shared Secret	Re-enter the shared secret to confirm.
Send all Traffic	Selecting this option protects data from being compromised, particularly on public networks.
Username	Specify the user name to use. The default value is $USERID$. Use this field to specify an alternate format, such as: $USERID$, $EMAIL$, $SAM_ACCOUNT_NAME$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$, $CUSTOM_DEVICE_Attributename$, $CUSTOM_USER_Attributename$, $NULL$ You can use combinations such as the following: • $USERID$:$EMAIL$ • $USERID$_$EMAIL$ Enter $NULL$ if you want the field presented to the user to be blank. Users will need to fill in the relevant username. ⓘ Some enterprises have a strong preference concerning which identifier is exposed.

TABLE 44. PROXY - NONE SETTINGS (CONT.)

Item	Description
User Authentication	Select the authentication method to use**:** **Password** or **RSA SecureID**.
Password	Specify the password to use (required.) The default value is $PASSWORD$. Include at least one of the following variables: $USERID$, $EMAIL$, $PASSWORD$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$, $CUSTOM_DEVICE_Attributename$, $CUSTOM_USER_ Attributename$, $NULL$ You can use combinations such as $EMAIL$:$PASSWORD$ Enter $NULL$ if you want the field presented to the user to be blank. Users will need to fill in the relevant password.

Proxy - Manual

Use the following guidelines to configure a L2TP VPN with a manual proxy.

TABLE 45. PROXY - MANUAL SETTINGS

Item	Description
Name	Enter a short phrase that identifies this VPN setting.
Description	Provide a description that clarifies the purpose of these settings.
Channel	For macOS only. Select one of the following distribution options: • Device channel - the configuration is effective for all users on a device. This is the typical option. • User channel - the configuration is effective only for the currently registered user on a device.
Connection Type	Select **L2TP**.
Server	Enter the IP address, hostname, or URL for the VPN server.
Proxy	Select **Manual**. To configure an automatic proxy, go to "Proxy - Automatic" on page 217.
Proxy Server	Enter the name for the proxy server.

TABLE 45. PROXY - MANUAL SETTINGS (CONT.)

Item	Description
Proxy Server Port	Enter the port number for the proxy server.
Type	Select **Static** or **Variable** for the type of authentication to be used for the proxy server.
Proxy Server User Name	If the authentication type is **Static**, enter the username for the proxy server. If the authentication type is **Variable**, the default variable selected is $USERID$.
Proxy Server Password	If the authentication type is **Static**, enter the password for the proxy server. Confirm the password in the field below. If the authentication type is **Variable**, the default variable selected is $PASSWORD$.
Proxy Domains (iOS only)	This setting applies to iOS and macOS devices only. The VPN will only proxy for the domain and domain suffixes specified here (`.com` and `.org` are examples of top-level domain suffixes). Domain suffixes can be used to match multiple domains. For example, `.com` would include all `.com` domains, and `example.com` would include all domains ending in example.com, such as `pages.example.com` and `mysite.example.com`. Wildcards are not supported. Click **Add+** to add a domain.
Shared Secret	The shared secret passcode. This is not the user's password; the shared secret must be specified to initiate a connection.
Confirm Shared Secret	Re-enter the shared secret to confirm.
Send all Traffic	Selecting this option protects data from being compromised, particularly on public networks.
Username	Specify the user name to use. The default value is $USERID$. Use this field to specify an alternate format, such as: $USERID$, $EMAIL$, $SAM_ACCOUNT_NAME$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$, $CUSTOM_DEVICE_Attributename$, $CUSTOM_USER_Attributename$, $NULL$ You can use combinations such as the following: • $USERID$:$EMAIL$ • $USERID$_$EMAIL$

TABLE 45. PROXY - MANUAL SETTINGS (CONT.)

Item	Description
	Enter $NULL$ if you want the field presented to the user to be blank. Users will need to fill in the relevant username. ⓘ Some enterprises have a strong preference concerning which identifier is exposed.
User Authentication	Select the authentication method to use:**Password** or **RSA SecureID**.
Password	Specify the password to use (required.) The default value is $PASSWORD$. Include at least one of the following variables: $USERID$, $EMAIL$, $PASSWORD$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$, $CUSTOM_DEVICE_Attributename$, $CUSTOM_USER_Attributename$, $NULL$ You can use combinations such as $EMAIL$:$PASSWORD$ Enter $NULL$ if you want the field presented to the user to be blank. Users will need to fill in the relevant password.

Proxy - Automatic

Use the following guidelines to configure a L2TP VPN with an automatic proxy.

TABLE 46. PROXY - AUTOMATIC SETTINGS

Item	Description
Name	Enter a short phrase that identifies this VPN setting.
Description	Provide a description that clarifies the purpose of these settings.
Channel	For macOS only. Select one of the following distribution options: • Device channel - the configuration is effective for all users on a device. This is the typical option. • User channel - the configuration is effective only for the currently registered user on a device.
Connection Type	Select **L2TP**.

TABLE 46. PROXY - AUTOMATIC SETTINGS (CONT.)

Item	Description
Server	Enter the IP address, hostname, or URL for the VPN server.
Proxy	Select **Automatic**. To configure a Manual proxy, go to "Proxy - Manual" on page 215.
Proxy Server URL	Enter the URL for the proxy server. Enter the URL of the location of the proxy auto-configuration file.
Proxy Domains (iOS only)	This setting applies to iOS and macOS devices only. The VPN will only proxy for the domain and domain suffixes specified here (`.com` and `.org` are examples of top-level domain suffixes). Domain suffixes can be used to match multiple domains. For example, `.com` would include all `.com` domains, and `example.com` would include all domains ending in example.com, such as `pages.example.com` and `mysite.example.com`. Wildcards are not supported. Click **Add+** to add a domain.
Shared Secret	The shared secret passcode. This is not the user's password; the shared secret must be specified to initiate a connection.
Confirm Shared Secret	Re-enter the shared secret to confirm.
Send all Traffic	Selecting this option protects data from being compromised, particularly on public networks.
Username	Specify the user name to use. The default value is $USERID$. Use this field to specify an alternate format, such as: $USERID$, $EMAIL$, $SAM_ACCOUNT_NAME$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$, $CUSTOM_DEVICE_Attributename$, $CUSTOM_USER_Attributename$, $NULL$ You can use combinations such as the following: • $USERID$:$EMAIL$ • $USERID$_$EMAIL$ Enter $NULL$ if you want the field presented to the user to be blank. Users will need to fill in the relevant username. ⓘ Some enterprises have a strong preference concerning which identifier is exposed.

TABLE 46. PROXY - AUTOMATIC SETTINGS (CONT.)

Item	Description
User Authentication	Select the authentication method to use:**Password** or **RSA SecureID**.
Password	Specify the password to use (required.) The default value is $PASSWORD$. Include at least one of the following variables: $USERID$, $EMAIL$, $PASSWORD$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$, $CUSTOM_DEVICE_Attributename$, $CUSTOM_USER_Attributename$, $NULL$ You can use combinations such as $EMAIL$:$PASSWORD$ Enter $NULL$ if you want the field presented to the user to be blank. Users will need to fill in the relevant password.

Tunnel (iOS and macOS)

This VPN connection type is supported on iOS and macOS devices only. It is not supported on Windows or Android devices.

To download the Guides:

- Click on the link above.
- Scroll down the page to **Tunnel** and click on the title.
- Under the appropriate version, select the needed Guide.

The linked item will appear in a new browser window.

Tunnel (Android)

This VPN connection type is supported on Android devices only. It is not supported on iOS, macOS and Windows devices.

Tunnel (Samsung Knox Workspace)

This VPN connection type is supported on Android devices only. It is not supported on iOS, macOS and Windows devices.

Tunnel (Windows)

This VPN connection type is supported on Windows devices only. It is not supported on iOS, macOS and Android devices.

Use this setting to configure Tunnel VPN for Windows 10. For information on how to set up and configure Tunnel VPN for Tunnel for Windows 10, see the *Tunnel for Windows 10 Guide for Administrators* on the Ivanti Product Documentation page.

NetMotion Mobility VPN (iOS)

This VPN connection type is supported on iOS devices. It is not supported on macOS, Android and Windows devices.

OpenVPN

This VPN connection type is supported on Android devices. It is not supported on iOS, macOS, and Windows devices.

Palo Alto Networks GlobalProtect

This VPN connection type is supported on iOS, macOS, and Android devices. It is not supported on Windows devices.

PPTP

This VPN connection type is supported on iOS, macOS, Android, and Windows devices.

Use the following guidelines to configure the PPTP VPN connection type.

- "Proxy - None (default)" below
- "Proxy - Manual" on page 222
- "Proxy - Automatic" on page 224

Proxy - None (default)

Use the following guidelines to configure a PPTP VPN without a proxy.

TABLE 47. PROXY - NONE (DEFAULT) SETTINGS

Item	Description
Name	Enter a short phrase that identifies this VPN setting.
Description	Provide a description that clarifies the purpose of these settings.
Channel	For macOS only. Select one of the following distribution options: • Device channel - the configuration is effective for all users on a device. This is the typical option. • User channel - the configuration is effective only for the currently registered user on a device.
Connection Type	Select **PPTP**.
Server	Enter the IP address, hostname, or URL for the VPN server.
Proxy	**None** is the default setting. To configure a Manual or Automatic proxy, go to "Proxy - Manual" on the next page or "Proxy - Automatic" on page 224
Encryption Level	Select **None**, **Automatic** or **Maximum** (128 bit).
Domain	Specify the network domain.
Send all Traffic	Selecting this option protects data from being compromised, particularly on public networks.
User Name	Specify the user name to use (required.) The default value is $USERID$. Use this field to specify an alternate format, such as: $USERID$, $EMAIL$, $SAM_ACCOUNT_NAME$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$, $CUSTOM_DEVICE_Attributename$, $CUSTOM_USER_Attributename$, $NULL$ You can use combinations such as the following: • $USERID$:$EMAIL$ • $USERID$_$EMAIL$ Enter $NULL$ if you want the field presented to the user to be blank. Users will need to fill in the relevant username.

TABLE 47. PROXY - NONE (DEFAULT) SETTINGS (CONT.)

Item	Description
	ⓘ Some enterprises have a strong preference concerning which identifier is exposed.
User Authentication	Select the authentication method to use**:** **Password** or **RSA SecureID**.
Password	Specify the password to use (required.) The default value is $PASSWORD$. Include at least one of the following variables: $USERID$, $EMAIL$, $PASSWORD$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$, $CUSTOM_DEVICE_Attributename$, $CUSTOM_USER_ Attributename$, $NULL$ You can use combinations such as $EMAIL$:$PASSWORD$ Enter $NULL$ if you want the field presented to the user to be blank. Users will need to fill in the relevant password.

Proxy - Manual

Use the following guidelines to configure a PPTP VPN with a manual proxy.

TABLE 48. PROXY - MANUAL SETTINGS

Item	Description
Name	Enter a short phrase that identifies this VPN setting.
Description	Provide a description that clarifies the purpose of these settings.
Channel	For macOS only. Select one of the following distribution options: • Device channel - the configuration is effective for all users on a device. This is the typical option. • User channel - the configuration is effective only for the currently registered user on a device.
Connection Type	Select **PPTP**.
Server	Enter the IP address, hostname, or URL for the VPN server.

TABLE 48. PROXY - MANUAL SETTINGS (CONT.)

Item	Description
Proxy	Select **Manual**. To configure an automatic proxy, go to "Proxy - Automatic" on the next page
Proxy Server	Enter the name for the proxy server.
Proxy Server Port	Enter the port number for the proxy server.
Type	Select **Static** or **Variable** for the type of authentication to be used for the proxy server.
Proxy Server User Name	If the authentication type is **Static**, enter the username for the proxy server. If the authentication type is **Variable**, the default variable selected is $USERID$.
Proxy Server Password	If the authentication type is **Static**, enter the password for the proxy server. Confirm the password in the field below. If the authentication type is **Variable**, the default variable selected is $PASSWORD$.
Proxy Domains (iOS only)	This setting does not apply to Windows devices.
Encryption Level	Select **None**, **Automatic** or **Maximum** (128 bit).
Domain	Specify the network domain.
Send all Traffic	Selecting this option protects data from being compromised, particularly on public networks.
Username	Specify the user name to use (required.) The default value is $USERID$. Use this field to specify an alternate format, such as: $USERID$, $EMAIL$, $SAM_ACCOUNT_NAME$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$, $CUSTOM_DEVICE_Attributename$, $CUSTOM_USER_Attributename$, $NULL$ You can use combinations such as the following: • $USERID$:$EMAIL$ • $USERID$_$EMAIL$ Enter $NULL$ if you want the field presented to the user to be blank. Users will need to fill in the relevant username.

TABLE 48. PROXY - MANUAL SETTINGS (CONT.)

Item	Description
	ⓘ Some enterprises have a strong preference concerning which identifier is exposed.
User Authentication	Select the authentication method to use**:** **Password** or **RSA SecureID**.
Password	Specify the password to use (required.) The default value is $PASSWORD$. Include at least one of the following variables: $USERID$, $EMAIL$, $PASSWORD$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$, $CUSTOM_DEVICE_Attributename$, $CUSTOM_USER_Attributename$, $NULL$ You can use combinations such as $EMAIL$:$PASSWORD$ Enter $NULL$ if you want the field presented to the user to be blank. Users will need to fill in the relevant password.

Proxy - Automatic

Use the following guidelines to configure a PPTP VPN with an automatic proxy.

TABLE 49. PROXY - AUTOMATIC SETTINGS

Item	Description
Name	Enter a short phrase that identifies this VPN setting.
Description	Provide a description that clarifies the purpose of these settings.
Channel	For macOS only. Select one of the following distribution options: • Device channel - the configuration is effective for all users on a device. This is the typical option. • User channel - the configuration is effective only for the currently registered user on a device.
Connection Type	Select **PPTP**.
Server	Enter the IP address, hostname, or URL for the VPN server.

Table 49. Proxy - Automatic settings (Cont.)

Item	Description
Proxy	Select **Automatic**. To configure a manual proxy, go to "Proxy - Manual" on page 222.
Proxy Server URL	Enter the URL for the proxy server. Enter the URL of the location of the proxy auto-configuration file.
Proxy Domains (iOS only)	This setting does not apply to Windows devices.
Encryption Level	Select **None**, **Automatic** or **Maximum** (128 bit).
Domain	Specify the network domain.
Send all Traffic	Selecting this option protects data from being compromised, particularly on public networks.
Username	Specify the user name to use (required.) The default value is $USERID$. Use this field to specify an alternate format, such as: $USERID$, $EMAIL$, $SAM_ACCOUNT_NAME$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$, $CUSTOM_DEVICE_Attributename$, $CUSTOM_USER_Attributename$, $NULL$ You can use combinations such as the following: • $USERID$:$EMAIL$ • $USERID$_$EMAIL$ Enter $NULL$ if you want the field presented to the user to be blank. Users will need to fill in the relevant username. ⓘ Some enterprises have a strong preference concerning which identifier is exposed.
User Authentication	Select the authentication method to use**: Password** or **RSA SecureID**.
Password	Specify the password to use (required.) The default value is $PASSWORD$. Include at least one of the following variables: $USERID$, $EMAIL$, $PASSWORD$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$, $CUSTOM_DEVICE_Attributename$, $CUSTOM_USER_Attributename$, $NULL$ You can use combinations such as $EMAIL$:$PASSWORD$

TABLE 49. PROXY - AUTOMATIC SETTINGS (CONT.)

Item	Description
	Enter $NULL$ if you want the field presented to the user to be blank. Users will need to fill in the relevant password.

Pulse Secure SSL

This VPN connection type is supported on iOS, macOS, Android, and Windows devices.

Ivanti recommends using the Pulse Secure SSL connection type instead of Juniper SSL.

Use the following guidelines to configure Pulse Secure SSL VPN.

- "Proxy - None (default)" below
- "Proxy - Manual" on page 228
- "Proxy - Automatic" on page 231

Within these selections, you may make settings for:

- "Windows Configuration" on page 232
- "Custom Data" on page 233

Proxy - None (default)

Use the following guidelines to configure a Pulse Secure SSL VPN without a proxy.

TABLE 50. PROXY - NONE (DEFAULT) SETTINGS

Item	Description
Name	Enter a short phrase that identifies this VPN setting.
Description	Provide a description that clarifies the purpose of these settings.
Channel	For macOS only. Select one of the following distribution options: • Device channel - the configuration is effective for all users on a device. This is the typical option.

TABLE 50. PROXY - NONE (DEFAULT) SETTINGS (CONT.)

Item	Description
	- User channel - the configuration is effective only for the currently registered user on a device.
Connection Type	Select **Pulse Secure SSL**.
Samsung Knox	This setting applies to Android devices only.
Deploy inside Knox Workspace	This setting applies to Android devices only.
Server	Enter the IP address, hostname, or URL for the VPN server.
Proxy	**None** is the default setting. To configure a Manual or Automatic proxy, go to "Proxy - Manual" on the next page or "Proxy - Automatic" on page 231.
Username	Enter a value for the username (required.) The default value is $USERID$. Include at least one of the following variables: $USERID$, $EMAIL$, $SAM_ACCOUNT_NAME$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$, $CUSTOM_DEVICE_Attributename$, $CUSTOM_USER_Attributename$, $NULL$ You can use combinations such as the following: - $USERID$:$EMAIL$ - $USERID$_$EMAIL$ Enter $NULL$ if you want the field presented to the user to be blank. Users will need to fill in the relevant username.
User Authentication	Select the user authentication to use: - Password - see next row for information. - Certificate - If you select Certificate, select the identity certificate to be used as the account credential. If you select Certificate, and extended authentication (EAP) is not used, this certificate will be sent out for IKE client authentication. If extended authentication is used, this certificate can be used for EAP-TLS.

TABLE 50. PROXY - NONE (DEFAULT) SETTINGS (CONT.)

Item	Description
Password	Specify the password to use (required.) The default value is $PASSWORD$. Use this field to specify a custom format, such as $PASSWORD$_$USERID$. Include at least one of the following variables: $USERID$, $EMAIL$, $PASSWORD$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$, $CUSTOM_DEVICE_Attributename$, $CUSTOM_USER_Attributename$, $NULL$ You can use combinations such as $EMAIL$:$PASSWORD$ Enter $NULL$ if you want the field presented to the user to be blank. Users will need to fill in the relevant password.
Role	Specify the Pulse user role to use as a restriction.
Realm	Specify the Pulse realm to use as a restriction.
VPN On Demand	This setting does not apply to Windows devices.
Per-app VPN	This setting does not apply to Windows devices.
Provider Type	This setting applies to iOS and macOS devices only.

Continue with "Windows Configuration" on page 232.

Continue with "Custom Data" on page 233.

Proxy - Manual

Use the following guidelines to configure a Pulse Secure SSL VPN with a manual proxy.

TABLE 51. PROXY - MANUAL SETTINGS

Item	Description
Name	Enter a short phrase that identifies this VPN setting.
Description	Provide a description that clarifies the purpose of these settings.
Channel	For macOS only. Select one of the following distribution options: • Device channel - the configuration is effective for all users on a device. This is the typical option.

TABLE 51. PROXY - MANUAL SETTINGS (CONT.)

Item	Description
	• User channel - the configuration is effective only for the currently registered user on a device.
Connection Type	Select **Pulse Secure SSL**.
Samsung Knox	This setting applies to Android devices only.
Deploy inside Knox Workspace	This setting applies to Android devices only.
Server	Enter the IP address, hostname, or URL for the VPN server.
Proxy	Select **Manual**. To configure an automatic proxy, go to "Proxy - Automatic" on page 231.
Proxy Server	Enter the name for the proxy server.
Proxy Server Port	Enter the port number for the proxy server.
Type	Select **Static** or **Variable** for the type of authentication to be used for the proxy server.
Proxy Server User Name	If the authentication type is **Static**, enter the username for the proxy server. If the authentication type is **Variable**, the default variable selected is $USERID$.
Proxy Server Password	If the authentication type is **Static**, enter the password for the proxy server. Confirm the password in the field below. If the authentication type is **Variable**, the default variable selected is $PASSWORD$.
Proxy Domains (iOS only)	This field applies to iOS and macOS devices only.
Username	Enter a value for the username (required.) The default value is $USERID$. Include at least one of the following variables: $USERID$, $EMAIL$, $SAM_ACCOUNT_NAME$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$, $CUSTOM_DEVICE_Attributename$, $CUSTOM_USER_Attributename$, $NULL$ You can use combinations such as the following: • $USERID$:$EMAIL$ • $USERID$_$EMAIL$

TABLE 51. PROXY - MANUAL SETTINGS (CONT.)

Item	Description
	Enter $NULL$ if you want the field presented to the user to be blank. Users will need to fill in the relevant username.
User Authentication	Select the user authentication to use: • Password - see next row for information. • Certificate - If you select Certificate, select the identity certificate to be used as the account credential. If you select Certificate, and extended authentication (EAP) is not used, this certificate will be sent out for IKE client authentication. If extended authentication is used, this certificate can be used for EAP-TLS.
Password	Specify the password to use (required.) The default value is $PASSWORD$. Use this field to specify a custom format, such as $PASSWORD$_$USERID$. Include at least one of the following variables: $USERID$, $EMAIL$, $PASSWORD$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$, $CUSTOM_DEVICE_Attributename$, $CUSTOM_USER_ Attributename$, $NULL$ You can use combinations such as $EMAIL$:$PASSWORD$ Enter $NULL$ if you want the field presented to the user to be blank. Users will need to fill in the relevant password.
Role	Specify the Pulse user role to use as a restriction.
Realm	Specify the Pulse realm to use as a restriction.
VPN On Demand	This setting does not apply to Windows devices.
Per-app VPN	This setting does not apply to Windows devices.
Provider Type	This setting applies to iOS and macOS devices only.

Continue with "Windows Configuration" on page 232.

Continue with "Custom Data" on page 233.

Proxy - Automatic

Use the following guidelines to configure a Pulse Secure SSL VPN with an automatic proxy.

TABLE 52. PROXY - AUTOMATIC SETTINGS

Item	Description
Name	Enter a short phrase that identifies this VPN setting.
Description	Provide a description that clarifies the purpose of these settings.
Channel	For macOS only. Select one of the following distribution options: • Device channel - the configuration is effective for all users on a device. This is the typical option. • User channel - the configuration is effective only for the currently registered user on a device.
Connection Type	Select **Pulse Secure SSL**.
Samsung Knox	This setting applies to Android devices only.
Deploy inside Knox Workspace	This setting applies to Android devices only.
Server	Enter the IP address, hostname, or URL for the VPN server.
Proxy	Select **Automatic**. To configure a manual proxy, go to "Proxy - Manual" on page 228
Proxy Server URL	Enter the URL for the proxy server. Enter the URL of the location of the proxy auto-configuration file.
Proxy Domains (iOS only)	This setting applies to iOS and macOS devices only.
Username	Enter a value for the username (required.) The default value is $USERID$. Include at least one of the following variables: $USERID$, $EMAIL$, $SAM_ACCOUNT_NAME$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$, $CUSTOM_DEVICE_Attributename$, $CUSTOM_USER_Attributename$, $NULL$ You can use combinations such as the following: • $USERID$:$EMAIL$ • $USERID$_$EMAIL$

TABLE 52. PROXY - AUTOMATIC SETTINGS (CONT.)

Item	Description
	Enter $NULL$ if you want the field presented to the user to be blank. Users will need to fill in the relevant username.
User Authentication	Select the user authentication to use: • Password - see next row for information. • Certificate - If you select Certificate, select the identity certificate to be used as the account credential. If you select Certificate, and extended authentication (EAP) is not used, this certificate will be sent out for IKE client authentication. If extended authentication is used, this certificate can be used for EAP-TLS.
Password	Specify the password to use (required.) The default value is $PASSWORD$. Use this field to specify a custom format, such as $PASSWORD$_$USERID$. Include at least one of the following variables: $USERID$, $EMAIL$, $PASSWORD$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$, $CUSTOM_DEVICE_Attributename$, $CUSTOM_USER_Attributename$, $NULL$ You can use combinations such as $EMAIL$:$PASSWORD$ Enter $NULL$ if you want the field presented to the user to be blank. Users will need to fill in the relevant password.
Role	Specify the Pulse user role to use as a restriction.
Realm	Specify the Pulse realm to use as a restriction.
VPN On Demand	This setting does not apply to Windows devices.
Per-app VPN	This setting does not apply to Windows devices.
Provider Type	This setting applies to iOS and macOS devices only.

Continue with "Windows Configuration" below.

Continue with "Custom Data" on the next page.

Windows Configuration

Allowed Secured Resources (Windows Phone only)

Excluded Secured Resources (Windows Phone only)

See "Application-triggered VPN for Windows devices" on page 243 for information on how to configure these settings to set up application-triggered VPN for 8.0.1 devices.

TABLE 53. WINDOWS CONFIGURATIONS

Item	Description
Windows Configuration	Enter the secured resources (domains, IP ranges, or apps) used by the **Send All Traffic** option.
Always On	Select this option to keep the VPN on. **Lock Down** supersedes this option for Windows devices.
Lock Down	You cannot change the assigned settings unless 1) the **Lock Down** setting is removed from the profile and the new profile is pushed to the device or 2) the device is un-enrolled from Core. This option supersedes the **Always On** option.

Custom Data

- **Add+** - Click to add a new key / value pair.
- **Key / Value** - Enter the Key / value pairs necessary to configure the VPN setting. The app creator should provide the necessary key / value pairs.

Samsung Knox IPsec

This VPN connection type is supported on Android devices. It is not supported on iOS, macOS, and Windows devices.

SonicWall Mobile Connect

This VPN connection type is supported on iOS, macOS, and Windows devices. It is not supported on Android devices.

Use the following guidelines to configure a SonicWall Mobile Connect VPN.

- "Proxy - None (default)" on the next page
- "Proxy - Manual " on page 235
- "Proxy - Automatic" on page 239

Within these selections, you may make settings for:

- "Windows Configuration" on page 243
- "Custom Data" on page 243

Proxy - None (default)

Use the following guidelines to configure a SonicWall Mobile VPN connection without a proxy.

TABLE 54. PROXY - NONE SETTINGS

Item	Description
Name	Enter a short phrase that identifies this VPN setting.
Description	Provide a description that clarifies the purpose of these settings.
Channel	For macOS only. Select one of the following distribution options: • Device channel - the configuration is effective for all users on a device. This is the typical option. • User channel - the configuration is effective only for the currently registered user on a device.
Connection Type	Select **SonicWall Mobile Connect**.
Server	Enter the IP address, hostname, or URL for the VPN server.
Proxy	**None** is the default setting. To configure a Manual or Automatic proxy, go to "Proxy - Manual " on the next page or "Proxy - Automatic" on page 239
Username	Specify the user name to use (required.) The default value is $USERID$. Use this field to specify an alternate format, such as: $USERID$, $EMAIL$, $SAM_ACCOUNT_NAME$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$, $CUSTOM_DEVICE_Attributename$, $CUSTOM_USER_Attributename$, $NULL$ You can use combinations such as the following: • $USERID$:$EMAIL$ • $USERID$_$EMAIL$

TABLE 54. PROXY - NONE SETTINGS (CONT.)

Item	Description
	Enter $NULL$ if you want the field presented to the user to be blank. Users will need to fill in the relevant username. ⓘ Some enterprises have a strong preference concerning which identifier is exposed.
User Authentication	Select the user authentication to use: • Password - see next row for information. • Certificate - If you select Certificate, select the identity certificate to be used as the account credential.
Password	Specify the password to use (required.) The default value is $PASSWORD$. Include at least one of the following variables: $USERID$, $EMAIL$, $PASSWORD$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$, $CUSTOM_DEVICE_Attributename$, $CUSTOM_USER_Attributename$, $NULL$ You can use combinations such as $EMAIL$:$PASSWORD$ Enter $NULL$ if you want the field presented to the user to be blank. Users will need to fill in the relevant password.

Continue to "Windows Configuration" on page 243

Continue to "Custom Data" on page 243.

Proxy - Manual

Use the following guidelines to configure a SonicWall Mobile VPN connection with a manual proxy.

TABLE 55. PROXY - MANUAL SETTINGS

Item	Description
Name	Enter a short phrase that identifies this VPN setting.
Description	Provide a description that clarifies the purpose of these settings.
Channel	For macOS only. Select one of the following distribution options:

TABLE 55. PROXY - MANUAL SETTINGS (CONT.)

Item	Description
	• Device channel - the configuration is effective for all users on a device. This is the typical option. • User channel - the configuration is effective only for the currently registered user on a device.
Connection Type	Select **SonicWall Mobile Connect**.
Server	Enter the IP address, hostname, or URL for the VPN server.
Proxy	Select **Manual**. To configure an Automatic proxy, go to "Proxy - Automatic" on page 239
Proxy Server	Enter the name for the proxy server.
Proxy Server Port	Enter the port number for the proxy server.
Type	Select **Static** or **Variable** for the type of authentication to be used for the proxy server.
Proxy Server User Name	If the authentication type is **Static**, enter the username for the proxy server. If the authentication type is **Variable**, the default variable selected is $USERID$.
Proxy Server Password	If the authentication type is **Static**, enter the password for the proxy server. Confirm the password in the field below. If the authentication type is **Variable**, the default variable selected is $PASSWORD$.
Proxy Domains (iOS only)	This field is applicable to iOS only. The VPN will only proxy for the domain and domain suffixes specified here (`.com` and `.org` are examples of top-level domain suffixes). Domain suffixes can be used to match multiple domains. For example, `.com` would include all `.com` domains, and `example.com` would include all domains ending in example.com, such as `pages.example.com` and `mysite.example.com`. Wildcards are not supported. Click **Add+** to add a domain.
Username	Specify the user name to use (required.) The default value is $USERID$. Use this field to specify an alternate format, such as:

TABLE 55. PROXY - MANUAL SETTINGS (CONT.)

Item	Description
	$USERID$, $EMAIL$, $SAM_ACCOUNT_NAME$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$, $CUSTOM_DEVICE_Attributename$, $CUSTOM_USER_Attributename$, $NULL$ You can use combinations such as the following: • $USERID$:$EMAIL$ • $USERID$_$EMAIL$ Enter $NULL$ if you want the field presented to the user to be blank. Users will need to fill in the relevant username. ⓘ Some enterprises have a strong preference concerning which identifier is exposed.
User Authentication	Select the user authentication to use: • Password - see next row for information. • Certificate - If you select Certificate, select the identity certificate to be used as the account credential.
Password	Specify the password to use (required.) The default value is $PASSWORD$. Include at least one of the following variables: $USERID$, $EMAIL$, $PASSWORD$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$, $CUSTOM_DEVICE_Attributename$, $CUSTOM_USER_Attributename$, $NULL$ You can use combinations such as $EMAIL$:$PASSWORD$ Enter $NULL$ if you want the field presented to the user to be blank. Users will need to fill in the relevant password.
Login Group or Domain	The LDAP group or domain associated with users.
VPN on Demand	This setting applies to iOS and macOS devices only. Select to enable VPN On Demand. The "SonicWall Mobile Connect" on page 233 field displays. On Demand rules are associated with an array of dictionaries that define the network match criteria identifying a particular network location.

TABLE 55. PROXY - MANUAL SETTINGS (CONT.)

Item	Description
	VPN On Demand matches the dictionaries in the On Demand Rules against properties of your current network connection to determine whether domain-based rules should be used in determining whether to connect, then handles the connection as follows: • If domain-based matching is enabled for a matching On Demand Rule dictionary, then for each dictionary in that dictionary’s connection evaluation array, VPN On Demand compares the requested domain against the domains listed in the Domains array. • If domain-based matching is not enabled, the specified behavior (Connect, Disconnect, Allow, or Ignore) is used if the dictionary otherwise matches. VPN On Demand rules are applied when the device's primary network interface changes, for example when the device switches to a different Wi-Fi network. • A matching rule is not required. The Default Rule is applied if a matching rule is not defined. • If you select Evaluate Connection, a matching rule is not required. • You can create up to 10 On Demand matching rules. • For each matching rule you can create up to 50 Type and Value pairs.
Per-app VPN	Select **Yes** to create a per-app VPN setting. An additional license may be required for this feature. The Provider Type field displays. Per-app VPN is supported on iOS devices version 9.0 or supported newer versions. You cannot delete a per-app VPN setting that is being used by an app. Remove the per-app VPN setting from the app before you delete the setting.

TABLE 55. PROXY - MANUAL SETTINGS (CONT.)

Item	Description
	You can enable per-app VPN for an app when you: • add the app in the App Catalog. • edit an in-house app or an App Store app in the App Catalog. ⓘ When multiple labels are assigned to associate the selected VPN configurations in the Per-App VPN section, then VPN prioritization will happen in the order of the selected list. See the *Core Apps@Work Guide* for information about how to add or edit apps.
Provider Type	If Per-App VPN is set to Yes, define whether the per-app VPN service will tunnel traffic at the application layer (**app-proxy**) or the IP layer (**packet-tunnel**). Select **app-proxy** (default) or **packet-tunnel**.

Continue to "Windows Configuration" on page 243

Continue to "Custom Data" on page 243.

Proxy - Automatic

Use the following guidelines to configure a SonicWall Mobile VPN connection with an automatic proxy.

TABLE 56. PROXY - AUTOMATIC SETTINGS

Item	Description
Name	Enter a short phrase that identifies this VPN setting.
Description	Provide a description that clarifies the purpose of these settings.
Channel	For macOS only. Select one of the following distribution options: • Device channel - the configuration is effective for all users on a device. This is the typical option. • User channel - the configuration is effective only for the currently registered user on a device.

TABLE 56. PROXY - AUTOMATIC SETTINGS (CONT.)

Item	Description
Connection Type	Select **SonicWall Mobile Connect**.
Server	Enter the IP address, hostname, or URL for the VPN server.
Proxy	Select **Automatic**. To configure a manual proxy, go to "Proxy - Manual " on page 235
Proxy Server URL	Enter the URL for the proxy server. Enter the URL of the location of the proxy auto-configuration file.
Proxy Domains (iOS only)	This field is applicable to iOS only. The VPN will only proxy for the domain and domain suffixes specified here (`.com` and `.org` are examples of top-level domain suffixes). Domain suffixes can be used to match multiple domains. For example, `.com` would include all `.com` domains, and `example.com` would include all domains ending in example.com, such as `pages.example.com` and `mysite.example.com`. Wildcards are not supported. Click **Add+** to add a domain.
Username	Specify the user name to use (required.) The default value is $USERID$. Use this field to specify an alternate format, such as: $USERID$, $EMAIL$, $SAM_ACCOUNT_NAME$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$, $CUSTOM_DEVICE_Attributename$, $CUSTOM_USER_Attributename$, $NULL$ You can use combinations such as the following: • $USERID$:$EMAIL$ • $USERID$_$EMAIL$ Enter $NULL$ if you want the field presented to the user to be blank. Users will need to fill in the relevant username. ⓘ Some enterprises have a strong preference concerning which identifier is exposed.
User Authentication	Select the user authentication to use: • Password - see next row for information.

TABLE 56. PROXY - AUTOMATIC SETTINGS (CONT.)

Item	Description
	• Certificate - If you select Certificate, select the identity certificate to be used as the account credential.
Password	Specify the password to use (required.) The default value is $PASSWORD$. Include at least one of the following variables: $USERID$, $EMAIL$, $PASSWORD$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$, $CUSTOM_DEVICE_Attributename$, $CUSTOM_USER_Attributename$, $NULL$ You can use combinations such as $EMAIL$:$PASSWORD$ Enter $NULL$ if you want the field presented to the user to be blank. Users will need to fill in the relevant password.
Login Group or Domain	The LDAP group or domain associated with users.
VPN on Demand	This setting applies to iOS and macOS devices only. Select to enable VPN On Demand. The "SonicWall Mobile Connect" on page 233 field displays. On Demand rules are associated with an array of dictionaries that define the network match criteria identifying a particular network location. VPN On Demand matches the dictionaries in the On Demand Rules against properties of your current network connection to determine whether domain-based rules should be used in determining whether to connect, then handles the connection as follows: • If domain-based matching is enabled for a matching On Demand Rule dictionary, then for each dictionary in that dictionary's connection evaluation array, VPN On Demand compares the requested domain against the domains listed in the Domains array. • If domain-based matching is not enabled, the specified behavior (Connect, Disconnect, Allow, or Ignore) is used if the dictionary otherwise matches. VPN On Demand rules are applied when the device's primary network interface changes, for example when the device switches to a different Wi-Fi network.

TABLE 56. PROXY - AUTOMATIC SETTINGS (CONT.)

Item	Description
	• A matching rule is not required. The Default Rule is applied if a matching rule is not defined. • If you select Evaluate Connection, a matching rule is not required. • You can create up to 10 On Demand matching rules. • For each matching rule you can create up to 50 Type and Value pairs.
Per-app VPN	Select **Yes** to create a per-app VPN setting. An additional license may be required for this feature. The Provider Type field displays. Per-app VPN is supported on iOS devices version 9.0 or supported newer versions. You cannot delete a per-app VPN setting that is being used by an app. Remove the per-app VPN setting from the app before you delete the setting. You can enable per-app VPN for an app when you: • add the app in the App Catalog. • edit an in-house app or an App Store app in the App Catalog. ⓘ When multiple labels are assigned to associate the selected VPN configurations in the Per-App VPN section, then VPN prioritization will happen in the order of the selected list. See the *Core Apps@Work Guide* for information about how to add or edit apps.
Provider Type	If Per-App VPN is set to Yes, define whether the per-app VPN service will tunnel traffic at the application layer (**app-proxy**) or the IP layer (**packet-tunnel**). Select **app-proxy** (default) or **packet-tunnel**.

Continue to "Windows Configuration" on the next page

Continue to "Custom Data" on the next page.

Windows Configuration

Allowed Secured Resources (Windows Phone only)
Excluded Secured Resources (Windows Phone only)

See "Application-triggered VPN for Windows devices" below for information on how to configure these settings to set up application-triggered VPN for 8.0.1 devices.

TABLE 57. WINDOWS CONFIGURATIONS

Item	Description
Windows Configuration	Enter the secured resources (domains, IP ranges, or apps) used by the **Send All Traffic** option.
Always On	Select this option to keep the VPN on. **Lock Down** supersedes this option for Windows devices.
Lock Down	You cannot change the assigned settings unless 1) the **Lock Down** setting is removed from the profile and the new profile is pushed to the device or 2) the device is un-enrolled from Core. This option supersedes the **Always On** option.

Custom Data

- **Add+** - Click to add a new key / value pair.
- **Key / Value** - Enter the Key / value pairs necessary to configure the VPN setting. The app creator should provide the necessary key / value pairs.

Custom SSL

This VPN connection type is supported on iOS devices. It is not supported on macOS, Android, and Windows devices.

Application-triggered VPN for Windows devices

Administrators can choose to specify what applications trigger a VPN connection and what applications do not. Core exposes all key-value pairs for app triggers and app filters rules to provide administrators with the ability to manually add AppTrigger rules separately from rather than TrafficFilter rules, rather than automatically being added whenever a TrafficFilter rule was applied to an application.

Previous to the Core 9.2.0.0 release, Core automatically added an AppTrigger rule whenever adding the TrafficFilter rule, without also including the AppTrigger in the Admin Portal. As of 9.2.0.0, if you set up VPN profiles in previous releases these profiles will not change, but Core automatically adds the AppTrigger rule that it added in the background with the TrafficFilter rule. Both are included in the **Policies & Configs > Configurations > Add New > VPN > Custom Data** table.

With this separation between AppTrigger and TrafficFilter rules, you can remove a rule if you do not want to trigger the VPN on an application. While existing profiles will not change, you can modify existing rules or configure them to separate between trigger and filter.

Configuring VPNs triggers

Use these steps to set up VPN triggers by connecting AppTrigger with TrafficFilter rules.

To configure VPN triggers:

1. Log into the Admin Portal.
2. Go to **Policies and Configs** > **Configurations**.
3. Click **Add New** > **VPN**.
4. Scroll to the **Custom Data** section.
5. Enter a TrafficFilter rule in the **KEY** column.
6. Enter the application to trigger the VPN in the **VALUE** column.
7. Enter an AppTrigger to pair with the TrafficFilter.
8. Enter the same application in the VALUE column.
9. Click **Save**.

How to set up exclusions for VPN traffic

If the VPN configuration is set up to send all traffic through VPN, you can configure exclusions.

To exclude traffic from using VPN:

1. In the Admin Portal, go to **Policies and Configs** > **Configurations**.
2. Click **Add New** > **VPN**, or select an existing VPN setting to **Edit**.

3. Ensure that **Send All Traffic** is checked.
4. In the **Excluded Secured Resources (Windows Phone only)** section, click **Add +**.

   Create a separate entry for each domain name, IP range, or app.
5. Enter the following information:

Item	Description
Secured Resources	Enter one of the following: • Domain name: Apps connecting to the domain name will be excluded from using the VPN connection. Wildcard '*' prefix is required. Example: *.corp.example.com We also strongly suggest to add *.*yourcoredomain*.com to the exclusion list. This excludes the use of VPN when the device connects to Core. If your Core domain is not in the exclusion list, and the device fails to establish a VPN connection, the device will not be able to connect to Core. • Valid IP range: Enter IP range. Apps connecting to an IP address in the range will be excluded from using the VPN connection. You must enter a valid IP range. Example: 192.0.2.0/24 • App GUI ID: Enter the GUID for the app. Traffic from the app will be excluded from using the VPN connection.
Description	Enter a description for the secure resource.

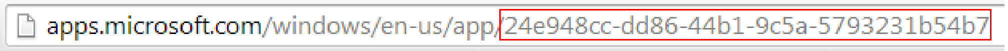
6. Click **Save**.

How to get the app GUID for a Windows Phone 8.1 device app

To get the app GUID for a 8.1 app:

1. Go to the Windows Phone 8.1 app store.
2. Search and click on the app for which you want the app GUID.

   The app GUID is the numbers and letters in the tail end of the URL, in the address bar of the app details page.



apps.microsoft.com/windows/en-us/app/24e948cc-dd86-44b1-9c5a-5793231b54b7

Azure Services

This section addresses the different Azure services that Core supports.

- "Azure Services Overview" below
- "Register devices in AAD and MDM" below
- "Join Azure and Core for Windows 10" on page 250
- "Windows Information Protection" on page 254
- "Business Store Portal" on page 261
- "Windows PIN management for PassPort For Work/Windows Hello" on page 264
- "Windows license management" on page 268

Azure Services Overview

This chapter describes the Azure services that Core supports. For all Azure services, you need to set up your system both within Core and using 3rd party tools and websites. This chapter describes the prerequisites for using any Azure service with Core, as well as how to configure these services.

Standard prerequisites for all Azure services

Ivanti recommends you have met the following prerequisites before setting up any Azure service:

- A Premier license for Azure Active Directory
- Azure tenant for Azure Active Directory
- Azure user for Azure Active Directory.

Register devices in AAD and MDM

The documentation provided below, can be given to your employees with little or no modifications. Once the device user completes the registration process, both the user and the device are registered and you can track compliance.

These steps can change without notice. Contact Microsoft for the most up-to-date instructions.

The registration step to tracking compliance is for the device user to configure Azure Active Directory (AAD) registration on the enterprise-owned device. Use the following scenarios to register the devices in AAD and MDM:

- "OOBE sign up for AAD enrollment" below (first time set up)
- "Post OOBE sign up for AAD enrollment" on the next page (enterprise-owned not OOBE)
- "Workplace sign up for AAD enrollment" on the next page (employee-owned not OOBE)
- "Terms of Service Customization" on the next page (customize the Terms of Service page)

OOBE sign up for AAD enrollment

When a device is registered for the first time, the user will answer a few questions about the device. The AAD registration begins here.

1. Indicate who owns the device by making one of the following selections:
2. **My organization**
    - I own it
    - Click **Next**.
3. Select **Join Azure AD** > **Next**.
4. Enter your enterprise user name and password.
5. Use the same credentials you use to log into your enterprise’s Office 365. Contact your administrator, if you cannot sign in for any reason.
6. Click **Sign In** to connect to both Azure and the Core.
7. Read the MDM terms and conditions.
8. Click **Accept** to complete registration into Azure and MDM.
9. Microsoft requires pin registration for all AAD devices.
10. Enter a PIN and click **OK**.
11. In addition to the **Set up a Pin** screen, some users will be asked to verify that they are the correct user. This verification screen does not appear for all users. The User and device is now registered and can be used both by Azure and MDM. Compliance can now be tracked.

Post OOBE sign up for AAD enrollment

Device users can follow this procedure for company-owned devices that are not OOBE devices.

1. Click **Start** > **Settings** > **Accounts**.
2. Click **Access Work or School**.
3. Click **+Connect**.
4. Enter your enterprise email address in the text box.
5. Click **Next**.
6. Enter your enterprise user name and password.
7. Use the same credentials you use to log into your enterprise's Office 365. Contact your administrator, if you cannot sign in for any reason.
8. Click **Sign in** to register your device and verify that it can be signed up for MDM service.

Workplace sign up for AAD enrollment

Device users can follow this procedure for BYOD devices.

1. Click **Start** > **Settings** > **Accounts**.
2. Click **Access Work or School**.
3. Click **+Connect**.
4. Go to the **Alternate actions** section and click **Join this device to Azure Active Directory**.
5. Enter your enterprise user name and password.
6. Use the same credentials you use to log into your enterprise's Office 365. Contact your administrator, if you cannot sign in for any reason.
7. Click **Sign in** to register your device and verify that it can be signed up for MDM service.

Terms of Service Customization

Administrators can customize their Core Terms of Service pages for users with new Azure Active Directory registration.

To customize the Terms of Service page:

1. Log into the Admin Portal.
2. Click **Settings** > **System Settings** > **Users & Devices** > **Registration**.
3. Scroll to the **End User Terms of Service** section and click **Add+**.
4. Select a language.
5. Go to the **Type** field and select **AAD Enrollment**.
6. Customize the header text.
7. Add customized text in the **Agreement Content** box.
8. Click **Save > Save**.

   Users with new AAD registration will see this new Terms of Service page.

Join Azure and Core for Windows 10

This section describes how to set up Azure and Core platforms to share data about device compliance. Administrators use shared compliance information to set up rules for blocking access to applications (Office 365, for example) until the device is in compliance.

Prerequisites for joining Azure and Core

We recommend you have met the following prerequisites before starting this section:

- "Standard prerequisites for all Azure services" on page 247

Join Azure and Core work flow

This section describes the overall work flow for joining Azure and Core for Windows 10 devices:

- "Set up Azure to join with Core" below
- "Set up Core to join with Azure" on page 253
- "Manage device compliance" on page 254

Set up Azure to join with Core

The first step is to Set up Azure to join with Core.

To set up Core with Microsoft Azure Intune, see Azure Tenant.

These steps can change without notice. Contact Microsoft for the most up-to-date instructions.

Add the MDM application

Follow this procedure to add the Mobile Device Management (MDM) application to Azure.

1. Log into the Microsoft Azure portal.
2. In the left panel, click **Azure Active Directory**.
3. Click **Mobility (MDM and MAM)**.
4. Click **+ Add application**.
5. Select the generic On-premises MDM application.
6. Enter a unique name that can easily be remembered to associate with MDM sign up and then click Add.

   The app with the name you selected is added to a list of apps in the directory it was assigned.

   - Only one MDM vendor can be associated at a time.
   - If you add Intune, only Microsoft can remove the app manually.
   - You can have multiple on-premise MDM apps at the same time, but make sure these apps' user scopes do not overlap.
   - _MDM is used only for cloud customers.
7. Complete the steps in "Configure the application" below.

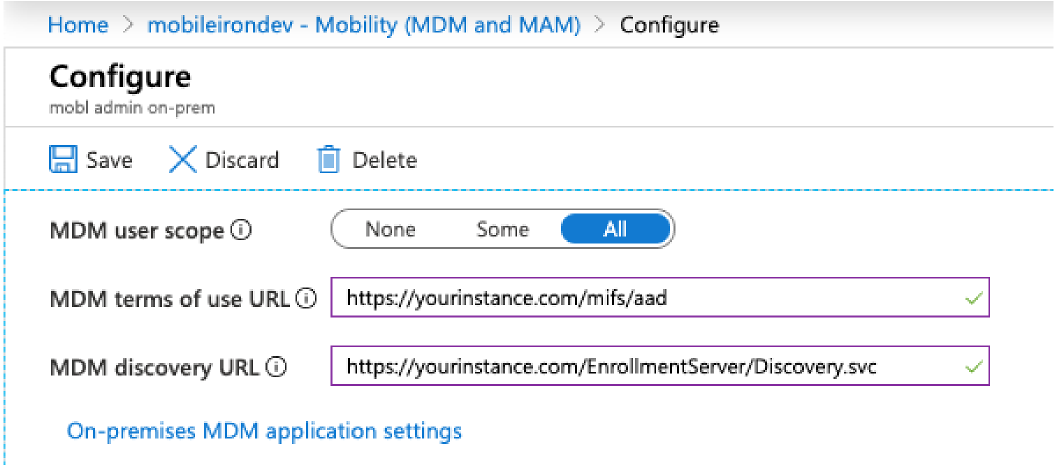
Configure the application

This procedure describes how administrators configure the settings required to connect to their instance of Core.

1. Open the MDM app you created.
2. On the Configure page, enter the URL of your Core instance into the following fields:
   - **MDM DISCOVERY URL**
   - **MDM TERMS OF USE URL**
3. Add */EnrollmentServer/Discovery.svc* after *.com* in the **MDM DISCOVERY URL** field.
4. Add *mifs/aad* after *.com* in the **MDM TERMS OF USE URL** field.

5. In the MDM user scope field, select **All** to apply configuration to all users. Select **Some** if you want to a specify a group (Additional fields will display.)

> Applying the configuration to **None** will negate using this app to any users in the directory and will bypass using Core for MDM management.



Home > mobileirondev - Mobility (MDM and MAM) > Configure

Configure

mobl admin on-prem

MDM user scope: None Some [✓ All]

MDM terms of use URL: https://yourinstance.com/mifs/aad

MDM discovery URL: https://yourinstance.com/EnrollmentServer/Discovery.svc

On-premises MDM application settings

6. Click the **On-premises MDM application** settings link.

7. In the Overview tab, click **Application ID URI** and in the new page, click **Edit** to enter the URL of your Core instance.

8. In the left panel, click **Authentication**.

9. Add a new entry of redirect URIs, select the web type, enter the URL of your Core instance for redirect URIs, and then click **Save**.

10. Copy the Application (client) ID. You will enter this into the **Azure Client ID** field in Core (see "Set up Core to join with Azure" on the next page).

11. In the left panel, click **Certificates and Secrets**.

12. To add a new key, click **+New client secret**.

13. Copy and save the new key. You will enter this into the **Azure Key** field in Core.

    - This key is also called a "client secret key" to the Application Client ID.
    - Select a 1- or 2-year activation period for the key.

- The key is not visible until the configuration is changed.
- The key is only visible after you save the configuration for the first time.
- You can generate a new key, for any reason, using the same steps.

14. In the left pane, click **API permissions**. Note that under Permissions, the AAD Graph Read / Write device permissions field is selected.
15. Click **+Add permissions**.
16. Select **Azure Service Management**.
17. In the Azure Service Management page, click **Delegated permissions**.
18. In the Permissions section, select the user_impersonation check box and then click **Add permission**.
19. Complete the steps in "Set up Core to join with Azure" below.

Set up Core to join with Azure

The second step is to join Azure with Core.

1. Log into the Core Admin Portal.
2. Select **Settings** > **System Settings** > **Windows** > **Advanced Menu**.
3. Select **Enable Microsoft Azure Menu**.

> ⓘ You do not need to turn on the **Enabling Custom SyncML Menu** option to work with Azure. However, if it was already turned on, do not turn it off as it might be required for other features in Core.

4. Click **Save**.
5. Click the **Systems Settings** tab.
6. In the left navigational pane, go to **Microsoft Azure** and expand the section. Alternately, find the Microsoft Azure tile on the Systems Settings page.
7. Click **Autopilot & Device Compliance for Windows**. The Autopilot & Device Compliance for Windows page opens.
8. Select the **Enable Azure Device Compliance** check box. New fields display below.

9. Enter the appropriate information for:

    - **Azure Domain ID** - The name of your Azure tenant.
    - **Azure Client ID** - the Client ID you noted from your Azure Configuration.
    - **Azure Key** - the key you noted from your Azure Configuration.

10. Click **Save**.

    You can edit the information at any time.

11. Provide your device users with the steps in "Register devices in AAD and MDM" on page 247.

12. Complete the steps in "Manage device compliance" below.

Manage device compliance

Finally, now that the device is managed, Core can begin to report compliance to Azure.

- Administrators can set up rules in Core to determine if a device is out of compliance.
- Core then sends that information to Azure, when a device becomes out of compliance.
- If an administrator sets up rules in Azure, they are put in place when the device is out of compliance.

Azure Compliance Setting

The **Trust Level**, in Azure, indicates if a device is compliant or not.

- **Compliant**: the device is compliant
- **Managed**: the device has fallen out of compliance

Windows Information Protection

As more enterprises take advantage of BYOD with Windows devices, the risk of accidental data leak through apps and services (email, social media, the public cloud) outside of an enterprise’s control increases. Windows Information Protection (WIP), previously known as Enterprise Data Protection (EDP), helps protect against this potential data leakage without otherwise interfering with the user experience.

This feature is supported on Windows 10 devices.

Recommendations for using WIP

We recommend you have met the following in place before starting this section (however they are not required):

- "Standard prerequisites for all Azure services" on page 247
- A DRA certificate (contact your Microsoft sales and services associate for more information or go here: https://docs.microsoft.com/en-us/windows/threat-protection/windows-information-protection/create-and-verify-an-efs-dra-certificate)

Verify WIP profiles

You can view a device to see if the required profile settings to use WIP are correct. Currently, there is no compliance based on these settings, however you do have the ability to verify that the device has the proper profiles.

To verify WIP profiles:

1. Go to **Device & Users> Devices**.
2. Select the device.
3. Click the **Policies** tab.
4. Scroll to the **WIP Policy2-3** section and expand, if necessary.
5. Review the **WIP** settings.
6. Verify that both **Setting Value** and **Device Value** are set to **On**.

   These must match to be compliant.

WIP work flow

This section describes the overall work flow for setting up WIP:

1. "Set up App Control rule" below
2. "Creating a Windows Information Protection policy" on the next page
3. "Apply the profile to a label" on page 261

Set up App Control rule

The App Control rule is a list of applications that can use and protect data with WIP. These apps will be a combination of enlightened and un-enlightened applications.

Enlightened applications are those apps that have been written to use the functions Microsoft has defined for use with WIP. These functions will help the application know the difference between:

- Business data
- Personal data

Otherwise, the application treats all data as business data.

Setting up an App Control rule

This procedure describes how to set up an App Control rule.

1. Select **Apps** > **App Control**> **Add**.
2. Select **WIP** as the **Type** and enter a name for the rule.
3. Enter the first application you want to be able to use WIP data, including the following fields:
   - App
   - **App Identifier/Name** (required)
   - **Device Platform** (required)
   - Comment
4. Click the green plus sign (+) to add additional applications, as necessary.
5. Click **Save**.

   Click **OK** in the **Success** window.
6. Complete the steps in "Creating a Windows Information Protection policy" below.

Creating a Windows Information Protection policy

To create a WIP policy:

1. Go to **Policies & Configs** > **Policies**.
2. Select **Add New** > **Windows** > **Windows Information Protection**.
3. Modify one or more of the fields, as necessary.

   Refer to the "Windows Information Protection Fields " on the next page table for details.
4. Click **Save** > **Apply** to save the changes.
5. Click **Save** again to save the WIP policy.

6. Complete the steps in "Apply the profile to a label" on page 261

7. See also the *Core Getting Started Guide* for details.

New Windows Information Protection window

The following table summarizes fields and descriptions in the **New Windows Information Protection** window:

TABLE 58. WINDOWS INFORMATION PROTECTION FIELDS

Fields	Description
Name	A name use to keep track of the profile in Core
Description	Describes the profile's purpose (optional)
App Control Group	Lists applications protected by this policy, as defined in the appropriate App Control rule. (See the *Device Management Guide for Windows Devices* for more information.)
Enforcement Level	Select one of the following enforcement modes: • **Block**: WIP looks for inappropriate data sharing practices and stops the employee from completing the action. This can include sharing info across non-enterprise-protected apps in addition to sharing enterprise data between other people and devices outside of your enterprise. • **Override**: WIP looks for inappropriate data sharing, warning employees if they do something deemed potentially unsafe. However, this management mode lets the employee override the policy and share the data, logging the action to your audit log. • Ivanti recommends that you start with **Override** while verifying with a small group that you have the right apps on your protected apps list. After you're done, you can select your final enforcement policy, either **Override** or **Block**. • **Silent**: WIP runs silently, logging inappropriate data sharing, without blocking anything that would've been prompted for employee interaction while in Override mode. Unallowed actions, like apps inappropriately trying to access a network resource or WIP-protected data, are still blocked. • **Off** (not recommended): WIP is turned off and doesn't help to protect or audit your data. After you turn off WIP, an attempt is made to decrypt any closed WIP-tagged files on the locally attached drives.
Enterprise Protected Domain Names	Enter your corporate identity.

TABLE 58. WINDOWS INFORMATION PROTECTION FIELDS (CONT.)

Fields	Description
	Corporate identity is usually expressed as your primary Internet domain (miacme.com, for example). It helps to identify and tag your corporate data from apps You have marked as protected by WIP. For example, emails using miacme.com are identified as being corporate and are restricted by your Windows Information Protection policies. You can specify multiple domains owned by your enterprise by separating them with the "|" character. For example, (miacme.com|newmiacme.com). With multiple domains, the first one is designated as your corporate identity and all of the additional ones as being owned by the first one. Ivanti strongly recommends that you include all of your email address domains in this list.
Enterprise Network Domain Names	Specify the DNS suffixes used in your environment. All traffic to the fully-qualified domains appearing in this list will be protected. This setting works with the IP ranges settings to detect whether a network endpoint is enterprise or personal on private networks. If you have multiple resources, you must separate them using the "," delimiter. For example "contoso.sharepoint.com,Fabrikam.com".
Enterprise Cloud Resources	Specify the cloud resources you want to be treated as corporate and protected by WIP. For each cloud resource, you can optionally specify a proxy server from your **Enterprise Internal Proxy Servers** list to route traffic for this cloud resource. Be aware that all traffic routed through your enterprise internal proxy servers is considered enterprise. If you have multiple resources, you must separate them using the "|" delimiter. If you don't use proxy servers, you must also include the "," delimiter just before the "|". For example: URL <,proxy>|URL <,proxy>. **Examples**: • "With proxy: "contoso.sharepoint.com,contoso.internalproxy1.com |contoso.visualstudio.com,contoso.internalproxy2.com" • "Without proxy: "contoso.sharepoint.com|contoso.visualstudio.com" There is a UI constraint of 64 chars. In the **Enterprise IP Range** field, specify the addresses for a valid IPv4 value range within your intranet. These addresses, used with your enterprise network domain names, define your corporate network boundaries. If you have multiple ranges, you must separate them using the "," delimiter

TABLE 58. WINDOWS INFORMATION PROTECTION FIELDS (CONT.)

Fields	Description
	Example: 3.4.0.1-3.4.255.254,10.0.0.1-10.255.255.254
Enterprise IP Ranges Are Authoritative	Click this box if you want Windows to treat the IP ranges you specified in the network boundary definition as the complete list of IP ranges available on your network. If you clear this box, Windows searches for additional IP ranges on any domain-joined devices connected to your network (auto-detect).
Data Recovery Certificate	Paste your Base64-encoded DRA certificate (.CER) string into the **Data Recovery Certificate** text box. After you create and deploy your WIP policy to your employees, Windows begins to encrypt your corporate data on the employees' local device drive. If the employees' local encryption keys get lost or revoked, the encrypted data can become unrecoverable. To help avoid this possibility, the DRA certificate lets Windows use an included public key to encrypt the local data, while you maintain the private key that can unencrypt the data.
Allow User Decryption	Determines whether users can see the **Personal** option for files within File Explorer and the **Save As** dialog box in Windows. If selected, employees can choose whether a file is **Work** or **Personal** in File Explorer and the **Save As** dialog box. If not selected, only the **Work** option is available. ⓘ If you pick this option, apps that use the **Save As** dialog box might encrypt new files as corporate data unless a different file path is given during the original file creation. After this happens, decryption of work files becomes more difficult. This option works only for devices using the Anniversary Edition of Windows 10 (1607). This options has been deprecated by the OS in all versions greater than the Anniversary Edition.
Revoke On Unenroll	Determines whether to revoke a user's local encryption keys from a device when it is unenrolled from WIP. If the encryption keys are revoked, a user no longer has access to encrypted corporate data. Uncheck this box to keep local encryption keys when migrating between MDM solutions.
Show WIP Icons	Determines whether the **Windows Information Protection** icon overlay appears on corporate files in the **Save As** and File Explore views.

TABLE 58. WINDOWS INFORMATION PROTECTION FIELDS (CONT.)

Fields	Description
Require Protection Under Lock	This options applies only to Windows 10 Mobile. It determines whether to encrypt enterprise data using a key that is protected by an employee's PIN code on a locked device. Apps will not be able to read corporate data when the device is locked.
Neutral Resources	Specify your authentication redirection endpoints for your company. These locations are considered enterprise or personal, based on the context of the connection before the redirection. If you have multiple resources, you must separate them using the "," delimiter. Example: sts.contoso.com,sts.contoso2.com
Enterprise Proxy Servers	Specify your externally-facing proxy server addresses, along with the port through which traffic accesses the Internet. This list must not include any servers listed in the **Enterprise Internal Proxy Servers** list, because they are used for WIP-protected traffic. This setting is also required if there's a chance you could are behind a proxy server on another network. In this situation, if you don't have a proxy server pre-defined, you might find that enterprise resources are unavailable to your client device, such as when you are visiting another company and not on the guest network. To make sure this doe not happen, the client device also needs to be able to reach the pre-defined proxy server through the VPN network. If you have multiple resources, you must separate them using the ";" delimiter. Example: proxy.contoso.com:80;proxy2.contoso.com:443
Enterprise Proxy Servers Are Authoritative	Click this box if you want Windows to treat the proxy servers you specified in the network boundary definition as the complete list of proxy servers available on your network. If you clear this box, Windows will search for additional proxy servers in your immediate network (auto-detect).
Enterprise Internal Proxy Servers	Specify the proxy servers your devices will go through to reach your cloud resources. Using this server type indicates that the cloud resources you're connecting to are enterprise resources. This list shouldn't include any servers listed in the **Enterprise Proxy Servers** list, which are used for non-WIP-protected traffic. If you have multiple resources, you must separate them using the ";" delimiter. Example: contoso.internalproxy1.com;contoso.internalproxy2.com
Allow Azure RMS	Check this box if WIP is to be used in conjunction with Azure Rights Management Service. Azure Rights Management (Azure RMS) can be used if company-wide information protection is desired.
RMS TemplateID	Specify your Azure RMS TemplateID.

Apply the profile to a label

This section describes how to apply the WIP profile to a label.

1. Select **Policies & Configs** > **Policy**.
2. Select the WIP policy you want to apply to a label.
3. Select **Actions** > **Apply to Label**.
4. Locate and select the label.
5. Click **Apply**.

ⓘ One note that we see with this profile is that once applied there can be cases where the profile is not removed once un-enrolled in UEM. It is recommended to test with VMs and WIP at this time.

Business Store Portal

The Windows Business Store Portal (BSP) The Store for Business provides app purchases based on organizational identity, flexible distribution options, and the ability to reclaim or re-use licenses. Organizations can also use the Store for Business to create a private store for their employees that includes apps from the Store, as well private Line-of-Business (LOB) apps.

BSP allows organizations to:

- make volume purchases of Windows applications
- create a private store for their employees (with Store apps and Line-of-Business (LOB) applications)
- shut off the Microsoft Store on devices
- get applications from offline mode and silently install without relying on Microsoft Store to push applications

ⓘ Refer to the *Core Apps@Work Guide* for more information about managing applications for Windows devices.

Prerequisites for BSP

We recommend you have met the following prerequisites before starting this section:

- "Standard prerequisites for all Azure services" on page 247
- One or more applications to add to Azure

BSP work flow

This section describes the overall work flow for setting up Core and BSP to work together:

- Add a BSP app in Azure
- Add and activate the Azure App in BSP
- Add the Azure information into Core
- Deploying apps

Add a BSP app in Azure

The first step to using Core with BSP is to create an Azure app under your tenant.

1. Log into Microsoft Azure.
2. Go to the tenant to which you want to add the app.
3. Click **NEW** on the bottom of the window to open a wizard.
4. Click **Add an application my organization is developing**.
5. Enter a name for the app in the **NAME** field.

   The name should be easy to remember, but personalized to your organization. You will use this name later in this process.
6. Click **WEB APPLICATION AND/OR WEB API** then click the right arrow to continue.
7. Set up the following 2 URLs.
   - **SIGN-ON URL**: URL for your instance of Core.
   - **APP ID URL**: to the Core administrator Login instance.
8. Click the check mark to save the configuration.
9. Go to **Azure Applications**.
10. Select the app and click **Configure**.

11. Make note of the ID in the **CLIENT ID** field to use it in Core later.

12. Select a key in the **keys** section.

    Ivanti recommends using a 2-year activation period for the key. Remember to refresh this key before activation period has gone by or access to the portal will stop. If you lose your key you can generate a new one

13. Save the changes on this page.

14. Make note key to enter into Core later.

15. Click **Add application**.

16. Complete the steps in "BSP set up" below.

BSP set up

The section describes how to set up BSP to allow access to the BSP from Azure.

1. Log into BSP (https://businessstore.microsoft.com).

2. Select **Settings** > **Management Tools**.

3. Click the **Add a management tool** link.

4. Enter the name of the app you added (in "Add a BSP app in Azure " on the previous page).

5. Click **Save**.

6. Select **Settings** > **Offline licensing**.

7. Click the **Activate** link for the app.

   Core integration is setup for use primarily with offline licensing. Online licensing requires administrators keep the Microsoft store open to users as online licensing cannot be distributed silently.

8. Complete the steps in "Core Setup" below.

Core Setup

The section describes how to set up Core to allow access to the BSP from Azure.

1. Log into the Core Admin Portal.

2. Select **Settings** > **System Settings** > **Windows** > **Business Store Portal**.

3. Click **Enable Business Store Portal**.
4. Enter the following information you generated in the "Add a BSP app in Azure " on page 262:

   Tenant ID (enter into **BSP Domain** field)

   Client ID (enter into **BSP Client ID** field)

   Secret Key (enter into **BSP Key** field)
5. Select how often you want to sync to the BSP.
6. Click **Save**.
7. Complete the steps in "Deploying applications" below.

Deploying applications

Refer to the *Core Apps@Work Guide*for details on how to:

- import apps, edit, deploy, and apply them to the labels.
- silently install offline in-house apps
- distribute online apps

All BSP Apps will be shown with a BSP Version so that administrators can tell the difference between BSP and apps loaded through other means. The size of the app will be the largest package available to the administrator. This may not be the same size as what is on the device.

Windows PIN management for PassPort For Work/Windows Hello

Use this feature to set up PIN Management for PassPort For Work/Windows Hello, including rules to manage both PINs and biometrics (iris, voice, fingerprints). You can also use it to create an identity change the AAD registration flow for future devices to take advantage of PassPort For Work/Windows Hello.

Prerequisites for setting up a PassPort For Work/Windows Hello policy are:

- Configuring an Azure Active tenant.
- "Enabling Microsoft Azure Menu" on the next page
- "Enabling PassPort For Work/Windows Hello with Microsoft Azure" on the next page

Enabling Microsoft Azure Menu

Enabling the Microsoft Azure Menu is a required step before you can use PassPort For Work/Windows Hello in a policy.

To enable WIP:

1. Select **Settings > System Settings > Windows > Advanced Menu**.
2. Select the **Enable Microsoft Azure Menu** check box.
3. Click **Save**.

Enabling PassPort For Work/Windows Hello with Microsoft Azure

Enabling PassPort For Work/Windows Hello with Microsoft Azure is a required step before you can use it in a policy.

To enable pin management for PassPort For Work/Windows Hello:

1. Select **Settings > System Settings > Windows > Microsoft Azure**.
2. Select the **Enable PassPort For Work/Windows Hello** check box.
3. Click **Save**.

Creating a PassPort For Work/Windows Hello policy

Use this feature to set up options for PIN management. You can use only one type of rule per profile.

Procedure

1. To create a PassPort For Work/Windows Hello policy:
2. Select **Policies & Configs > Policies**.
3. Select **Add New > Windows > PassPort For Work/Windows Hello**.
4. Modify fields in the New Windows PassPort For Work/Windows Hello Policy window, as necessary. Refer to the "New Windows PassPort For Work/Windows Hello Policy window" on the next page table for details.
5. Click **Save**.
6. Apply the policy to a label.

New Windows PassPort For Work/Windows Hello Policy window

The following table summarizes fields and descriptions in the **New Windows Information Protection** window:

TABLE 59. NEW WINDOWS PASSPORT FOR WORK/WINDOWS HELLO POLICY FIELDS

Fields	Description
Name	Add the unique name of the policy.
Status	Options are Active or Inactive.
Priority	Set the priority based on other policies. Each policy has an assigned hierarchy and Priority 1 taking precedence.
Description	Add a description of the policy
User PassPort For Work/Windows Hello	Options are Enabled or Disabled
Required Trusted Platform Module	Options are Enabled or Disabled
Minimum PIN Length	Range is 4 - 127 chars. Default is 4. Cannot be less than 4.
Maximum PIN Length	Maximum value cannot be more than 127. Cannot be less than the Min value.
Uppercase Letters in PIN	Values are: 0 - Allows the use of uppercase letters in PIN 1 - Requires the use of at least one uppercase letters in PIN 2 - Does not allow the use of uppercase letters in PIN (default)
Lowercase Letters in PIN	Values are: 0 - Allows the use of lowercase letters in PIN 1 - Requires the use of at least one lowercase letters in PIN 2 - Does not allow the use of lowercase letters in PIN (default)
Special Characters in PIN	Values are: 0 - Allows the use of special characters in PIN 1 - Requires the use of at least one special characters in PIN 2 - Does not allow the use of special characters in PIN (default)
Digits in PIN	Values are: 0 - Allows the use of digits in PIN 1 - Requires the use of at least one digits in PIN 2 - Does not allow the use of digits in PIN (default)

Table 59. New Windows PassPort For Work/Windows Hello Policy Fields (Cont.)

Fields	Description
PIN History	Integer value that specifies the number of past PINs that can be associated to a user account that can't be reused. The largest number you can configure for this policy setting is 50. The lowest number you can configure for this policy setting is 0. If this policy is set to 0, then storage of previous PINs is not required. Default is 0.
PIN Expiration	Integer value specifies the period of time (in days) that a PIN can be used before the system requires the user to change it. The largest number you can configure for this policy setting is 730. The lowest number you can configure for this policy setting is 0. If this policy is set to 0, then the user's PIN will never expire. Default is 0.
Use Remote Passport	Options are **Enabled** or **Disabled**. Use this option to enable or disable the use of remote Windows Hello for Business. Remote Windows Hello for Business provides the ability for a portable, registered device to be usable as a companion device for desktop authentication. Remote Windows Hello for Business requires that the desktop be Azure AD joined and that the companion device has a Windows Hello for Business PIN. Default is **Disabled**.
Use Biomentrics	Options are **Enabled** or **Disabled**. Use this option to enable or disable the of remote Windows Hello for Business. Remote Windows Hello for Business provides the ability for a portable, registered device to be usable as a companion device for desktop authentication. Remote Windows Hello for Business requires that the desktop be Azure AD joined and that the companion device has a Windows Hello for Business PIN. Default is **Disabled**.
Facial Features Use Enhanced Anti-Spoofing	Options are **Enabled** or **Disabled**. Use this option to enable or disable enhanced anti-spoofing for facial feature recognition on devices which support it. If this policy is not configured, the user can choose whether they want anti-spoofing on or off. If you set this policy to true, enhanced anti-spoofing is required on devices which support it. If you set this policy to false, enhanced anti-spoofing is turned off and the user cannot turn it on. This value can only be set if Use Biometrics is True. If False this should not be set. Default is **Enabled**.

Viewing status in device details

To see the policy status on a device:

1. Select **Devices & Users > Devices**.
2. Double-click the name of device.
3. Click the **Policies** tab.

   If the policy was pushed to the selected device, it will be listed in the table.

The status (Applied/Partially Applied) is based on if the policy has be synced to the device. If there a discrepancy in the policy the device will fall out of compliance the same as it would if passwords were out of compliance.

Windows license management

This features is for Windows 10 Desktop devices only.

Windows license management allows administrators to use Volume Licenses for BYOD for other devices to be upgraded. You can now use your Volume OS key to upgrade any Windows 10 desktop, HoloLens, or IoT device with a Pro or Enterprise SKU on the device.

Upgrade license paths:

- Pro --> Enterprise
- Any desktop with a Pro license --> Enterprise
- Consumer --> Enterprise
- For use with HoloLens and IoT devices

Upgrading Windows Licenses

To upgrade a Windows license:

1. Log into the Admin Portal.
2. Go to **Policies & Configs > Configurations**.
3. Select **Add New > Windows Licensing (Windows 10 only)**.
   - In the Windows License dialog box, enter the following options:
   - Name (required)
   - Description
   - Windows Key (Required) - used for Windows 10 Desktop, HoloLens, and IoT devices.
4. Click **Save**.

Managing Certificates and Configuring Certificate Authorities

This section addresses components related to managing certificates and certificate authorities.

Certificates overview

Core is capable of distributing and managing certificates.

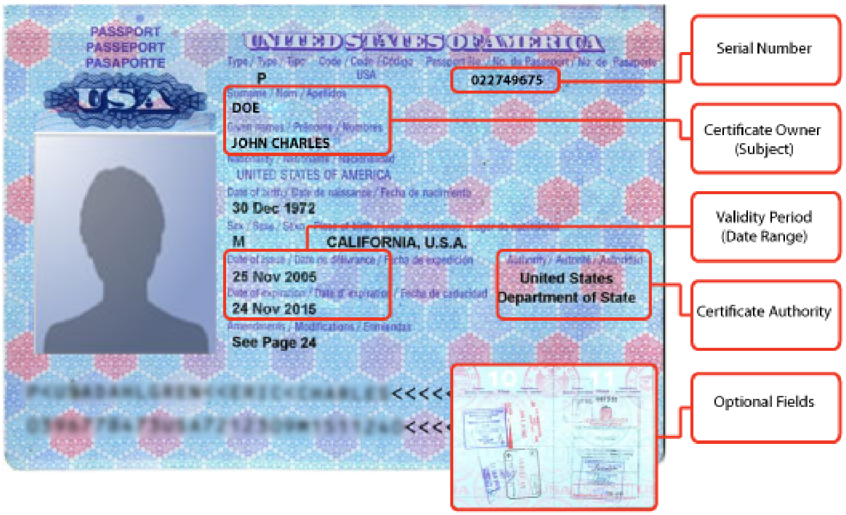
Certificates are mainly used for the following purposes:

- Establishing secure communications
- Encrypting payloads
- Authenticating users and devices

Certificates establish user identity while eliminating the need for users to enter user names and passwords on their mobile devices. Certificates streamline authentication to key enterprise resources, such as email, Wi-Fi, and VPN. Some applications require the use of certificates for authentication.

The following diagram compares a certificate to a passport:

FIGURE 1. COMPARING CERTIFICATES TO A PASSPORT



The certificate includes information that identifies the following information:

- the issuing certificate authority
- acceptable uses for the certificate
- information that enables the certificate to be validated.

This solution provides the flexibility to use Core as a local certificate authority, an intermediate certificate authority, or as a proxy for a trusted certificate authority.

Types of certificates

Core uses the following types of certificates:

TABLE 60. CERTIFICATE TYPES

Certificate type	Description
Portal HTTPS	The identify certificate and its certificate chain, including the private key, that identifies Core, allowing a client (such as a browser or app) to trust Core. Typically, this certificate is the same certificate as the Client TLS and iOS Enrollment certificates. Core sends this certificate to the client as part of the TLS handshake over port 443 or 8443 when the client initiates a request to Core. ⓘ This certificate must be a publicly trusted certificate from a well-known Certificate Authority if you are using mutual authentication. **Related topics** “Certificates you configure on the System Manager” in the Core System Manager Guide
Client TLS	The identify certificate and its certificate chain, including the private key, that identifies Core, allowing Mobile@Work for iOS and Android to trust Core. Typically, this certificate is the same certificate as the Portal HTTPS and iOS Enrollment certificates. Core sends this certificate to Mobile@Work for iOS or Android as part of the TLS handshake over port 9997 when Mobile@Work initiates a request to Core. **Related topics** “Certificates you configure on the System Manager” in the *Core System Manager Guide*
MobileIron Core server SSL	Can be either self-signed or third-party certificates. By default, Core generates self-signed certificates. You can use trusted certificates from third-party certificate providers such as Verisign, Thawte, or Go Daddy. Kerberos and Entrust certificates are also supported.
Sentry server SSL	Identifies the Sentry to the client and secures communication, over port 443, between devices and the Sentry.
Windows Phone Enrollment	Issued by Core to authenticate the device. This is the local CA certificate.
Client identity	Verifies the identity of users and devices and can be distributed through Certificate Enrollment.

Windows devices require a root or intermediate certificate from a trusted certificate authority (CA) for registering with Core.

Managing certificates issued by certificate enrollment configurations

Core runs a process each day at 3:45 am that manages all certificates issued using certificate enrollment configurations.

Certificates have a limited lifetime that is defined when certificates are issued. When the certificate lifetime is within the expiry window (60 days, by default), Core does not automatically renew the certificates. Only a forced manual renewal/creation is possible.

Re-issued certificates are sent to the managed device configuration and the expiring certificates become inactive. The inactive certificates are purged from the system once the certificates are expired or confirmed to be revoked.

Supported certificate scenarios

Core supports the following certificate scenarios:

- "Core as a certificate authority" below
- "Using Core as a certificate proxy" on the next page
- "Using Core as a certificate enrollment reverse proxy" on page 274
- "Supported certificate scenarios" above

Core as a certificate authority

You can configure Core as a local certificate authority (CA) for the following scenarios:

- Core as an Independent Root CA (self-signed)—Configure Core as an independent root certificate authority if you are using a self-signed certificate. Use this option if your company does not have its own certificate authority and you are using Core as the certificate authority.
- Core as an Intermediate CA—Use this option when your company already has its own certificate authority. Using Core as an Intermediate CA gives your mobile device users the advantage of being able to authenticate to servers within your company intranet.

Using Core as a certificate proxy

Core can act as a proxy to a 3rd party CA by using APIs exposed by the 3rd party CA or the SCEP protocol to obtain certificates required by a Certificate Enrollment. This enables you to configure certificate-based authentication for devices.

Using Core as a certificate proxy has the following benefits:

- Certificate verifies Exchange ActiveSync, Wi-Fi and/or VPN connections, eliminating the need for passwords that are complex to manage
- Core can manage certificates by checking status against a CA's CRL, deactivating revoked certificates and requesting replacement when certificates are about to expire
- Core can detect and address certificate renewal and ensure that devices cannot reconnect to enterprise resources if they are out of compliance with company policies.
- Simplified enrollment with the following:
    - MS Certificate Enrollment
    - Entrust
    - Local CA
    - Symantec Managed PKI
    - User provided certificates
    - Open Trust
    - Symantec Web Services Managed PKI

The following applications are supported.

- Wi-Fi.

For information about how to create certificate enrollment settings in Core, see "Certificate Enrollment settings" on page 297.

Using Core as a certificate enrollment reverse proxy

Identity certificates with Microsoft Certificate Enrollment are supported. A root or intermediate certificate from a trusted certificate authority (CA) is required, and you must set up Core to act as a SCEP reverse proxy.

Windows devices originate the certificate request. When the Windows device requests a certificate, the Core acts as a Certificate Enrollment reverse proxy and communicates with the Certificate Enrollment server to deliver the certificate to the device.

Certificate scenarios supported for Windows 8.1 Phone

TABLE 1. CERTIFICATE SCENARIOS SUPPORTED FOR WINDOWS 8.1 PHONE

	Windows Phone 8.1
Portal	Public trusted[1]
Core as certificate authority	-
Certificate Enrollment proxy	-
Reverse Certificate Enrollment	Yes[2]
Kerberos	Yes

1. The portal certificate must be issued by a trusted third-party certificate authority for successful device registration.
2. Supported for email, Wi-Fi, VPN configurations and in-house apps.

Core as a certificate authority

You can configure Core as a local certificate authority for the following scenarios:

- **Core as an Independent Root CA (self-signed)**— Configure Core as an independent root certificate authority if you are using a self-signed certificate. Use this option if your company does not have its own certificate authority and you are using Core as the certificate authority.

  See "Configuring Core as an independent root CA (Self-Signed)" on the next page.

- **Core as an Intermediate CA**—Use this option when your company already has its own certificate authority. Using Core as an Intermediate CA gives your mobile device users the advantage of being able to authenticate to servers within your company intranet.

  See "Configuring Core as an intermediate CA" on page 279.

Configuring Core as an independent root CA (Self-Signed)

Configuring Core as an independent root CA requires configuring your infrastructure to trust Core as an independent root CA.

To configure Core as an independent root CA, you must follow these basic steps:

1. Generate a self-signed certificate

   See "Generating a self-signed certificate" below.

2. Create a local CA certificate enrollment setting for the self-signed certificate

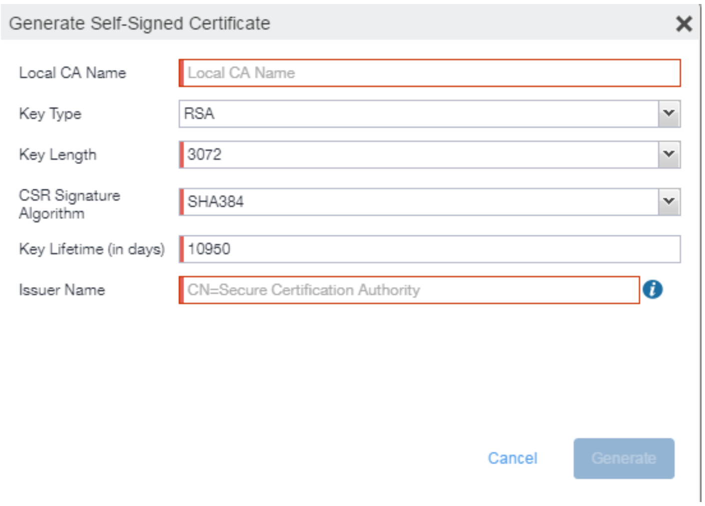
   See "Creating a local certificate enrollment setting" on page 279.

Generating a self-signed certificate

This section addresses how to generate the self-signed certificate.

Procedure

1. Log into the Admin Portal.
2. Go to **Services** > **Local CA**.
3. Select **Add > Generate Self-Signed Cert**.



Generate Self-Signed Certificate

Local CA Name	Local CA Name
Key Type	RSA
Key Length	3072
CSR Signature Algorithm	SHA384
Key Lifetime (in days)	10950
Issuer Name	CN=Secure Certification Authority

4. Enter the following information.

   - **Local CA Name**: Enter a recognizable name to identify the self-signed certificate. This name will appear in the list of local certificate authorities in **Services > Local CA**.
   - **Key Type**: Specify the key type. The options are RSA (default) or Elliptical Curve.
   - **Key Length**: Specify the key length. The values are 2048, 3072 (the default), and 4096. The longer the key length, the more secure the certificate.

- **CSR Signature Algorithm**: The values are SHA1, SHA256, SHA384 (default), and SHA512.
    - **Key Lifetime (in days)**: Enter number of days. The key will expire after the entered number of days.

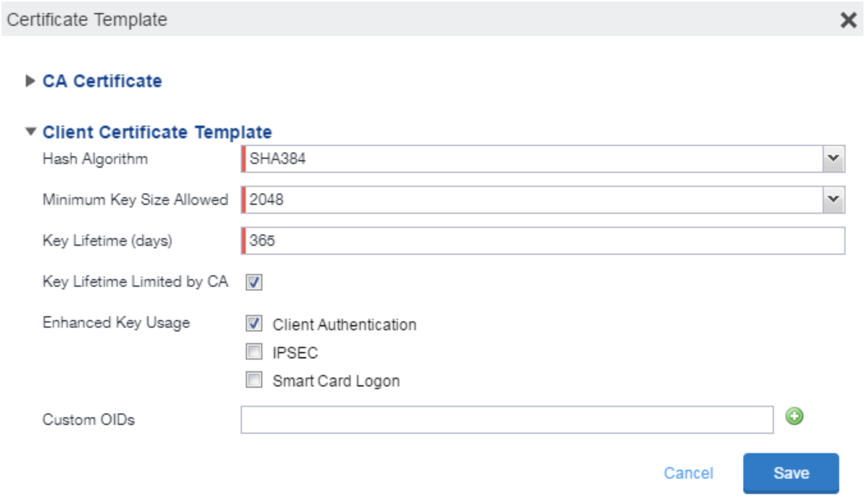
      The default is 10,950 days. Ivanti recommends 5 years or longer; 61 days is the minimum.
    - **Issuer Name**: Requires an X.509 name. For example, CN=www.yourcompany.com, DC=yourcompany, DC=com.

      The **Issuer Name** field uses an X.509 distinguished name. You can use one or more X.509 codes, separated by commas. The following table describes the valid codes for the Issuer Name field:

Code	Name	Type	Max Size	Example
C	Country/Region	ASCII	2	C=US
DC	Domain Component	ASCII	255	DC=company, DC=com
S	State or Province	Unicode	128	S=California
L	Locality	Unicode	128	L=Mountain View
O	Organization	Unicode	64	O=Company Name, Inc.
OU	Organizational Unit	Unicode	64	OU=Support
CN	Common Name	Unicode	64	CN=www.company.com

If you have a registered DNS name that you use to send SMTP mail, a best practice is to use the domain component convention and the DNS name for the certificate name.

5. Click **Generate**.



Certificate Template

▶ CA Certificate

▼ Client Certificate Template

Hash Algorithm: SHA384

Minimum Key Size Allowed: 2048

Key Lifetime (days): 365

Key Lifetime Limited by CA ☑

Enhanced Key Usage
- ☑ Client Authentication
- ☐ IPSEC
- ☐ Smart Card Logon

Custom OIDs

6. Configure the **Client Certificate Template**.

   Values depend on the purpose for the certificate and the requirements of your environment.

   - **Hash Algorithm**: The larger the hash number, the more secure. The options are SHA256, SHA384 (default), SHA512—part of the SHA2 secure hash algorithm family required for U.S. government applications. The number signifies the output bits.
   - **Minimum Key Size Allowed**: The longer the key length is, the more secure the certificate.
   - **Key Lifetime (days)**: 365 days or longer is recommended; 61 days is the minimum.
   - **Key Lifetime limited by CA**: Select to use the key lifetime specified for the self-signed CA.

     Ivanti recommends enabling this option. Enabling this option ensures that client certificate validity periods do not exceed the life time of the issuing CA certificate.
   - **Enhanced Key Usage**: When a certificate is presented to an application, the application can require the presence of an Enhanced Key Usage OID specific to that application. Leave these deselected if you do not have any applications that require additional OIDs.
   - **Custom OIDs**: If you are using this certificate for SSL authentication, enter the OID in this field.

7. Click **Save**.

   The newly created self-signed certificate will be listed in **Services > Local CA**.

Creating a local certificate enrollment setting

After you have generated the self-signed certificate, you need to create a local CA certificate enrollment setting for the self-signed certificate. Creating a local CA certificate enrollment setting enables proxy functionality so that Core generates the certificates and caches the generated keys.

1. Log into the Admin Portal.
2. Go to **Policies & Configs** > **Configurations.**
3. Click **Add New** > **Certificate Enrollment** > **Local**.

For more information on configuring the settings, see "Certificate Enrollment settings" on page 297.

Pruning revoked CRL certificates

Revoked certificates can be automatically pruned from a Core Local CA Certificate Revocation List (CRL).

To configure CRL pruning of local CA certificates:

Procedure

1. From the Admin portal, go to **Services > Local CA** page and select a certificate.
2. From the Actions menu, select **Edit**. The certificate template window opens.
3. Click the caret to the left of **CA Certificate** to open the section.
4. Click **CRL Pruning** to enable it.
5. Enter the number of days of revoked certificates you want to include in the CRL before pruning. The default is **365**.
6. Enter the **CRL lifetime** in hours, after which Core regenerates the list. The default is **168 hours** (7 days).
7. Click **Save**. Expired certificates beyond the revocation date are pruned from the CRL.

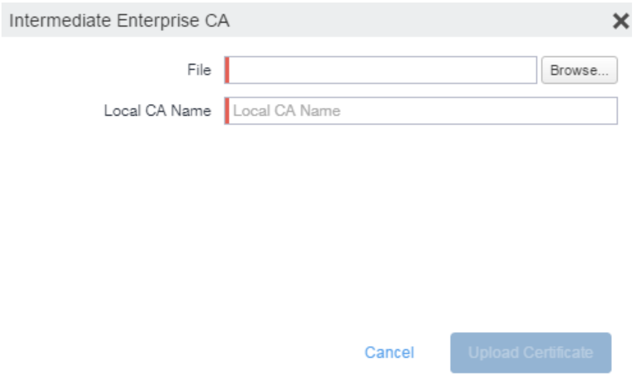
Configuring Core as an intermediate CA

When you configure Core as an intermediate certificate authority, the managed device users can authenticate to servers within your company intranet; not just the Core system.

After you get the certificate from your certificate vendor, you can add the certificates to Core to create the intermediate certificate authority (CA).

Procedure

1. In the Core Admin Portal go to **Services > Local CA**.
2. Click on **Add > Intermediate Enterprise CA**.



3. Click **Browse** and navigate to the combined file.
4. Click **Open**.
5. Enter a recognizable name in the **Local CA Name** field.
6. Click **Upload Certificate**.

   Your local certificate authority is now available to use. The local CA will be listed in **Services > Local CA**.

Mutual authentication between devices and Core

Core supports mutual authentication, which means that not only must the device trust Core, but Core must trust the device. Therefore, with mutual authentication, a registered device can continue to communicate with Core only if the device provides the right certificate to Core. Mutually authenticated communication between the device and Core enhances security.

A device authenticating to Core with a certificate is also known as certificate-based authentication to Core.

Scenarios that can use mutual authentication

The device can present a client identity certificate to Core in the following cases:

TABLE 61. MUTUAL AUTHENTICATION USAGE BY PLATFORM

Platform	Mutual Authentication usage
iOS	• Mobile@Work for iOS device check-in • AppConnect for iOS check-in • iOS MDM device check-in • Apps@Work for iOS communication • Certificate pinning policy
macOS	• Mobile@Work for macOS device check-in • macOS MDM device check-in
Android	• Mobile@Work for Android device check-in, which includes AppConnect check-in • Apps@Work for Android communication
Windows 10	Device check-in

Mutual authentication is not possible at the time Mobile@Work registers with Core, because the device receives its identity certificate during the registration process.

Core port usage with devices, with and without mutual authentication

The following table summarizes Core port usage for registration and further communication with devices. The port usage for some cases is different depending on whether mutual authentication is enabled.

TABLE 62. CORE PORT USAGE WITH DEVICES WITH AND WITHOUT MUTUAL AUTHENTICATION

	Without mutual authentication	With mutual authentication
Mobile@Work for iOS	9997	443
Mobile@Work for Android	9997	443
Mobile@Work for macOS	Not applicable. Mobile@Work for macOS always uses mutual authentication with Core.	443
iOS and macOS MDM agent provisioning and agent check-in	443	443
Windows 10	Not applicable. Windows 10 always uses mutual authentication with Core.	443

Port 9997 is configurable in the System Manager in Settings > Port Settings > Sync TLS Port. However, changing the port is rare.

The mutual authentication setting on Core

The setting on Core to enable mutual authentication is in the Admin Portal in **Settings > System Settings > Security > Certificate Authentication.** Whether the setting is automatically selected on new installations and upgrades is described by the following table.

TABLE 63. SETTING FOR MUTUAL AUTHENTICATION ON NEW INSTALLS AND UPGRADES

	Setting to enable mutual authentication
New installations	Not selected. Mutual authentication is **not** enabled.
Upgrade from a previous version of Core in which mutual authentication was **not** enabled. Or Upgrade from a version of Core prior to Core 9.7.0.0 in which the Android mutual authentication setting was **not** enabled.	Not selected. Mutual authentication is **not** enabled.
Upgrade from a previous version of Core in which mutual authentication **was** enabled. Or Upgrade from a version of Core prior to Core 9.7.0.0 in which the Android mutual authentication setting **was** enabled.	Selected. Mutual authentication **is** enabled.

IMPORTANT: Once mutual authentication is enabled on Core, it cannot be disabled.

The mutual authentication setting impacts mutual authentication usage only on:

- Mobile@Work for Android
- Apps@Work for Android
- However, to enable mutual authentication for Apps@Work for Android:
  - You must also select **Certificate Authentication** for Apps@Work at **Apps** > **Apps@Work Settings** > **App Storefront Authentication**.
  - The device must be using Mobile@Work 10.2.0.0 for Android or supported newer versions.
- Mobile@Work 9.8 or supported newer versions.
- iOS MDM
- macOS MDM

The mutual authentication setting has no impact on mutual authentication usage on:

- Versions of Mobile@Work for iOS prior to Mobile@Work 9.8

  These versions of Mobile@Work for iOS **never** use mutual authentication.

- Apps@Work for iOS

- Apps@Work for iOS **always** uses mutual authentication from Core 11.3.0.1 and newer versions.

- Mobile@Work for macOS

  Mobile@Work for macOS **always** uses mutual authentication.

- Windows 10 devices

  Windows 10 devices **always** uses mutual authentication.

When devices use mutual authentication

Whether devices use mutual authentication depends on:

- The device platform
- Whether mutual authentication was enabled before upgrade
- Whether mutual authentication is enabled after upgrade
- Whether mutual authentication is enabled after a new installation
- For Mobile@Work for iOS, the version of Mobile@Work

The following table summarizes when devices use mutual authentication and the port they use in communication with Core.

TABLE 64. CORE MUTUAL AUTHENTICATION (MA) SETTING IMPACT TO DEVICE COMMUNICATION

	New Core installation **or** **Core upgrade in which: MA setting was NOT enabled before upgrade**	**New Core installation in which you enable MA setting after installation.** **or** **Core upgrade in which: MA setting was NOT enabled before upgrade but you enable it after the upgrade.**	**Core upgrade in which:** **MA setting WAS enabled before upgrade**
Mutual authentication setting	Not enabled	Enabled	Enabled
Device client			
Android: Mobile@Work (all Mobile@Work versions that Core supports)	Port: 9997 MA: not used	Devices that register after enabling MA: • Port: 443 • MA: used Devices that were already registered: • Port: 9997 • MA: not used.	Port: 443 MA: used
iOS: Mobile@Work 9.8 or supported newer versions	Port: 9997 MA: not used	Devices that register after enabling MA: • Port: 443 • MA: used Devices that were already registered: • Port: 9997 • MA: not used.	Devices that register after enabling MA: • Port: 443 • MA: used Devices that were already registered: • Port: 9997 • MA: not used.
iOS: Mobile@Work versions prior to 9.8	Port: 9997 MA: not used	Port: 9997 MA: not used	Port: 9997 MA: not used

TABLE 64. CORE MUTUAL AUTHENTICATION (MA) SETTING IMPACT TO DEVICE COMMUNICATION (CONT.)

	New Core installation **or** **Core upgrade in which: MA setting was NOT enabled before upgrade**	**New Core installation in which you enable MA setting after installation.** **or** **Core upgrade in which: MA setting was NOT enabled before upgrade but you enable it after the upgrade.**	**Core upgrade in which:** **MA setting WAS enabled before upgrade**
iOS: iOS MDM check-in	Port: 443 MA: not used	Port: 443 MA: used	Port: 443 MA: used.
macOS: Mobile@Work	Port: 443 MA: used	Port: 443 MA: used	Port: 443 MA: used
macOS macOS MDM agent check-in	Port: 443 MA: not used	Port: 443 MA: used	Port: 443 MA: used
Windows 10	Port: 443 MA: used	Port: 443 MA: used	Port: 443 MA: used

On new Core installations (not upgrades), if you enable mutual authentication **before any devices register,** you can disable port 9997 (in the System Manager in Settings > Port Settings > Sync TLS Port) because it is not used. If devices were registered before enabling mutual authentication, disabling the port causes those devices to not be able to check-in.

Mutual authentication identity certificate for Core

You provide an identity certificate for Core to use in mutual authentication in the Portal HTTPS certificate. You configure this certificate on the System Manager at **Security > Certificate Mgmt.** The certificate is the identify certificate and its certificate chain, including the private key, that identifies Core, allowing the devices to trust Core. This certificate must be a publicly trusted certificate from a well-known Certificate Authority when using mutual authentication.

Mutual authentication client identity certificate

You enable mutual authentication for iOS and Android devices in the Admin Portal in **Settings > System Settings > Security > Certificate Authentication.** The certificate enrollment setting specifies how the identity certificate that the device will present to Core is generated.

By default, the certificate enrollment setting for mutual authentication is generated with Core as a local Certificate Authority (CA). Most customers use the default selection. However, if necessary due to your security requirements, you can instead specify a SCEP certificate enrollment setting that you create. In that case, see "Create the SCEP enrollment certificate" on page 315

Related topics

See "Handling client identity certificate expiration for Android devices" on page 291 and "Handling client identity certificate expiration for iOS devices" on page 291

Supported custom attributes for mutual authentication certificates

From Core release 10.8.0.0 through the latest release supported by Ivanti, Core supports only the following list of custom attributes in the **Subject** field for mutual authentication enrollment certificates:

- $RANDOM_16$
- $RANDOM_32$
- $RANDOM_64$
- $CONFIG_UUID$
- $TIMESTAMP_MS$

If, after upgrading to release 10.8.0.0 or supported newer versions, the existing selected mutual authentication certificate includes unsupported attributes, Core will replace them with the value $RANDOM_32$ for new device registrations and for existing device certificate renewals.

The **Admin portal > Settings > System Settings > Client Mutual Certificate Authentication > Certificate Enrollment setting** drop-down menu displays only the Simple Certificate Enrollment Protocol (SCEP) configurations with the five supported custom attributes in the **Subject** field. Configurations with other custom attributes do not display.

New endpoint for mutual certification authentication

Once mutual authentication is enabled on Core by the administrator, new mutual authentication devices endpoints are available for use by iOS and Android clients. The existing (old) OAuth endpoint is not protected by 2FA or mutual certificate authentication and is vulnerable to password spraying and DOS attacks. There is an option for the administrator to disable the original OAuth endpoint and utilize the new endpoint.

ⓘ If mutual authentication migration is not enabled, then older client installations will continue to lack mutual authentication functionality.

This feature is applicable on Mobile@Work for Android version 11.1.0.0 and Mobile@Work for iOS version 12.11.10 or supported newer versions.

Below is an example scenario of the old OAuth versus the new endpoint:

TABLE 65. OLD OAUTH VS NEW ENDPOINT

New endpoint	Old OAuth
Not configured	Enabled (old OAuth endpoint works)
Enabled	Enabled (new endpoint works)
Enabled	Disabled (new endpoint works)
Disabled	Disabled (Error)

Note the following: You can have mutual certificate authentication on Mobile@Work clients (both iOS and Android) and on the watchOS app, however, it will mean less security. Ivanti does not recommend putting mutual certificate authentication on the watchOS app.

To implement this setup, two endpoints are required:

1. A current OAuth endpoint that can be used by watchOS app, an old or updated Mobile@Work for iOS, OR an old or updated Mobile@Work for Android and cURL script.

2. A new endpoint that will always require mutual certificate authentication.

Before you begin

- Administrators should have enabled mutual certificate authentication and have migrated all the devices. Check-ins will occur on port 443 and not sync the TLS port 9997.
- Clients need to be upgraded to the version that supports the new endpoint.

Procedure

1. Go to **Settings > System Settings**.
2. In the left navigational pane, click **Security > Certificate Authentication**.

   The Client Mutual Certification Authentication page displays in the right pane.

3. Use the below guidelines to complete this form.

Table 66. Client Mutual Certification Authentication

Item	Description
Enable client mutual certificate authentication on Android client, iOS client, iOS and macOS MDM and AppConnect communications	Selecting the check box is a pre-requisite to enabling the new endpoint.
Certificate Enrollment Setting	Select **System-Mutual Auth CE** from the drop-down.
Enable new OAuth Endpoint with Mutual certificate Authentication	Select this to enable the new endpoint. If this field is greyed out, it means you did not meet the pre-requisite requirements of enabling mutual certificate authentication and migrating all client devices. See Before you begin.
Disable legacy OAuth Endpoint	This should only be done after the client devices have been updated to Mobile@Work for Android version X and Mobile@Work for iOS version X. a. When selecting the Disable legacy OAuth Endpoint box, a confirmation displays. Click **Disable**. b. A second confirmation dialog box displays, click **Disable**. Once disabled, the WatchOS app will no longer work. This setting can be reversed by de-selecting it. ⓘ Before disabling the legacy OAuth endpoint, make sure that all devices are migrated to the new endpoint.

4. Click **Save**.

Handling client identity certificate expiration for Android devices

Mobile@Work 10.1 for Android handles the expiration of the client identity certificate used for mutual authentication between Mobile@Work for Android and Core. In the Admin Portal, on the sync policy for the device, specify a renewal window for the certificate. The renewal window is a number of days prior to the certificate expiration. When Mobile@Work determines the renewal window has begun, it requests a new certificate from Core.

If Mobile@Work is out of contact with Core during the renewal window, but is in contact again within 30 days after the expiration, Mobile@Work requests a new certificate from Core.

If Mobile@Work is not in contact with Core either during the renewal window or within 30 days after the expiration, the device will be retired and will need to re-register with Core.

Mobile@Work versions prior to 10.1 do not support certificate expiration. When the certificate expires, the device user must re-register Mobile@Work.

Procedure

1. In the Admin Portal, go tos **Policies & Configs** > **Policies**.
2. Select the appropriate sync policy.
3. For **Mutual Certificate Authentication Renewal Window**, enter the number of days prior to the expiration date that you want to allow devices to renew their identity certificate. Enter a value between 1 and 60.

   ⓘ A blank value defaults to 60 days.

4. Click **Save**.
5. Click **OK**.

Handling client identity certificate expiration for iOS devices

Mobile@Work 11.1.0 for iOS handles the expiration of the client identity certificate used for mutual authentication between Mobile@Work for iOS and Core version 10.3.0.1 or supported newer versions. In the Admin Portal, on the sync policy for the device, specify a renewal window for the certificate. The renewal window is a number of days prior to the certificate expiration. When Mobile@Work determines the renewal window has begun, it requests a new certificate from Core.

If Mobile@Work is out of contact with Core during the renewal window, but is in contact again within 30 days after the expiration, Mobile@Work requests a new certificate from Core.

If Mobile@Work is not in contact with Core either during the renewal window or within 30 days after the expiration, the device will be retired and will need to re-register with Core.

Mobile@Work versions prior to 11.1.0 do not support certificate expiration. When the certificate expires, the device user must re-register Mobile@Work.

Procedure

1. In the Admin Portal, go to **Policies & Configs** > **Policies**.
2. Select the appropriate sync policy.
3. For **Mutual Certificate Authentication Renewal Window**, enter the number of days prior to the expiration date that you want to allow devices to renew their identity certificate. Enter a value between 1 and 60.

   A blank value defaults to 60 days.

4. Click **Save**.
5. Click **OK**.

Mutual authentication and Apps@Work

Both Apps@Work for Android and Apps@Work for iOS can use mutual authentication.

Apps@Work for iOS uses mutual authentication if you select **Certificate Authentication** at **Apps > Apps@Work Settings > App Storefront Authentication**. It does *not* depend on the mutual authentication setting at **Settings > System Settings > Security > Certificate Authentication.**

However, Apps@Work for Android uses mutual authentication only if you do both of the following:

- Select **Certificate Authentication** at **Apps** > **Apps@Work Settings** > **App Storefront Authentication**.
- Enable the mutual authentication setting at **Settings** > **System Settings** > **Security** > **Certificate Authentication.**

Related topics

- "Setting up Apps@Work for iOS and macOS" in the *Core Apps@Work Guide*
- "Apps@Work in Mobile@Work for Android in the *Core Apps@Work Guide*

Enabling mutual authentication for Apple and Android devices

The Core mutual authentication setting enables mutual authentication for:

- Mobile@Work for Android
- Apps@Work for Android
  - You must also select **Certificate Authentication** for Apps@Work at **Apps > Apps@Work Settings > App Storefront Authentication**.
  - The device must be using Mobile@Work 10.2.0.0 for Android or supported newer versions.
- Mobile@Work 9.8 for iOS or supported newer versions.
- iOS MDM
- macOS MDM

Mutual authentication is automatically enabled in the cases described in "The mutual authentication setting on Core" on page 282.

Important After you enable mutual authentication, you cannot disable it.

Before you begin

1. As discussed in in "Mutual authentication client identity certificate" on page 287, create a SCEP certificate enrollment setting if you do not want to use the default local certificate enrollment setting for mutual authentication. The SCEP setting requires that you enable the following options:
   - **Decentralized**
   - **Proxy requests through Core**

   For details, see "Certificate Enrollment settings" on page 297.

When you enable mutual authentication, change the certificate enrollment selection for mutual authentication ***before any more devices register***. Any devices already registered and using mutual authentication will not be able to check-in with Core. Those devices will need to re-register with Core. Note that devices already registered but not using mutual authentication can continue to check-in.

2. If you are using iOS devices with the Apps@Work web clip using certificate authentication, change the **Apps@Work Port** field in the System Manager in **Settings > Port Settings**. Ivanti recommends port 7443. However, you can use any port except the port that the Admin Portal uses, which is either 443 or 8443, which you specify in the **MIFS Admin Port** field in the System Manager in **Settings > Port Settings**.

Procedure

1. In the Admin Portal, go to **Settings > System Settings > Security > Certificate Authentication.**
2. Select **Enable client mutual certification on Android client, iOS client and Apple MDM communication**.
3. In the **Certificate Enrollment Configuration** field, most customers use the default selection. Otherwise, select a SCEP certificate enrollment setting.
4. Click **Save**.

Related topics

- “Setting up Apps@Work for iOS and macOS” in the *Core Apps@Work Guide*
- "Port settings" in the *Core System Manager Guide*
- “Apps@Work for Android authentication to Core” in the *Core Apps@Work Guide*

Enabling TLS inspecting proxy support when using mutual authentication

Contact Ivanti Professional Services or an Ivanti certified partner to set up this deployment.

Core can support a TLS inspecting proxy to handle HTTPS requests from your devices to Core when using mutual authentication. For example, you can use a TLS offload proxy such as an Apache or F5 server. This proxy is also known as a Trusted Front End. It intercepts and decrypts HTTPS network traffic and when it determines that the final destination is Core, it re-encrypts and forwards the traffic to Core. The devices that register to Core (using port 443) must send HTTPS requests to the TFE rather than to Core. Also, the TFE must be provisioned with digital certificates that establish an identity chain of trust with a legitimate server verified by a trusted third-party certificate authority.

Related topics

"Advanced: Trusted Front End" in the *Core System Manager Guide*

Migrating Mobile@Workfor Android and iOS to use mutual authentication

For devices that register after enabling mutual authentication, Mobile@Work uses port 443 for device check-ins. However, devices that were already registered continue to use port 9997. You can migrate Mobile@Work for Android from using port 9997 without mutual authentication to using port 443 with mutual authentication. The device users do not need to re-register with Core.

Before you begin

Instruct Android and iOS device users to upgrade to Mobile@Work 10.1 for Android or or Mobile@Work 12.11.10 for iOS or supported newer versions. Prior Mobile@Work releases do not support migration.

Procedure

1. In the Admin Portal, go to **Policies & Configs > Policies**.
2. Select the sync policy for the devices that you want to migrate. Select **Edit**.
3. In the Modify Sync Policy dialog box, select **Migrate Mobile@Work Client**.
4. Click **Save**.
5. Click **OK**.

On the next device check-in, Core will send the mutual authentication client identity certificate to the device. In all subsequent device check-ins, the device will use mutual authentication on port 443.

On that first device check-in, the device's **client migration status** changes to **Pending**. After Core has sent the mutual authentication client identity certificate to the device, the **client migration status** changes to **Success**. You can search on this value in the **Client Migration Status** field in **Advanced Search** on **Devices & Users > Devices**.

Related topics

"When devices use mutual authentication" on page 284

Certificates settings

Use a certificate setting to upload a trusted public key root certificate or certificate chain. If it is a certificate chain, it can include the root certificate or only intermediate certificates.

IMPORTANT: You cannot upload an identity certificate -- a certificate that contains a private key -- into a certificate setting. To upload an identity certificate to Core, use the certificate enrollment setting called single file identity.

You configure Core to deliver the uploaded certificate or certificate chain to devices so that the devices can trust, for example, specific web services, email servers, or network components like VPN and Wi-Fi.

Two ways are available to deliver the certificate to a device:

- You reference the certificate setting from another Core setting, and apply the appropriate labels to the referencing setting. Only the following settings can reference a certificate setting:
  - An AppConnect app configuration, Web@Work setting, or Docs@Work setting can reference a certificate setting as the value of a key-value pair.
  - A Wi-Fi setting can reference a certificate setting in its **Apply to Certificates** field (used with specific authentication and data encryption values on the Wi-Fi setting).
- You want to deliver a trusted public key certificate directly to a set of devices, without referencing the certificate setting from another setting. In this case, label the certificate setting. This case is less common.

Note the following:

- When upgrading from a Core prior to Core 9.5.0.0, each certificate setting that contained an identity certificate is automatically converted to a single file identity certificate enrollment setting. Any settings that referenced the certificate setting refer to the new single file identity certificate enrollment setting.
- You cannot import a certificate setting from a Core prior to Core 9.4.0.0 if the certificate setting contained an identity certificate. You must manually create a single file identity certificate enrollment setting.

Adding a certificate setting

Procedure

1. Log in to the Admin Portal.
2. Go to **Policies & Configs > Configurations**
3. Click **Add New > Certificates**.
4. Fill in the entries:
   - **Name**: Enter brief text that identifies certificate setting.
   - **Description**: Enter additional text that clarifies the purpose of this certificate setting.
   - **File Name**: Click **Browse** to select the X.509 certificate file (.cer, .crt, .pem, or .der) to upload to Core Core. The certificate must be encoded as binary DER or ASCII PEM.
5. Click **Save**.

Label the certificate setting if you want to deliver the certificate directly to a set of devices, regardless whether it is referenced from another setting. If you are referencing the certificate setting from another setting, label the other setting.

Certificate Enrollment settings

Identity certificates can be distributed via Apps@Work.

Certificate enrollment settings are used as follows:

- As part of a larger process of setting up a certificate enrollment server to support authentication for VPN on demand, Wi-Fi, Exchange ActiveSync, AppTunnel and so on.
- To provide devices identity certificates that you uploaded to Core for the case when you want to provide the same identity certificate to many users' devices.
- To provide user-provided certificates to devices when end users use the Core user portal to upload their identity certificates to Core.

The available options are:

- **Blue Coat**: Select **Blue Coat** to create a Blue Coat certificate enrollment setting for integrating with the Blue Coat Mobile Device Security service.
- Client-Provided: Select **Client-Provided** if you want AppConnect apps to use derived credentials for authentication, digital signing, or encryption.
- **Entrust**: Select **Entrust** if you are using the Entrust Datacard certificate enrollment solution.
- **GlobalSign**: Select **GlobalSign** if you are using GlobalSign as the CA for certificate enrollment.
- **Local**: Select Local if you are using Core as the CA.
- **OpenTrust**: Select **OpenTrust** if you are using the OpenTrust integration. See "Configuring OpenTrust CA" on page 310.
- Single File Identity: Select **Single File Identity** to upload an identity certificate for distribution to devices.
- **SCEP**: Select **SCEP** for standard certificate-based authentication using a separate CA.

  SCEP Configurations created before upgrading to Core 7.0.0.0 or later should be replaced with a new SCEP Configuration. Failure to do so might result in cert renewal failure from Core 9.4.0.0.

- **Symantec Managed PKI**: Select **Symantec Managed PKI** if you are using Symantec's Certificate Enrollment solution. See "Configuring Symantec Managed PKI" on page 320 for more information.
- **Symantec Web Services Managed PKI**: Select **Symantec Web Services Managed PKI** if you are using the Symantec Web Services Managed PKI solution. See "Configuring Symantec Web Services Managed PKI " on page 323for more information.

- **User-Provided**: Select **User-Provided** if device users will upload their personal certificates. The user portal includes a certificate upload section for this purpose. A web services API is also available for you to upload user-provided certificates.

If Certificate Enrollment integration is not an option

If Certificate Enrollment integration is not an option for your organization, consider configuring Core as an intermediate or root CA. See "Certificate Enrollment settings" on page 297 for more information.

Supported variables for certificate enrollment

The following variables are supported for the required and optional fields when configuring integration with supported Certificate Authorities (CA's):

- $EMAIL$
- $USERID$
- $FIRST_NAME$
- $LAST_NAME$
- $DISPLAY_NAME$
- $USER_DN$
- $USER_UPN$
- $USER_LOCALE$
- $DEVICE_UUID$
- $DEVICE_UUID_NO_DASHES$
- $DEVICE_UDID$
- $DEVICE_IMSI$
- $DEVICE_IMEI$
- $DEVICE_SN$
- $DEVICE_ID$

- $DEVICE_MAC$
- $DEVICE_CLIENT_ID$
- $USER_CUSTOM1$
- $USER_CUSTOM2$
- $USER_CUSTOM3$
- $USER_CUSTOM4$
- $REALM$
- $TIMESTAMP_MS$
- $RANDOM_16$
- $RANDOM_32$
- $RANDOM_64$
- $CONFIG_UUID$*

* This substitution variable works only for the values under the **Subject Alternative Names** section for the following configurations: Entrust, Local, SCEP, Symantec Managed KPI. It is used for Sentry certificate-based tunneling (CBT).

Configuring a client-provided certificate enrollment setting

This section covers client-provided certificate enrollment settings.

Client-provided certificate enrollment settings are applicable only to iOS and Android devices.

Overview of client-provided certificate enrollment settings

Derived credentials are identity certificates derived from the certificates on a smart card. The derived credentials are stored on the device in Mobile@Work on iOS devices, and in Secure Apps Manager on Android devices. AppConnect apps on mobile devices can use derived credentials for these purposes:

- authentication to backend servers, such as email servers, web servers, or app servers
- digital signing

- encryption
- decryption of older emails for which the original encryption certificate has expired (iOS only)
- authenticating the user to Standalone Sentry when using AppTunnel with Kerberos authentication to the backend server

You create a client-provided certificate enrollment setting when you want an AppConnect app to use derived credentials for one of these purposes. You then refer to the client-provided certificate enrollment in the appropriate setting.

The certificate enrollment setting is called *client-provided* because Mobile@Work for iOS or Secure Apps Manager for Android, known as *client* apps, provide the identity certificate to the AppConnect app.

Only the following settings can refer to a client-provided certificate enrollment setting:

- AppConnect app configuration

  It can refer to a client-provided certificate enrollment setting in:

  - the value in a key-value pair in its **App-specific Configurations** section
  - the identity certificate in its **AppTunnel Rules** section
- Web@Work setting

  It can refer to a client-provided certificate enrollment setting in:

  - the value in a key-value pair in its **Custom Configurations** section
  - the identity certificate in its **AppTunnel Rules** section
- Docs@Work setting

  It can refer to a client-provided certificate enrollment setting in:

  - the value in a key-value pair in its **Custom Configurations** section
  - the identity certificate in its **AppTunnel Rules** section

Make sure the version of Mobile@Work for iOS or the Secure Apps Manager for Android on the device supports client-provided certificate enrollment settings as shown in the following table:

Reference to the client-provided certificate enrollment setting	**iOS:** **Mobile@Work prior to 8.5**	**iOS:** **Mobile@Work 8.5 and 8.6**	**iOS:** **Mobile@Work 9.0 or supported newer versions**	**Android:** **All versions of Secure Apps Manager supported or compatible with Core**
In key-value pairs	Not supported	Supported	Supported	Supported
In AppTunnel rules	Not supported	Not supported	Supported	Not supported

Related topics

- *Core Derived Credentials Guide*
- PIV-D Manager App for iOS Release Notes
- *PIV-D Entrust App for Android Release Notes*

Specifying a client-provided certificate enrollment setting

To specify a client-provided certificate enrollment setting:

1. Go to **Policies & Configs** > **Configurations**.
2. Select **Add New** > **Certificate Enrollment** > **Client-Provided**.
3. In the New Client-Provided Certificate Enrollment Setting dialog box, use the following guidelines to specify your settings.

Item	**Description**
Name	Enter brief text that identifies this certificate enrollment setting.
Description	Enter additional text that clarifies the purpose of this certificate enrollment setting.
Select purpose	Select one of the following, depending on the intended use of the client-provided identity certificate:

Item	Description
	• **Authentication** • **Decryption** • **Encryption** • **Signing**
Provider	Select the derived credential provider.

4. Click **Save**.

Configuring an Entrust CA

Core supports integration with the Entrust Administration Services (EAS). This integration allows Core to work with Entrust to obtain certificates directly from the CA.

Entrust Prerequisites

The information in this section assumes the following:

- You have the URL for your Entrust server (received from Entrust).
- You have the Admin ID and password.

Procedure

1. Go to **Policies & Configs** > **Configurations** and click **Add New** > **Certificate Enrollment** > **Entrust**.
2. Use the following guidelines to specify the settings.
   - **Name**: Enter brief text that identifies this group of settings.
   - **Description**: Enter additional text that clarifies the purpose of this group.
   - **API URL**: Enter the URL for your Entrust server (received from Entrust).
   - **Admin ID**: The administrator credentials to log into the Entrust server.
   - **Admin Password**: Enter the Admin Password.

- **Group**: The Entrust group associated with users. Custom attribute variable substitutions are supported.

  ⓘ If the profile you selected contains an iggroup variable, then the you must configure the same value here as well

- **Key Usage**: Use these options to filter out the certificates returned by Entrust, which may return multiple certificates with different uses depending on the selected profile.

  ⓘ When multiple certificates are returned by a DigitalID profile, the first one that matches the selected key usage flags is used. If none of the returned certificates match the selected key usage flags, an error is raised. Use the **Issue Test Certificate** feature to ensure the expected certificate is selected.

- **Profile**: Use these options to filter out the certificates returned by Entrust, which may return multiple certificates with different uses depending on the selected profile.

  Select a profile template from Entrust. Once you select this profile, more options (required and optional variables) are available to you based on the profile you select. Entrust refers to profiles as DigitalIDs.

- **Profile Description**: Pre-populated based on the profile you select.
- **Application Description**: Pre-populated based on the profile you select.
- **Centralized**: Select to allow Core to retrieve certificates on behalf of devices.
- **Decentralized**: Select to let managed devices retrieve their own certificates.

  This feature is supported on iOS devices only.
  Store keys on Core: Specifies whether Core stores the private key sent to each device. When storing keys is enabled, private keys are encrypted and stored on the local Core.

  - If you select this option **after** devices have been provisioned, certificates will be re-provisioned for all impacted devices.

- **User Certificate**: Specifies that the certificate is distributed to multiple devices assigned to a single user.

- **Device Certificate**: Specifies that the certificate is bound to the given device.
- **Entrust SCEP CA**:
  - **URL**: Enter the URL of the Entrust SCEP CA.
  - **Key Type**: Select RSA.
  - **Subject Alternative Names table**: Select a type and value. At run-time, these variables are resolved into user values. (See "Certificate Enrollment settings" on page 297 for more information.) Custom attribute variable substitutions are supported.

3. (Optional) Click **Issue Test Certificate** to verify the configuration by generating a test certificate to ensure there are no errors. Although this step is optional, it is recommended. A real certificate is not generated.
4. Click **Save**.

If values that you enter in fields result in errors, you cannot save the configuration. If values that you enter result in warnings, you can save the configuration after confirming the warning messages. To see configuration errors, go to **Services > Overview.**

Revoking the certificate

You can revoke an Entrust API Version 9 certificate.

Revoking a certificate adds the certificate to the CRL (Certificate Revocation List). The certificate is also removed from the Entrust manager. When a device authenticates with Core, the system first checks the CRL to verify that the certificate is not on the list. If the certificate is on the list, authentication fails.

To revoke a certificate:

1. Navigate to **Logs** > **Certificate Management**.
2. Select the certificate that you want to revoke.
3. Select **Actions** > **Revoke**.

Configuring a GlobalSign CA

Core supports integration with GlobalSign as a certificate authority (CA) for certificate enrollment. This integration enables GlobalSign to perform the proxy tasks that would normally be performed by Core, allowing the device to obtain certificates from the GlobalSign CA.

GlobalSign Prerequisites

The information in this section assumes that you have set up the following information with GlobalSign:

- A user name and password for Core to use to access the GlobalSign server
- GlobalSign profiles
- Whether you want the generated certificates to have the enhanced key usage extension Encrypting File System (EFS)
- Whether you want the generated certificates to be the GlobalSign type “personal” or “department”

To specify GlobalSign settings:

1. Go to **Policies & Configs** > **Configurations** and click **Add New** > **Certificate Enrollment** > **GlobalSign**.
2. Use the following guidelines to specify the settings.
    - **Name**: Enter brief text that identifies this certificate enrollment setting.
    - **Description**: Enter additional text that clarifies the purpose of this certificate enrollment setting.
    - **Store keys on Core**: Specifies whether Core stores the private key sent to each device. When storing keys is enabled, private keys are encrypted and stored on the local Core.

      If you select this option **after** devices have been provisioned, certificates will be re-provisioned for all impacted devices.
    - **User Certificate**: Specifies that the certificate is distributed to multiple devices assigned to a single user.
    - **Device Certificate**: Specifies that the certificate is bound to the given device.

- **URL**: Enter the URL for the GlobalSign server. This field defaults to:

  https://system.globalsign.com/cr/ws/GasOrderService

  Typically, you only change this if you are working with a GlobalSign test environment.

- **User Name**: The user name for Core to use to access the GlobalSign server. Custom device and user attributes variable names are supported.

- **Password**: Enter the password then re-enter to confirm. Custom device and user attributes variable names are supported.

- **Profile**: Click **Refresh** to populate the drop-down list of profiles from GlobalSign. Then, select a profile.

  ⓘ You must enter a valid **User Name** and **Password** before clicking **Refresh**.

- **Profile Description**: Pre-populated based on the profile you select.

- **Application Description**: Pre-populated based on the profile you select.

- **Product Code**: Select either **EPKIPSPersonal** or **EPKIPSDept**, depending on whether you want the generated certificates to be the GlobalSign type “personal” or “department”.

- **Certificate Expiration**: Specify when the generated certificate will expire.

- **EFS option**: Select this setting if you want the generated certificate to have the enhanced key usage extension Encrypting File System (EFS).

  Selecting this setting has no impact if the selected profile has disabled EFS.

- **Common Name**: Specify the Common Name to use in the generated certificate.

- **Organization Unit**: Specify the Organization Unit to use in the generated certificate.

- **E-Mail**: Specify the email address to use in the generated certificate.

- **Subject Alternative Names Value**: Enter a type and value. At run-time, these variables are resolved into user values. Add multiple SAN entries with corresponding values. Click **Add+**, select the SAN type (NT Principal Name) from the drop-down list, then select one of the available values. (See "Supported variables for certificate enrollment" on page 299 for more information.)

3. (Optional) Click **Issue Test Certificate** to verify the configuration by generating a test certificate to ensure there are no errors. Although this step is optional, it is recommended. A real certificate is not generated.

4. Click **Save**.

If values that you enter in fields result in errors, you cannot save the configuration. If values that you enter result in warnings, you can save the configuration after confirming the warning messages. To see configuration errors, go to **Services > Overview.**

Revoking the certificate

You can revoke a GlobalSign certificate.

Revoking a certificate adds the certificate to the CRL (Certificate Revocation List). The certificate is also removed from the GlobalSign server. When a device authenticates with Core, the system first checks the CRL to verify that the certificate is not on the list. If the certificate is on the list, authentication fails.

To revoke a certificate:

1. Navigate to **Logs** > **Certificate Management**.

2. Select the certificate that you want to revoke.

3. Select **Actions** > **Revoke**.

Configuring Core as the CA

This section describes how to configure Core as the CA.

Procedure

To specify local settings:

1. Go to **Policies & Configs** > **Configurations.**

2. Click **Add New** > **Certificate Enrollment** > **Local**.

3. Use the following guidelines to specify the settings.

    - **Name**: Enter brief text that identifies this group of settings. Example: Local Certificate Settings for Wi-Fi

    - **Description**: Enter additional text that clarifies the purpose of this group of settings.

    - **Store keys on Core**: Specifies whether Core stores the private key sent to each device. When storing key is enabled, private keys are encrypted and stored on the local Core.

      If you select this option **after** devices have been provisioned, certificates will be re-provisioned for all impacted devices.

      Select this option for certificates used for email on devices with multi-user sign-in.

    - **User Certificate**: Specifies that the certificate is distributed to multiple devices assigned to a single user.

      Select this option for certificates used for email on devices with multi-user sign-in.

    - **Device Certificate**: Specifies that the certificate is bound to the given device.

    - **Local CAs**: Select the name of the self-signed certificate you generated.

    - **Key Type**: Specifies the key exchange algorithm used (typically RSA or elliptic curve).

    - **Subject**: Enter an X.509 name represented as an array of OIDs and values.

      See "Supported variables for certificate enrollment" on page 299 for more information.

    - **Subject Common Name Type**: Select the CN type specified in the certificate template. If you enter the $USER_DN$ variable in the Subject field, select **None** from the drop-down list.

    - **Key Usage**: Specify acceptable use of the key (signing and/or encryption).

    - **Key Length**: Select a Key Length.

      The values are 1024, 1536, 2048 (the default), 3072, and 4096.

- **CSR Signature Algorithm**: Select the signature algorithm.

  The values are SHA1, SHA256, SHA384 (default), and SHA512.

- **Subject Alternative Names table**: Enter a type and value. At run-time these variables are resolved into user values.

  See "Supported variables for certificate enrollment" on page 299 for more information.

4. (Optional) Click **Issue Test Certificate** to verify the configuration by generating a test certificate to ensure there are no errors. Although this step is optional, it is recommended. A real certificate is not generated.

5. Click **Save**.

If values that you enter in fields result in errors, you cannot save the configuration. If values that you enter result in warnings, you can save the configuration after confirming the warning messages. To see configuration errors, go to **Services > Overview.**

Revoking the certificate

You can revoke a local certificate.

Revoking a certificate adds the certificate to the CRL (Certificate Revocation List). When a device authenticates with Core, the system first checks the CRL to verify that the certificate is not on the list. If the certificate is on the list, authentication fails.

Procedure

1. Navigate to **Logs** > **Certificate Management**.

2. Select the certificate that you want to revoke.

3. Click **Actions** > **Revoke**.

Configuring OpenTrust CA

Core supports integration with the OpenTrust Mobile Provisioning Server (MPS). This integration enables OpenTrust to perform the proxy tasks that would normally be performed by Core. The following describes the configuration in Core.

Note the following - for Compatibility:

- This integration does not support the pushing Certificate Authorities Bundles to devices, which is offered by OpenTrust.
- Core supports one certificate per OpenTrust configuration. OpenTrust supports creating profiles having multiple credentials (called application in the OpenTrust context).

Before you begin

The information in this section assumes the following:

- You have the URL for your OpenTrust cloud instance.
- You have the client-side JSON connector identity certificate Core will use to authenticate to the MPS.
- You have implemented a centralized OpenTrust cloud.
- You have created a Mobile Management Profile on MPS containing a single centralized credential.

Procedure

1. Go to **Policies & Configs > Configurations** and click **Add New > Certificate Enrollment > OpenTrust**.
2. Use the following guidelines to specify the settings:

   Although optional fields are not required by OpenTrust, they are still used if present. Therefore, you must still specify the appropriate variable for each optional field. For example, the phone number might be an optional field because the tablets in your organization do not have phone numbers. However MPS might still use this information to request a certificate from the PKI server if it is present.

   - **Name**: Enter brief text that identifies this group of settings.
   - **Description**: Enter additional text that clarifies the purpose of this group.
   - **Store keys on Core**: Specifies whether Core stores the private key sent to each device. When storing key is enabled, private keys are encrypted and stored on the local Core.
   - If you select this option after devices have been provisioned, certificates will be re-provisioned for all impacted devices

- **User Certificate**: Specifies that the certificate is distributed to multiple devices assigned to a single user.
- **Device Certificate**: Specifies that the certificate is bound to the given device.
- **API URL**: Enter the URL for the OpenTrust server.
- **Certificate 1**: This is the name of the uploaded certificate.
- **Password 1** (Optional): This password is optional.
- **Add Certificate**: Click this link to add one or more certificates, as necessary.
- **Profile**: This is the MPS Mobile Profile to use for the integration. If you do not see an expected profile, then it most likely contains multiple credentials, a configuration that Core does not currently support.
- **Profile Description**: This is pre-populated based on the profile you select.
- **Application Description**: This is populated automatically with the corresponding OpenTrust content associated with the selected profile.

3. (Optional) Click **Issue Test Certificate** to verify the configuration by generating a test certificate to ensure there are no errors. Although this step is optional, it is recommended. A real certificate is not generated.
4. Click **Save**.

ⓘ If values that you enter in fields result in errors, you cannot save the configuration. If values that you enter result in warnings, you can save the configuration after confirming the warning messages. To see configuration errors, go to **Services > Overview.**

Revoking the certificate

You can revoke a OpenTrust certificate.

Revoking a certificate adds the certificate to the CRL (Certificate Revocation List). The certificate is also removed from the OpenTrust manager. When a device authenticates with Core, the system first checks the CRL to verify that the certificate is not on the list. If the certificate is on the list, authentication fails.

Procedure

1. Navigate to **Logs > Certificate Management**.
2. Select the certificate that you want to revoke.
3. Click **Actions > Revoke**.

Configuring a single file identity certificate enrollment setting

Use a single file identity certificate enrollment setting to upload an identity certificate to Core for distribution to devices. A typical use case for a single file identity certificate is using the certificate to authenticate devices to a network server, such as:

- Standalone Sentry
  When device authentication on Standalone Sentry is configured as Group Certificate, you typically distribute the same identity certificate to multiple devices.
- a Wi-Fi network component
  When you configure a Wi-Fi setting to use TLS or TTLS for its EAP type, you can distribute the same identity certificate to multiple devices.
- a VPN network component
  When you configure a VPN setting, depending on the type of VPN setting, you can use certificate-based authentication. For the authentication, you can distribute the same identity certificate to multiple devices.

You can upload either:

- An identity certificate.
  The certificate is a PKCS 12 certificate which contains exactly one private key. It is a .p12 or .pfx file. The file can optionally include the certificate chain. The certificate chain can include only intermediate certificates, or intermediate certificates through the root certificate. The root certificate is not necessary if it is from a well known certificate authority.
  You also provide the password for the identity certificate’s private key.

- Multiple files, which include among them:
  - the private key and its password.
  - the public certificate.
  - the supporting certificates in the certificate chain. The root certificate is not necessary if it is from a well known certificate authority.
- Examples of combinations you can upload are:
  - a .p12 or .pfx file containing a an identity certificate and its private key and password, plus additional .pem files containing the intermediate certificates.
  - a .pem file containing the private key and password, a .pem file containing the public certificate, plus additional .pen files containing the intermediate certificates.

Procedure

1. Log in to the Admin Portal.
2. Go to **Policies & Configs** > **Configurations**
3. Click **Add New** > **Certificate Enrollment** > **Single File Identity**.
4. Fill in the entries:
   - **Name**: Enter brief text that identifies certificate enrollment setting.
   - **Description**: Enter additional text that clarifies the purpose of this certificate enrollment setting.
   - **Certificate 1**: Click **Browse** to select the .p12 or .pfx file of the identity certificate, if you are uploading only one file.
   - If you are uploading multiple files, select the file (.p12, .pfx, or .pem) that contains the private key.
   - **Password 1**: Enter the password for the certificate’s private key.
5. If you are uploading multiple files, click **Add Certificate** to add another file.

6. Fill in the entries:

   - **Certificate 2**: Click **Browse** to select the .pem file to upload to Core Core. The certificate must be formatted as binary DER or ASCII PEM.
   - **Password 2**: The Password field is applicable only for the file that contains the private key.

7. Optionally, click **Add Certificate** to add another file**.**

8. Click **Save**.

After you save the single file identity certificate enrollment setting, you can view or change the certificate by editing the setting.

Configuring SCEP

This section describes how to specify settings that allow the device to obtain certificates from a certificate authority (CA) using Simple Certificate Enrollment Protocol (SCEP). For information about certificate pinning for SCEP enrollment configurations, see "Configuring certificate pinning for registered devices" in the Security Settings > Certificate Mgmt section of the *Core System Manager Guide*.

Create the SCEP enrollment certificate

To create a new SCEP certificate of enrollment:

1. Go to **Policies & Configs** > **Configurations** and click **Add New** > **Certificate Enrollment** > **SCEP**.

2. Use the following guidelines to specify the settings:

   - **Name**: Enter brief text that identifies this group of settings.
   - **Description**: Enter additional text that clarifies the purpose of this group.
   - **Centralized**: Core retrieves certificates on behalf of devices. Core also manages the certificate lifetime and triggers renewals. See “"SCEP proxy functions" on page 319”.

     Select this option for certificates used for email on devices with multi-user sign-in.

- **Decentralized**: Devices retrieve their own certificates.

  Use this feature if using the SCEP setting for mutual authentication. It is not supported for any other use cases with Android devices. See "Enabling mutual authentication for Apple and Android devices" on page 293.

- **Store keys on Core**:

  Specifies whether Core stores the private key sent to each device. When storing key is enabled, private keys are encrypted and stored on the local Core.

  If you select this option after devices have been provisioned, certificates will be re-provisioned for all impacted devices.

  ⓘ Select this option for certificates used for email on devices with multi-user sign-in.

- **Proxy requests through Core**:

  When this option is enabled, Core acts as a reverse proxy between devices and the target certificate authority. This option is only available when **Decentralized** is selected.

- **User Certificate**: Specifies that the certificate is distributed to multiple devices assigned to a single user.

  ⓘ Select this option for certificates used for email on devices with multi-user sign-in.

- **Device Certificate**: Specifies that the certificate is bound to the given device.
- **URL**: Enter the URL for the SCEP server.
- **CA-Identifier**: (Optional) Enter the name of the profile for SCEP servers that support named-profiles.

- **Subject**: Enter an X.509 name represented as a comma-separated array of OIDs and values. Typically, the subject is set to the user's fully qualified domain name. For example,

  C=US,DC=com,DC=MobileIron,OU=InfoTech or

  CN=www.mobileiron.com.

  You can also customize the Subject by appending a variable to the OID. For example, CN=www.mobileiron.com-$DEVICE_CLIENT_ID$.

  For ease of configuration you can also use the $USER_DN$ variable to populate the Subject with the user's FQDN.

- **Subject Common Name Type**: Select the CN type specified in the certificate template. If you enter the $USER_DN$ variable in the Subject field, select None from the drop-down list.
- **Key Usage**: Specify acceptable use of the key by signing.
- **Encryption**: Specify acceptable use of the key by encryption.
- **Key Type**: Specify the key type.
- **Key Length**: The values are 1024, 1536, 2048 (the default), 3072, and 4096.
- **CSR Signature Algorithm**: The values are SHA1, SHA256, SHA384 (default), and SHA512.
- **Finger Print**: The finger print of the CA issuing the root certificate.
- **Challenge Type**: Select **None**, **Microsoft SCEP**, or **Manual** to specify the type of challenge to use. The Challenge Type will depend on what the NDES server is configured to use.
- **Challenge URL**: For a Microsoft SCEP challenge type, enter the URL of the trustpoint defined for your Microsoft CA.
- **User Name**: Enter the user name for the Microsoft SCEP CA.
- **Password**: Enter the password for the Microsoft SCEP CA.

- **Subject Alternative Names Type**: Select NT Principal Name, RFC 822 Name, or None, based on the attributes of the certificate template. You can enter four alternative name types.

  If this SCEP setting is for authenticating the device to the Standalone Sentry using an identity certificate: select NT Principal Name and select Distinguished Name for a second Subject Alternative Name

- **Subject Alternative Names Value**: Select the Subject Alternate Name Value from the drop-down list of supported variables. You can also enter custom variables in addition to and instead of the supported variables.

  If this SCEP setting is for authenticating the device to the Standalone Sentry using an identity certificate: enter $USER_UPN$ for the value corresponding to NT Principal Name and enter $USER_DN$ for the value corresponding to Distinguished Name.

3. (Optional) Click **Issue Test Certificate** to verify the configuration by generating a test certificate to ensure there are no errors. Although this step is optional, it is recommended. A real certificate is not generated.

4. Click **Save**.

   You cannot make changes to the saved SCEP settings. When you open a saved SCEP setting, the **Save** button is disabled.

   If values that you enter in fields result in errors, you cannot save the configuration. If values that you enter result in warnings, you can save the configuration after confirming the warning messages. To see configuration errors, go to **Services > Overview.**

X.509 Codes

The Subject field uses an X.509 distinguished name. You can use one or more X.509 codes, separated by commas. This table describes the valid X.509 codes:

TABLE 67. X.509 CODES

Code	Name	Type	Max Size	Example
C	Country/Region	ASCII	2	C=US
DC	Domain Component	ASCII	255	DC=company, DC=com

TABLE 67. X.509 CODES (CONT.)

Code	Name	Type	Max Size	Example
S	State or Province	Unicode	128	S=California
L	Locality	Unicode	128	L=Mountain View
O	Organization	Unicode	64	O=Company Name, Inc.
OU	Organizational Unit	Unicode	64	OU=Support
CN	Common Name	Unicode	64	CN=www.company.com

If the SCEP entry is not valid, then you will be prompted to correct it; partial and invalid entries cannot be saved.

SCEP proxy functions

You can enable SCEP proxy functions. The benefits for this include:

- A single certificate verifies Exchange ActiveSync, Wi-Fi, and VPN configurations
- There is no need to expose a SCEP listener to the Internet.
- Core can detect and address revoked and expired certificates.

Uploading a Certificate Authority chain for SCEP enrollment configurations

With Core 11.4.0.0 and later releases, you can upload a specific Certificate Authority (CA) chain for Simple Certificate Enrollment Protocol (SCEP) enrollment configurations. In some cases, the SCEP CA may send more CA certificates than you need. When you need to use a specific certificate chain, use this feature to upload that exact chain.

Before you begin

- You must have a valid SCEP enrollment configuration to use this feature. See "Create the SCEP enrollment certificate" on page 315. If you do not upload a CA chain, Core continues its previous behavior of using the CA certificates directly acquired from the SCEP server.

  > The option to upload the CA chain is available only for SCEP enrollment configurations. Certificate enrollment settings such as **System - Mutual Auth CE** setting use a local CA, which is already available on Core.

- Client mutual authentication must be enabled to use this feature. See "Mutual authentication client identity certificate" on page 287.

Procedure

1. From the Admin portal, navigate to the Settings > System Settings > Security > Certificate Authentication > **Client Mutual Certificate Authentication** page.

2. From the **Certificate Enrollment Setting** menu, select one of the SCEP enrollment configurations from the dropdown menu.

3. Select the option to upload the CA certificate chain.

4. After uploading the CA certificate chain, click **Save**.

Configuring Symantec Managed PKI

Symantec Managed PKI support enables you to configure certificate-based authentication. Symantec Managed PKI is a source for certificates that you can reference in a variety of configurations, such as for Exchange, VPN, and AppConnect.

Before you begin

Before you begin, make sure you have the following in place:

- A valid Symantec Verisign Managed PKI account is required.

- (Optional) Get finger print from issuing CA for root certificate.

- One or more client certificate and password from CA.

Procedure

To specify the Symantec Managed PKI settings:

1. Go to **Policies & Configs** > **Configurations** and click **Add New** > **Certificate Enrollment** > **Symantec Managed PKI**.
2. Use the following guidelines to specify the settings:
   - **Name**: Enter brief text that identifies this group of settings.
   - **Description**: Enter additional text that clarifies the purpose of this group.
   - **Centralized**: Core retrieves certificates on behalf of devices. Core also manages the certificate lifetime and triggers renewals. See “"Using a proxy" on the next page”.

     ⓘ Select this option for certificates used for email on devices with multi-user sign-in.
   - **Decentralized**: Devices retrieve their own certificates.
   - **Store keys on Core**: Specifies whether Core stores the private key sent to each device. When storing key is enabled, private keys are encrypted and stored on the local Core.

     If you select this option **after** devices have been provisioned, certificates will be re-provisioned for all impacted devices.

     ⓘ Select this option for certificates used for email on devices with multi-user sign-in.
   - **Proxy requests through Core**:
     - When this option is enabled, Core acts as a reverse proxy between devices and the target certificate authority. This option is only available when **Decentralized** is selected.
   - **User Certificate**: Specifies that the certificate is distributed to multiple devices assigned to a single user.

     ⓘ Select this option for certificates used for email on devices with multi-user sign-in.
   - **URL Mode**: Specifies the mode and the corresponding URL supplied by Symantec.
   - **CA-Identifier**: Required information supplied by Symantec.

- **Subject**: See "Supported variables for certificate enrollment" on page 299 for more information.
- **Subject Common Name Type**: Select the CN type specified in the certificate template. If you enter the $USER_DN$ variable in the Subject field, select **None** from the drop-down list.
- **Key Usage**: Use these options to indicate which key usage to request from the CA.
- **Key Type**: This is the Key Exchange algorithm: RSA or Elliptic Curve.
- **Key Size**: The values are 1024, 1536, 2048 (the default), 3072, and 4096.
- **CSR Signature Algorithm**: The values are SHA1, SHA256, SHA384 (the default), and SHA512.
- **Finger Print**: The finger print of Symantec Managed PKI.
- **Certificate 1**: Upload for the client authentication with the server.
- **Password 1**: This password is optional.Best used when certificate and password are in separate files.
- **Subject Alternative Names table**: Enter a type and value. At run-time these variables are resolved into user values. (See "Supported variables for certificate enrollment" on page 299 for more information.)

  The Required Fields and Optional Fields for the certificate are displayed based on how the MDM (Web Service Client) profile was set up in the Symantec PKI manager.

3. (Optional) Click **Issue Test Certificate** to verify the configuration by generating a test certificate to ensure there are no errors. Although this step is optional, it is recommended. A real certificate is not generated.
4. Click **Save**.

   If values that you enter in fields result in errors, you cannot save the configuration. If values that you enter result in warnings, you can save the configuration after confirming the warning messages. To see configuration errors, go to **Services > Overview.**

Using a proxy

Choosing to enable proxy functions has the following benefits:

- A single certificate verifies Exchange ActiveSync, Wi-Fi, and VPN configurations
- There is no need to expose a SCEP listener to the Internet.
- Core can detect and address revoked and expired certificates.

Configuring Symantec Web Services Managed PKI

Integration with Symantec Web Services Managed PKI version 8.x enables you to configure certificate-based authentication. The following describes how to configure Symantec Web Managed PKI in Core.

Before you begin

- Set up your account for Symantec Web Services Managed PKI with Symantec.
- Create an MDM (Web Service Client) profile in the Symantec PKI manager that you will use for the Core integration.

  SeatID

  Be sure to include the Symantec SeatID as a required certificate profile field. In a Symantec Web Services Managed PKI environment, Symantec uses the SeatID to track the number of seats for billing purposes.

  To correctly track the number of seats, the SeatID value in the Core SCEP settings must map to the value you created for the SeatID in the Symantec PKI Manager. For example, if the user's email address is used as the SeatID in Symantec PKI Manager, the Core SCEP settings should map the Core email address attribute to the Symantec SeatID.

  Core associates each issued Symantec certificate to a SeatID in the Symantec PKI Manager. If the SeatID does not exist, a new Symantec user account and SeatID is automatically created for the user at the time the certificate is requested.
- Gather the following items:
  - The server address for the Symantec Web Services Managed PKI.
    On Core the default is set to pki-ws.symauth.com.
  - The Registration Authority (RA) certificate Core will use to authenticate to the Symantec CA.

Procedure

1. Go to **Policies & Configs > Configurations** and click **Add New > Certificate Enrollment > Symantec Web Managed PKI**.

2. Use the following guidelines to specify the settings:

   > The Required Fields and Optional Fields for the certificate are displayed based on how the MDM (Web Service Client) profile was set up in the Symantec PKI manager.

   - **Name**: Enter brief text that identifies this group of settings.
   - **Description**: Enter additional text that clarifies the purpose of this group.
   - **Store keys on Core**: Specifies whether Core stores the private key sent to each device. If you are using a Symantec profile that is set up to store keys on the Symantec server, you typically do not select this option.

     > If you select this option after devices have been provisioned, certificates will be re-provisioned for all impacted devices.

   - **User Certificate**: Specifies that the certificate is distributed to multiple devices assigned to a single user.

     The certificate is revoked when the user is removed from Core.

   - **Device Certificate**: Specifies that the certificate is bound to the given device. Make sure the Symantec certificates are unique for each device.

     The certificate is revoked when the device is retired from Core.

   a. **API URL**: Enter the server address for the Symantec Web Services Managed PKI (received from Symantec).

      The default is set to pki-ws.symauth.com.

      > Do not add https:// before the server name, and do not add path information after the server name.
      > Only the hostname of the Symantec CA server should be provided.

   - **Certificate 1**: Navigate and select the RA certificate you received from Symantec. This is usually a.p12 file. Enter the password for the certificate when prompted.
   - **Password 1**: (Optional if certificate and password are stored in the same file.) Enter the password for the certificate.
   - **Add Certificate**: Click this link to add one or more certificates, as necessary.
   - **Profile**: This is the profile to be used for the integration. If you do not see an expected profile, then it most likely contains multiple credentials, a configuration that Core does not currently support.
   - **Profile Description**: This is pre-populated based on the profile you select.
   - **Application Description**: This is populated automatically based on the selected profile.

3. (Optional) Click **Issue Test Certificate** to verify the configuration by generating a test certificate to ensure there are no errors. Although this step is optional, it is recommended. A real certificate is not generated.
4. Click **Save**.

ⓘ If values that you enter in fields result in errors, you cannot save the configuration. If values that you enter result in warnings, you can save the configuration after confirming the warning messages. To see configuration errors, go to **Services > Overview.**

Revoking the certificate

You can revoke a Symantec Web Services Managed PKI certificate.

Revoking a certificate adds the certificate to the CRL (Certificate Revocation List). The certificate is also removed from the Symantec Web Services Managed PKI manager. When a device authenticates with Core, the system first checks the CRL to verify that the certificate is not on the list. If the certificate is on the list, authentication fails.

Procedure

1. Navigate to **Logs** > **Certificate Management**.
2. Select the certificate that you want to revoke.

3. Click **Actions > Revoke**.

Configuring a user-provided certificate enrollment setting

One user-provided certificate enrollment setting for each purpose

Configure a user-provided certificate enrollment setting for every purpose for which users can upload a certificate (PKCS 12 file) in the user portal. For example, consider a case in which users have three different purposes for providing certificates: S/MIME signing, S/MIME encryption, and authenticating to a backend server. In this case, you create three user-provided certificate enrollment settings.

You provide a display name for each user-provided certificate enrollment setting. The display name you choose is important because the device user sees it in two places:

- in the user portal when deciding what certificate to upload
- In the user portal, the display name is called “configuration”. The user’s selection associates the uploaded certificate with a user-provided certificate enrollment setting. The user can upload the same certificate, or different certificates, for each display name.
- in Mobile@Work for iOS, when Mobile@Work for iOS prompts the user for the private key password.
- Mobile@Work prompts for the password if a password was not required when the user uploaded the certificate to the user portal. Mobile@Work uses the display name to inform the user about which certificate to provide the password for. For details, see "The private key password" on the next page.

Important notes

- The PKCS 12 file must contain the certificate and one private key. Core does not support PKCS 12 files with more than one private key.
- A web services V2 API is also available for uploading user-provided certificates to Core and associating the certificates with a user-provided certificate enrollment setting.
- See the *Core V2 API Guide*.

- The V1 API that uploaded user certificates to Core is no longer available. If you used the V1 API to upload user certificates, Core will continue to use the certificates until either:
  - the user uploads a replacement in the user portal
  - you use the V2 API to upload a replacement

    Note that the V1 API associated the user certificate with a certificate type: All, WIFI, VPN, SMIMESIGNING, SMIMEENCRYPTION, EMAIL or EXCHANGE. Although Core still supports using these certificates and their associated type, the user portal does not display these certificates in the user portal.

Core stores the certificate and private key

When the user uploads a user-provided certificate in the user portal, the user uploads a PKCS 12 file. Core stores the file, which includes the certificate and its private key. Core does not remove the PKCS 12 file after delivering it to the user's device. Therefore, if the user registers another device, the PKCS 12 file is available to deliver to the additional device.

The private key password

In each user-provided certificate enrollment setting, you specify whether the user is required to provide a password for the certificate's private key. When a password is required, users must provide a password when using the user portal to upload a certificate associated with this certificate enrollment setting.

Important: Always require a password unless both of the following are true: The devices that will use the user-provided certificate are iOS devices running Mobile@Work 9.0 or supported newer versions AND The apps that will use the certificate are AppConnect apps.

When you do not require a private key password when the user uploads a certificate, Mobile@Work for iOS and an AppConnect for iOS app that uses the certificate behave as follows:

1. When the AppConnect app launches, control switches to Mobile@Work for iOS.
2. Mobile@Work prompts the device user for the private key password.
3. The device user enters the password.

If the device user exits Mobile@Work without providing the password, when the AppConnect app next launches, Mobile@Work unauthorizes the app, with the reason that the app is missing credentials.

4. Control returns to the AppConnect app.

Whether you require a password depends on your security requirements. If a password is required, Core stores the password along with the PKCS 12 file containing the certificate and private key. However, if your security environment requires limiting the password’s storage to the device that uses the certificate, then do not require a password.

When the private key of a user-provided certificate is deleted

The private key of a PKCS 12 file, and password if provided, can be deleted from the Core file system. Whether you want the private key and password deleted from Core depends on your security requirements.

The following mechanisms are available to delete the private key and password:

- A user can delete the private key and password using the user portal.
- A web services API can delete the private key and password.
- You can specify in the Admin Portal that Core deletes private keys and passwords older than some number of days.

IMPORTANT: When the private key and associated password is deleted, Core retains the public certificate and maintains an entry in its certificate table so it can track where the certificate is used, when it expires and display information about it in the UI. Without the private key and associated password, Core is unable to use the identity certificate with any new certificate enrollments, AppConnect configuration and devices. Once the private key and associated password is deleted, the user-provided certificate must be uploaded again before it can be used.

Because the certificate without the private key is still available on Core, you can view information about the certificate, such as its expiration date. This information can help you manage devices still using the certificate.

Related topics

- "Viewing, replacing, and deleting certificates in the user portal" on page 460
- *Core V2 API Guide*

Specifying the settings for a user-provided certificate enrollment setting

To specify the settings for a user-provided certificate enrollment setting:

1. Go to **Policies & Configs > Configurations** and click **Add New > Certificate Enrollment > User-Provided**.
2. Use the following guidelines to specify the settings:
    - **Name**: Enter brief text that identifies this setting.
    - **Description**: Enter additional text that clarifies the purpose of this setting.
    - **Display Name**: Enter the name that will appear on the user portal where device users upload their certificates. This name also appears in Mobile@Work if Mobile@Work prompts the device user for a certificate’s private key password.
    - **Require Password**: This option requires the user to provide a password for the certificate’s private key when uploading a certificate associated with this certificate enrollment setting.
    - **Important**: Always require a password except as described in "The private key password" on page 327.
    - **Delete Private Keys After Days**: Select the number of days after a user-provided certificate is uploaded to Core after which Core deletes the private key and, if provided, its password, from Core.

      The default is **None**, which means Core does not delete the private key and its password.

      The default is **None**, which means Core does not delete the private key and its password.
3. Click **Save**.

Bridge

This section addresses components related to Bridge.

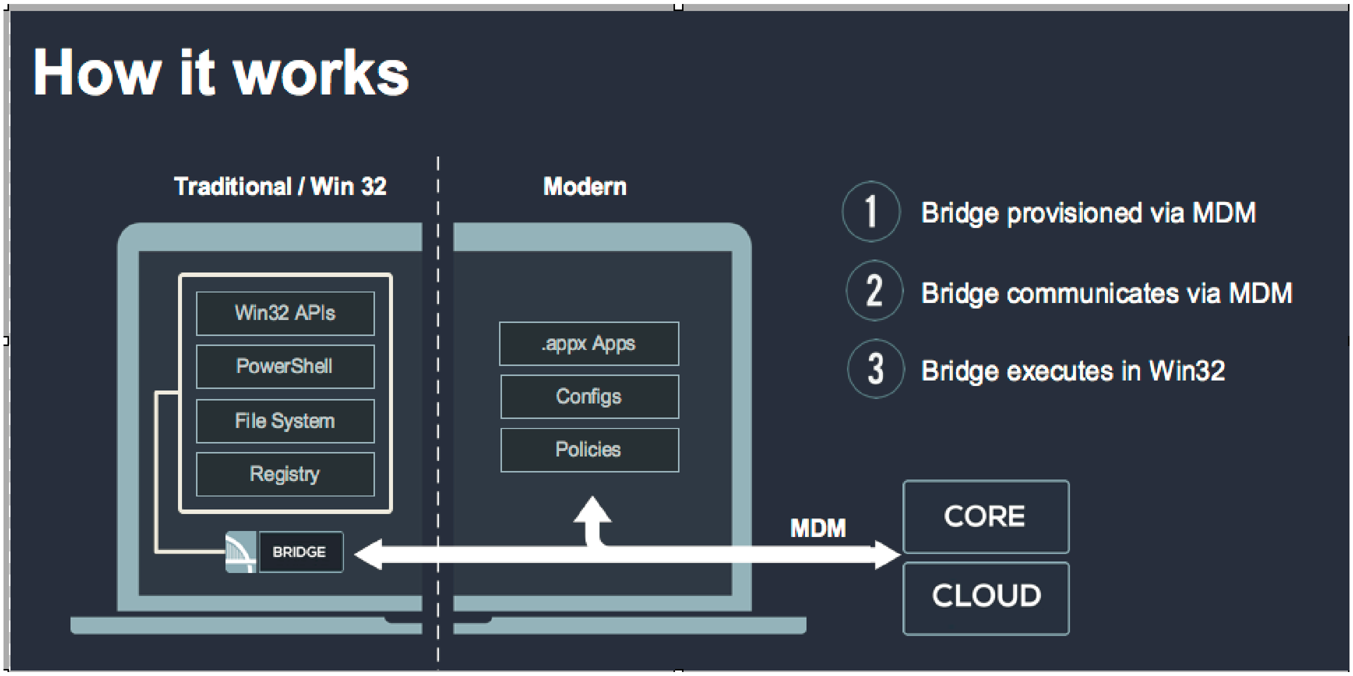
ⓘ Bridge is only used with Windows 10 Desktop devices.

Bridge overview

Core manages the modern partition of the Windows OS to secure Windows 10 Desktop devices using the MDM protocol. Bridge was developed, using the same MDM protocol, to manage the Traditional/Win32 half of the OS and secure legacy applications on Windows 10 Desktop devices.

By deploying the Bridge application to Windows 10 Desktop devices, enterprises can now use the same MDM protocol Core uses to send instructions to both partitions, use MDM API's and Group Policy Objects (GPOs) delivered via scripts to the device to better manage and secure devices.

FIGURE 1. BRIDGE ARCHITECTURE



Without Bridge, Core supports modern apps, configurations, and policies, but not Non-MSI wrapped Win32 apps. With Bridge, Core also supports the following files:

- PowerShell
- Registry
- Visual Basic scripts
- .EXE for Win32 application deployment

Some (but not all) of the actions you can take, using Bridge with Core, are to modify the device in the following areas:

- **Registry**: Reading, writing and updating registry values
- **Files**: Verify, read and update the contents of a file

Setting up Bridge

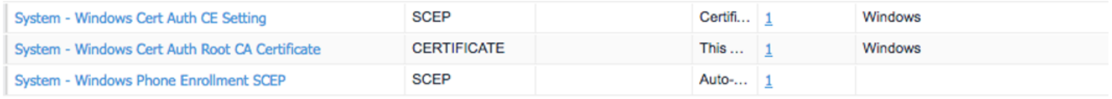
Setting up Bridge includes the following steps:

- **Step 1**: "Creating the Bridge certificate" below
- **Step 2**: "Enabling the Bridge certificate" below
- **Step 3**: "Deploying the Bridge app" on the next page
- **Step 4**: "Uploading scripts" on page 335

Creating the Bridge certificate

This step happens automatically, with no actions taken by administrators. Core creates a certificate with each latest release or update to be used by Bridge. This certificate is available to administrators to authenticate and communicate with both devices and servers.

FIGURE 1. BRIDGE SET UP



System - Windows Cert Auth CE Setting	SCEP		Certifi...	1	Windows
System - Windows Cert Auth Root CA Certificate	CERTIFICATE		This ...	1	Windows
System - Windows Phone Enrollment SCEP	SCEP		Auto-...	1	

Core sends this certificate to all Windows 10 Desktop devices at the time the Core Server is created and the Windows 10 device is registered.

Enabling the Bridge certificate

Before you can use Bridge, you must select the authentication certificate.

Procedure

1. Log into the Admin Portal.
2. Go to **Settings > System Settings > Windows > Certificate Authentication**.
3. Click the box next to **Enable certificate authentication for Windows 10 Bridge** to assign your cert for Bridge.

   You can also choose the same Certificate Enrollment with Apps@Work.

   If you use certificates for both Apps@Work and Bridge (by checking the **Enable certificate authentication for Windows 10 Apps@Work** option), Bridge uses the certificate in the device store and Apps@Work uses the certificate in the user store.
4. Click **Save**.

Deploying the Bridge app

Once the certificate is on the device you can deploy the Bridge app to Windows 10 Desktop devices.

Refer to the Apps@Work Guide for more information about managing applications for Windows devices.

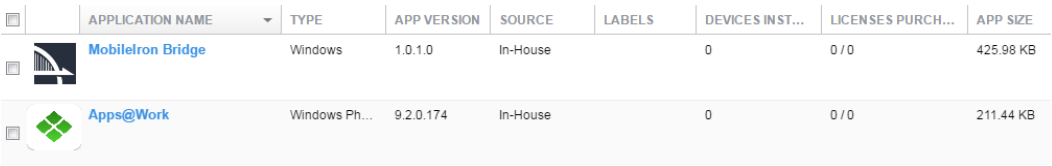
Procedure

1. Log into the Admin Portal.
2. Go to **Apps > App Catalog**.
3. Select the **MobileIron Bridge** app you want to install on the devices.

   There could be one or more versions of the app. For details on deploying the Bridge app, refer to the latest *Core Apps@Work Guide*

4. Sort the list, if necessary, to find the Bridge app.

FIGURE 2. FINDING BRIDGE APPS



□		APPLICATION NAME	TYPE	APP VERSION	SOURCE	LABELS	DEVICES INST...	LICENSES PURCH...	APP SIZE
□		MobileIron Bridge	Windows	1.0.1.0	In-House		0	0 / 0	425.98 KB
□		Apps@Work	Windows Ph...	9.2.0.174	In-House		0	0 / 0	211.44 KB

5. Select **Actions > Apply to Labels**.

6. Select the appropriate label(s) and click **Apply**.

   The app silently installs after devices sync with the label to which the Bridge app is associated.

Verifying Bridge installation

Once the app is deployed, administrators can view the device as a part of the application list by turning on the Windows 10 Inventory for Win32 applications.

Procedure

1. Log into the Admin Portal.
2. Go to **Policy & Configs > Policies**.
3. Select **Default Privacy Policy** and click the **Edit** button in the **Policy Details** pane.
4. Go to the **Windows 10 Inventory** section.
5. Click **Win 32 Inventory > Enabled > Save**.
6. Force a check-in or wait for the next sync period.
7. Go to **Devices & Users > Devices**.
8. Double-click a Windows 10 Desktop device.
9. Click the **Apps** tab to view the installed apps for the selected device.

Uploading scripts

There are two ways to manage actions in Bridge:

- "Uploading scripts using configurations" below
- "Pushing a single-use script to a device" below

Uploading scripts using configurations

After applying a label to a device with the Bridge app installed, the script is delivered the next time the device syncs with Core and the Bridge app executes the action defined by the script.

1. Log into the Admin Portal.
2. Go to **Policies & Configs > Configurations**.
3. Select **Add New > Windows > MobileIron Bridge (Windows 10 Only) > Script**.
4. Enter a name, upload an existing script, and click **Save.**
5. Select the configuration then click **Actions > Apply to Label**.
6. Select the appropriate label(s) and click **Apply**.

   When working with Bridge scripts make sure you have properly defined your labels by the types of devices (departments, geographically, etc.) you want to receive the actions created by the scripts.

Pushing a single-use script to a device

The other option for managing actions is by pushing a single-use Bridge script directly to a Windows 10 Desktop device. This is often useful for managing a single device for troubleshooting purposes.

Procedure

1. Log into the Admin Portal.
2. Go to **Devices & Users > Devices**.
3. Select a single device.

4. Select **Actions > Windows Only > MobileIron Bridge (Windows 10 only)**.

5. Enter a name, upload an existing Bridge Script, and click **Execute**.

Bridge script reversal

This feature allows administrators to set up Bridge action scripts (install scripts) as well as scripts to reverse those actions (uninstall scripts).

Not all actions have a corresponding undo action. Administrators need to be aware of these actions before attempting to upload uninstall scripts. In addition, Core cannot run an undo script if a user un-enrolls their device. To ensure that uninstall scripts can be activated, administrators need to restrict users from initiating MDM un-enrollment.

Administrators must complete the following prerequisites to successfully reverse script actions:

- Disable MDM un-enrollment by changing the lockdown policy for Windows devices and disabling MDM un-enrollment. See "Disabling MDM un-enrollment" on the next page section for details.

- Disable the phone reset feature by disabling the reset phone feature in the lockdown policy.

ⓘ Although Bridge is only available on Windows 10 Desktop devices, the disabling phone reset feature is still applicable to Bridge script reversal actions.

Resetting Windows 10 devices

To make sure users cannot un-enroll a device from MDM before Core can issue the undo scripts, administrators will want to reset the Windows 10 devices.

Procedure

1. Log into the Admin Portal.

2. Go to **Policies & Configs > Policies**.

3. Select the **Default Lockdown Policy** and then click **Edit**.

4. Scroll to the **Windows Phone - Corporate Owned Devices Only** section.

5. Select the **Disable** option for **Reset Phone**.

Disabling MDM un-enrollment

Procedure

1. Log into the Admin Portal.
2. Go to **Policies & Configs > Policies**.
3. Select **Default Lockdown Policies > Edit**.
4. Scroll to the **Windows Phone - Corporate Owned Devices Only** section.
5. Select the **Disable** option for **MDM Un-enrollment**.

Configuring reversal scripts

You can set up install and uninstall scripts at the same time. If you do not upload an uninstall script only the install script is used.

Setting up Bridge scripts and reversal scripts

1. Log into the Admin Portal.Go to **Policies & Configs > Configurations**.
2. Select **Add New > Windows > MobileIron Bridge (Windows 10 Only) > Scripts**.
3. Add a name for the configuration.
4. Enter a description and the target folder (optional).
5. Browse and select the action script in the **MobileIron Bridge Script** field.

   See "Supported variables as script arguments" on the next page for a list of arguments you can use.
6. Modify script arguments (optional).
7. Browse and select the reversal script in the **MobileIron Bridge Uninstall Script** field.

   See "Supported variables as script arguments" on the next page for a list of arguments you can use.

8. Modify script arguments (optional).
9. Click **Save**.

Supported variables as script arguments

- EMAIL
- USERID
- PASSWORD
- GOOGLE_AUTOGEN_PASSWORD
- FIRST_NAME
- LAST_NAME
- DISPLAY_NAME
- USER_DN
- USER_UPN
- USER_LOCALE
- DEVICE_UUID
- DEVICE_UUID_NO_DASHES
- DEVICE_UDID
- DEVICE_IMSI
- DEVICE_IMEI
- DEVICE_SN
- DEVICE_ID
- DEVICE_MAC
- DEVICE_CLIENT_ID
- USER_CUSTOM1

- USER_CUSTOM2
- USER_CUSTOM3
- USER_CUSTOM4
- MI_APPSTORE_URL
- REALM
- DEVICE_PIVD_ACTIVATION_LINK
- CN
- EMAIL_DOMAIN
- EMAIL_LOCAL
- OU
- SAM_ACCOUNT_NAME
- ICCID
- MODEL
- PHONE_NUMBER
- CONFIG_UUID
- TIMESTAMP_MS
- RANDOM_16
- RANDOM_32
- RANDOM_64

Enabling BitLocker

Using BitLocker allows Core administrators to encrypt data on Windows 10 Desktop devices and prevent the ability to copy data from a removable drive (such as a USB stick) to a fixed device and vice versa. Administrator create rules to enable BitLocker on Windows 10 Desktop devices to:

- encrypt devices
- enable USB sticks
- enable removable drives
- recover stored AD password
- recover a password from either AD or Core

Before you begin

Enable Bridge. See "Setting up Bridge" on page 332 for details.

Procedure

1. Log into the Admin Portal.
2. Go to **Policies & Configs > Policies**.
3. Click the **Default Security Policy** link and then click **Edit** in the Policy Details panel.
4. In the **Data Encryption** section, click **On** for **Data Encryption** to enforce the device password option.
5. In the **For Windows 10 Desktop** section, click Bit Locker On to enable it.
6. Make your configuration settings, referring to the "Enable BitLocker fields " on the next page table for details.
7. Click **Save.**

The encryption process begins after restarting the device. Depending on the size of the drive, the device can take anywhere from 45 minutes or longer to finish encrypting the device. This is a background process and does not interfere with the users. When a device is not encrypted it is shown out of compliance with Core until the encryption process is finished.

Bit Locker data encryption

The following table summarizes fields and descriptions for enabling **Bit Locker**:

TABLE 68. ENABLE BITLOCKER FIELDS

Fields	Description
Bit Locker	The options are **On** and **Off**. Bit Locker is applied only for Windows 10 desktop devices and only when Bridge is enabled.
Read Only for unencrypted removable drives	Click to encrypt removable drives (such as USB sticks) so the data is read only and cannot be moved to another device.
Read Only for unencrypted fixed drives	Click to encrypt fixed drives so the data is read only and cannot be moved to another device.
Encryption Type	The options are **128 bit** and **256 bit**.
Drive to encrypt	Select the OS drive you want to encrypt.
Recovery Options	You can recover a password and store it in Active Directory (AD), recover a password and store in both AD and Core, or disable password recovery.
TPM Options	TPM is Trusted Platform Module (used for encryption) and when configured requires the use of a password. The following options are for the users to set up startup passwords: A) If a user chooses the TPM option, then no additional startup password or startup PIN is required. Only the default Windows password is required. B) If a user chooses TPM + PIN option, then, in addition to the Windows password, the user is required to enter a startup PIN. This startup pin is required to be entered before the device boots up and loads windows. C) If a user chooses NO TPM, then in addition to the Windows password, the user is required to enter a startup password. This startup password is required to be entered before the device boots up and loads windows. ⓘ The startup PIN and password in B) and C) are in addition to the Windows password which is required in all 3 cases.
Restart Interval	Use this option to determine what the interval is after this security policy is applied before the device restarts.
Restart Message	Enter a message you want the user to see before the device restarts. If you do not enter a custom message, Core sends a default message.

Managing Windows device updates

To better manage security patches, administrators can create compliance policies based on update status or time periods. Devices that fall out of compliance are blocked from accessing specified services and applications such as Office 365 or Tunnel. Compliance information can also be sent to AAD for integration with Office 365.

Device update management is based on one or more of the following update status:

- Time of the last hotfix date
- Last hotfix ID
- Windows 10 build# on the device

View the update information in the **Device Details** page for selected devices.

This section contains the following topics:

- "Setting hotfix options" below
- "Setting up a compliance policy for device updates" on the next page

This feature requires Bridge. See "Setting up Bridge" on page 332 for details.

Setting hotfix options

This procedure describes how to set the hotfix options to obtain hotfix information such as the version and date.

Procedure

1. Log into the Admin Portal.
2. Go to **Policies & Configs** > **Configurations**.
3. Click **Add New** > **Windows** > **MobileIron Bridge**.
4. Select **Device Management** to open the **Device Management Settings** page.

5. Enter a name for the configuration.

   A description is optional.

6. Go to the hotfix section and click one or both of the **Allow** check boxes for the following options:

   - **View Last Hotfix Date**: to view the date of the most recent Windows hotfix update.
   - **View Last Hotfix ID**: to view the ID of the most recent Windows hotfix update.

7. Click **Save**.
8. Select the newly added configuration in the **Configurations** table.
9. Click **Actions > Apply to Label**.
10. Select a label associated with devices to track updates for hotfixes.
11. Click **Apply**.
12. Go to **Devices & Users > Devices**.
13. Open the details page of a device associated with the new label.
14. Click the **Device Details** tab to track the hotfix updates in the following rows:

    - **Last Hotfix ID**
    - **Last Hotfix Installed On** (date)

Setting up a compliance policy for device updates

This procedure describes how to set up device compliance based on hotfix and Windows 10 build information.

Procedure

1. Log into the Admin Portal.
2. Go to **Policies & Configs > Policies**.
3. Click **Default Security Policy**.
4. Scroll down to the **Access Control > For Windows devices** section.

5. Select one or more of the following options and provide the required information, where appropriate.

6. Click **Save**.

   The default policy will be applied to all Windows 10 desktop devices and labels, by default, to which no other policy has been applied.

Windows 10 Desktop device management

Administrators can control OS information on managed Windows 10 Desktop devices by restricting user access to the following areas on a device:

- Control Panel
- Task Manager
- File Explorer
- Registry Editor

This feature requires Bridge. See "Setting up Bridge" on page 332 for details.

Restricting access to device OS controls

Procedure

1. Log into the Admin Portal.

2. Go to **Policies & Configs** > **Configurations**.

3. Click **Add New** > **Windows** > **MobileIron Bridge**.

4. Select **Device Management** to open the **Device Management Settings** page.

5. Enter a name for the configuration.

   A description is optional.

6. Click the check box for one or more of the following options:
   - **Task Manager**
   - **Control Panel**
   - **File Explorer**

- **Registry Editor**

7. Click **Save**.

8. Select the new configuration in the **Configurations** table.

9. Click **Actions > Apply to Label > Windows**.

   This configurations will only apply to Windows 10 Desktop devices.

10. Click **Apply**.

Removable storage device management

Administrators can control access to any removable storage devices that can be plugged into a USB port by:

- **Removing read/writer access**. This prevents any access and is the most restrictive configuration.
- **Removing write-only access**. This allows limited access, but prevents unauthorized removal of data or the ability to add viruses, etc. to the device.
- **Allowing complete access to limited devices**. This lets administrators create a whitelist of devices, permitting users total access to only the removable storage device on the list.

Restricting access to removable storage devices

This feature requires Bridge. See "Setting up Bridge" on page 332 for details.

Procedure

1. Log into the Admin Portal.
2. Go to **Policies & Configs** > **Configurations**.
3. Click **Add New** > **Windows** > **MobileIron Bridge**.
4. Select **Device Management** to open the **Device Management Settings** page.

5. Enter a name for the configuration.

   A description is optional.

6. Go to the **USB** section and click one or both of the following options:

   - **Restrict Access to Removable Storage Devices**: to restrict all access (no read/write).
   - **Restrict Write Access to Removable Storage Devices**: to provide limited access (read-only).

7. Click **Save**.

8. Select the new configuration in the **Configurations** table.

9. Click **Actions > Apply to Label > Windows**.

   This configurations will only apply to Windows 10 Desktop devices.

10. Click **Apply**.

Creating a whitelist for removable storage devices

ⓘ This feature requires Bridge. See "Setting up Bridge" on page 332 for details.

Before you begin

If you want to create a whitelist of permitted USB devices, complete the following steps first:

1. Attach the USB storage devices you want to allow to a personal computer.
2. Open Device Manager and click on the USB controller.
3. Look at the settings for each controller for device information.
4. Store the device information to use when creating your whitelist.

Procedure

1. Log into the Admin Portal.
2. Go to **Policies & Configs** > **Configurations**.
3. Click **Add New** > **Windows** > **MobileIron Bridge**.

4. Select **Device Management** to open the **Device Management Settings** page.
5. Enter a name for the configuration.

   A description is optional.
6. Go to the **USB** section and click **Add+**.
7. Enter the device ID for one or more of the devices you want to add to the whitelist.
8. Click **Save**.
9. Select the new configuration in the **Configurations** table.
10. Click **Actions > Apply to Label > Windows**.

    This configurations will only apply to Windows 10 Desktop devices.
11. Click **Apply**.

Windows 10 Desktop customization

Use Core to customize Windows 10 Desktop devices by adding:

- Shortcuts to the desktop
- A screen saver image
- A locking screen image

Only Enterprise versions of Windows 10 can use the lock screen functionality.

Customizing desktops

This feature requires Bridge. See "Setting up Bridge" on page 332 for details.

Procedure

1. Go to **Policies & Configs** > **Configurations**.
2. Click **Add New** > **Windows** > **MobileIron Bridge** > **Desktop Settings**.
3. Enter a **Name** for the configuration.

4. Select one of the following **File Delivery** options for desktop settings.

   - **File Upload**: upload settings files to Core.
   - **Override URL**: provide override URLs with the settings files to download.

   Some fields on the page will change depending on what you select in this step.

5. Add a **Desktop Background** image using one of the following options.

   - Click **Browse** in the **Desktop Background** section to locate and upload a background image.
   - Enter the override URL in the **Desktop Background** section.

   Background images can be .JPEG, .PNG, .TIFF, .JPG, or .BMP file types.

6. Add a **Screensaver** image using one of the following options.

   - Click **Browse** in the **Screensaver** section to locate and upload a screensaver image.
   - Enter the override URL in the **Screensaver** section.

   Devices accept only the screen saver file type (.scr).

7. Check **Password-protect Screensaver** if you want to require use of a password to unlock screensaver mode.

8. Select a **Screensaver Timeout** period (in minutes).

9. Add a **Lock Screen** file using one of the following options.

   - Click **Browse** in the **Lock Screen** section to locate and upload a locked screen image.
   - Enter the override URL in the **Lock Screen** section.

   Lock screen images can be.JPEG, .PNG or .GIF file types.

10. Click **Add+** to set up application shortcuts to add to device desktops, then fill out the table using the following options.

a. **Location**: this will be desktop, taskbar or start menu.

b. **Target**: this will be an application.

   For webclips specify the browser to be used. Each browser accepts different commands to create a webclip.

c. **Description**: Specify the title below the shortcut.

d. **Icon File**: Specify the image for the icon file. This must be an .ICO file.

11. Click **Save**.
12. Select the new configuration in the **Configurations** table.
13. Click **Actions > Apply to Label > Windows**.

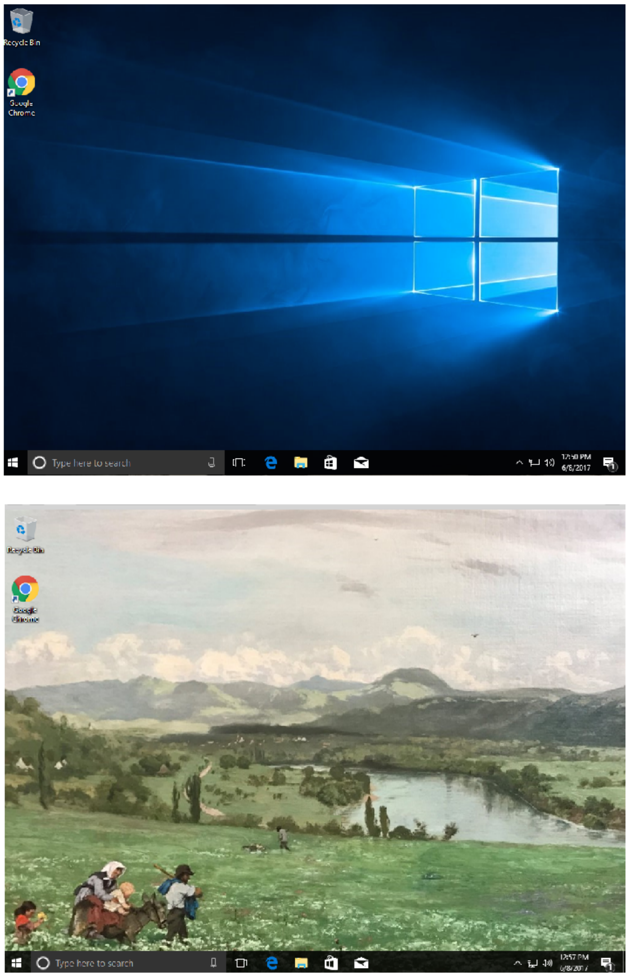
    This configurations will only apply to Windows 10 Desktop devices.

14. Click **Apply**.

Customized device desktop

The desktop, lock screen, and screen saver settings will take effect based on the associated configuration after the device is signed out and signed back in. For example, the desktop on the left is the default desktop for Windows 10 Desktop devices. The image on the right has been customized using Core’s Desktop Settings options. Shortcuts do not need a restart to take affect.

FIGURE 1. DEFAULT BACKGROUND IMAGE VS. CUSTOMIZED BACKGROUND IMAGE



Browser Settings for Windows 10 Desktop

This feature gives administrators greater control over the three browsers most commonly used by Windows 10 desktop (Chrome, Internet Explorer, Firefox).

Using browser settings

The device must be domain joined to respect the configuration for Chrome. See "Setting up Bridge" on page 332 for details.

Procedure

1. Log into the Admin Portal.
2. Go to **Policies & Configs > Configurations**.
3. Click **Add New > Windows > MobileIron Bridge > Browser Settings/Restrictions**.
4. Complete the form.

   Refer to "Browser Settings /Restrictions fields " below for details.

   Options vary depending on the browser you select.
5. Click **Save**.

Browser Settings/Restrictions window

ⓘ Chrome must be domain joined for the devices to respect the configuration.

The following table summarizes fields and descriptions for Bridge Browser Settings/Restrictions:

TABLE 69. BROWSER SETTINGS /RESTRICTIONS FIELDS

Item	Description	Default
Name	Add a name for this configuration (required).	N/A
Description	Add a description for this configuration (optional).	N/A
Browser types	Select one or more of the browsers (Chrome, Firefox, IE).	None
Browser Settings		
New Tab page URL	Enabling this option specifies the URL that the browser opens when adding a new tab page. If you do not set this option, no new tab page is provided.	N/A
All browser types	Select one or more options: • **Allow Saving Passwords**: enable this option to allow users to save passwords to the password manager.	Enabled for all options

TABLE 69. BROWSER SETTINGS /RESTRICTIONS FIELDS (CONT.)

Item	Description	Default
	- **Allow Outdated Plugins**: enable this option to allow users to use outdated plugins as normal plugins. If you disable it, users will not be asked for permission to run them. - **Safe Browsing Mode**: Safe Browsing shows a warning page when users navigate to sites that are flagged as potentially malicious. Enabling this setting prevents users from proceeding anyway from the warning page to the malicious site.	
Chrome and Firefox Only	Select **Allow Deleting Browser History** to allow users to delete their browser history and download history. Users cannot change this setting when enabled.	Enabled
Chrome and IE Only	Select **Enable Printing** to allow printing from a browser. If enabled, users cannot change this setting. If this option is not enabled, users cannot print from their browser, however they can print from plug-ins that bypass the browser.	Enabled
Chrome Only	Select one or more options: - **Show Home Button**: Select this option to enable this setting, so the Home button is always shown. Disable it so the Home button is never shown. - **Show the apps shortcut in the bookmark bar**: Select this option to show apps shortcut in the bookmark bar. - **Allow synchronization of data with Google**: Select this option to let users to synchronize in Google Chrome using Google-hosted synchronization services. - **Continue running background apps when Google Chrome is closed**: Select this option to allow background apps in the current browsing session to remain active, including any session cookies. The background process displays an icon in the system tray and can always be closed from there.	Enabled for all options

TABLE 69. BROWSER SETTINGS /RESTRICTIONS FIELDS (CONT.)

Item	Description	Default
Firefox Only	Enable **Allow Install Extensions** to allow a user to install the Firefox extension. Selecting disable prevents the user from installing this extension	Enabled
IE Only	Select **Allow Downloading Data from Websites** to allow users to download data from Websites.	Enabled
Browser favorites		
Browser Favorite Folders	Use this option to specify browser favorites folder and URLs. Click **Add+** to add each URL.	N/A
URL Control		
Control all Websites (Chrome and Firefox only)	Use these options to control what information websites use. Select one or more of the options, then click **Add+** to add each URL. • Block Cookies • Block Java Script • Block Plugins • Block Popups	N/A
URL Access Control		
Specify approved and blocked websites (Chrome only)	Use this option to control the access to websites. Each access control is limited to 1000 entries. See https://www.chromium.org/administrators/url-blocklist-filter-format. Click **Add+**, enter the URL, and select **Block** or **Allow**.	Block
Extension blacklist		
Specify blocked extensions (Chrome and IE only)	Use this option to set up blacklists that block extension Click **Add+**, select a browser type, and enter the Chrome extension ID.	N/A
Extension sources		

TABLE 69. BROWSER SETTINGS /RESTRICTIONS FIELDS (CONT.)

Item	Description	Default
Specify approved extension sources (Chrome only)	Use this option to specify approved extension sources. Each item is an extension-style match pattern. See https://developer.chrome.com/extensions/match_patterns for details. Click **Add+**, select a browser type, and enter the Chrome extension ID.	N/A
Extension forcelist		
Specify extensions to be force installed on browser (Chrome only)	Use this option to specify extensions to be force installed on browsers. Each item is a string that contains an extension Id and an update URL separated by a semicolon (;). Click **Add+**, then select an extension ID and extension update URL.	N/A
Allowed extension types		
Allowed extension types (Chrome only)	Use these options to specify allowed extensions types. Select one or more of the following extension type: • Chrome Extension ID/IE Add-on Class Identifier • Hosted App • Theme • Packaged App • User Script • Platform App	N/A

Bridge logs overview

This feature allows you to pull Bridge logs for individual devices for troubleshooting and diagnosing applications. The logs are sent at the next device check-in. You can wait for the next scheduled sync or perform a forced device check-in to get the logs quickly.

This topic has the following procedures:

- "Sending a request to the device" on the next page

- "Viewing a Bridge log" below

Sending a request to the device

This procedure describes how to pull logs from a device. Core sends a request to the device to pull Bridge log/s at the next device check-in.

Procedure

1. Log into the Admin Portal.
2. Go to **Devices & Users > Devices** and select a device.
3. Select **Actions > Windows Only > MobileIron Bridge (Windows 10 only)**.
4. Select one of the following options:
    - **Send Current Log**: requests Core pull the most recent Bridge log (up to 10 MB) on the device
    - **Send All Logs**: requests Core pull all Bridge logs (one zip file containing up to 11 log files) on the device
5. Click the appropriate **Send** button then **OK** after the log request is sent to the device.

Viewing a Bridge log

This procedure describes how to view a Bridge log after a device has sent it to Core.

Procedure

1. Log into the Admin Portal.
2. Go to **Logs > Devices**.
3. Check Bridge and select **test comments**.
4. Locate the device and click the **View Output** link to see:
    - **Current Log**: opening a new tab with the log content.
    - **All Logs**: automatically saving as “output.zip” file.

Removing unwanted applications

Administrators can remove unwanted applications (bloatware) that come on Windows 10 Desktop devices. There are several applications that administrators might not want users to access that come packaged with the OS. Rather than re-imaging a device with a smaller list of applications, Core and Bridge can help remove those applications at device enrollment.

The process for removing unwanted applications is for administrators to configure settings and apply the configuration to a label. When devices, associated with that label, sync with Core, the bloatware is removed from the device(s) based on the configuration settings.

Procedure

1. Log into the Admin Portal.
2. Go to **Devices & Users > Devices**.
3. Double-click on a device that has bloatware on it.
4. Scroll to the **Device UUID** detail and copy the UUID.

   Use the UUID, later in this procedure, to review the applications on a device.
5. Go to **Policies & Configs > Configurations**.
6. Click **Add New > Windows > MobileIron (Windows 10 Only) > Bloatware Remover**.
7. Enter the name of the configuration you will later apply to a label.
8. Enter the UUID in the **Device UUID for getting the list of application** field.
9. Click **Get installed applications**.

   Depending on how many applications are on the device, this can take a few minutes.

   Applications on the device are listed in the left pane.
10. Use the left and right arrows to move applications between the **Applications from device** list and the **Applications for delete** list.

    Applications will be removed from all devices associated with the configuration once applied to a label and the devices sync to Core.

11. Define options for removing applications:
    - **Run at log on**: runs the configuration when a user logs onto their device.
    - **Run every minute**: checks the device at the designated interval and removes any bloatware that was reinstalled.
    - **Suppress force restart after uninstall**: Does not restart the device after removing the bloatware.
12. Click **Save**.
13. Select the newly created bloatware removal configuration.
14. Select **Actions > Apply to Label**.
15. Select a label that is associated with Windows 10 Desktop devices containing bloatware you want to remove.
16. Click **Apply**.

    Based on the configuration, the label is applied and the unwanted applications are removed and the checks no longer apply.

Using the GPO Editor

Microsoft defines and releases more than 4000 Group Policy Objects (GPOs) to control Windows 10 Desktop devices. The GPO Editor allows administrators to view and search for GPOs quickly and easily, based on Microsoft's hierarchal groups and sub-groups. It also allows administrators to upload ADMX GPOs (custom for third party applications) that run outside of the Windows 10 operating system.

The GPO Editor validates all Microsoft GPO selections, the values provided for policy options, and the ADMX files. It also validates all custom ADMX GPO settings when the custom file specifies the key, with the exception of free form text.

Note the following:

- For more information about Microsoft GPOs, go to the following page: https://technet.microsoft.com/en-us/library/hh147307(v=ws.10).aspx. This page is controlled by a third party and can be removed, moved, or modified at any time without notice. It is provided here only as a courtesy.

- Any GPO configurations created before 9.6.0.0 will be deleted upon upgrading to 9.6.0.0 or supported newer versions. Ivantirecommends administrators save the settings created in before 9.5.0.0 and create a new profile after upgrading to any 9.6.0.0 or supported newer versions.

Adding a Windows 10 GPO

This procedure describes how to add GPOs that will modify the Windows Registry.

Procedure

1. Go to **Policies & Configs > Configurations**.
2. Click **Add New > Windows > MobileIron (Windows 10 Only) > Windows GPO**.
3. Enter the name of the GPO configuration in the **Name** field.
4. Click the arrow in the **Add Description** option if you want to add a description.
5. Click **Add**.
6. Expand the object tree to select a GPO or use the search field to find the GPO you want to add.

If you use the search feature, you can narrow the search scope by selecting the **Machine** (the default option) or **User** options. You can switch between these options.

7. Select **Enabled** to turn on the setting or create a new setting in the Registry.

Some settings simply turn on the setting with no additional configurations. If a setting has a sub-setting, complete the wizard after clicking **Enabled**.

8. Click **Save & Add another** to add more GPOs (optional).

Repeat steps 7-9 until you are done adding GPOs.

9. Click **Save & Close** when you are done adding GPOs.
10. Apply the configuration to a label to deploy the configuration to devices.

Select the configuration.

Click **Actions > Apply to Labels**.

Select one or more labels.

Click **Apply**.

Core pushes the configuration to devices associated with the applied label(s) after the next sync with Core.

Adding an ADMXGPO

This procedure describes how to add ADMX GPOs to upload custom third party applications. Refer to "ADMX file structure" below for details on creating the required folder structure to zip the .admx files.

Procedure

1. Log into the Admin Portal.
2. Go to **Policies & Configs > Configurations**.
3. Click **Add New > Windows > MobileIron (Windows 10 Only) > Windows GPO**.
4. Enter the name of the GPO configuration in the **Name** field.
5. Click the arrow in the **Add Description** option if you want to add a description.
6. Click **Add+**.
7. Click **Import ADMX+** next to the **Search** field to open the **Import ADMX files** window.
8. Click **Import** to locate and add the ADMX file.
9. Click **Import** again to import your ADMX file.
10. Click **Save & Add another** to add more GPOs (optional).

Repeat steps 7-10 until you are done adding GPOs.

11. Click **Save & Close** when you are done adding GPOs.
12. Apply the configuration to a label to deploy the configuration to devices.

Select the configuration.

Click **Actions > Apply to Labels**.

Select one or more labels.

Click **Apply**.

Core pushes the configuration to devices associated with the applied label(s) after the next sync with Core.

ADMX file structure

Create .admx zip files by zipping the folder containing the .admx file and the locale folders. Do not simply create is by zipping the contents of the folder.

Use the following file structure under the .admx package’s location:

```
|-- admx
|-- windows
|-- en-US
|-- win_policy_1.adml
|-- win_policy_2.adml
|-- win_policy_1.admx
|-- win_policy_2.admx
|-- google
|-- en-US
|-- google_policy_1.adml
|-- google_policy_2.adml
|-- google_policy_1.admx
|-- google_policy_2.admx
```

Disabling a GPO setting

This procedure describes how to disable a GPO setting to turn it off, but not to delete it.

> ℹ Some settings, once created, can never be deleted without a full device wipe.

Procedure

1. Log into the Admin Portal.
2. Go to **Policies & Configs > Configurations**.
3. Click **Add New > Windows > MobileIron (Windows 10 Only) > Windows GPO**.
4. Enter the name of the GPO configuration in the **Name** field.
5. Click **Add**.
6. Expand the object tree to select a GPO or use the search field to find the GPO you want to disable.

If you use the search feature, you can narrow the search scope by selecting the **Machine** or **User** options.

7. Select **Disabled** to turn off the setting.
8. Click **Save & Close**.

Printer management

Core allows administrators to create printer profiles and add them to devices. This section includes the following topics:

- "Adding a shared printer" below
- "Adding a network printer" on the next page

Adding a shared printer

A shared printer can only be set on domain joined devices. If you do not plan to domain join the device then a network printer option must be used. When the printer profile is sent to the device, the printer must be active, otherwise the device cannot discover it.

Procedure

1. Log into the Admin Portal.
2. Go to **Policies & Configs > Configurations**.
3. Click **Add New > Windows > MobileIron (Windows 10 Only) > Add Printer**.
4. Select **Shared Printer** as the **Printer type**.
5. Enter the name of the printer configuration in the **Name** field.
6. Enter the IP address in the **Print server** field.
7. Enter the printer name in the **Shared printer name** field.
8. Click **Save**.
9. Apply the printer configuration to a label to deploy the app to devices.

Select the newly created shared printer configuration.

Click **Actions > Apply to Labels**.

Select one or more labels.

Click **Apply**.

Based on the settings, the next time the devices associated with that label sync with Core, they will be connected to the configured printer.

Adding a network printer

Procedure

1. Log into the Admin Portal.
2. Go to **Policies & Configs > Configurations**.
3. Click **Add New > Windows > MobileIron (Windows 10 Only) > Add Printer**.
4. Select **Network-attached Printer** as the **Printer type**.
5. Enter the name of the printer configuration in the **Name** field.
6. Enter the printer name in the **Printer name** field.
7. Enter the address of the network printer in the **Printer port number** field
8. Enter the name of the printer driver in the **Printer driver name** field
9. Click **Save**.
10. Apply the printer configuration to a label to deploy the app to devices.

Select the newly created network printer configuration.

Click **Actions > Apply to Labels**.

Select one or more labels.

Click **Apply**.

Based on the settings, the next time the devices associated with that label sync with Core, they will be connected to the configured printer.

Bridge reporting

This feature provides details in logs of Bridge sent to and from applications, including the ability to report if the scripts Bridge initiates were successful or if they failed.

In addition, Core allows you to search logs using the following fields:

- State
- Object Name
- Message

This section includes the following additional topics:

- "Viewing Bridge reports" below
- "Using Bridge advanced search" below

Viewing Bridge reports

To view Bridge reports:

1. Log into the Admin Portal.
2. Go to **Logs > Audit Logs > Devices**.
3. Scroll down and select **MobileIron Bridge > Search**.

Note the **Success**/**Failed** values in the **State** column.

Using Bridge advanced search

To use advanced search options:

1. Log into the Admin Portal.
2. Go to **Logs** > **Audit Logs** > **Devices**.
3. Enter search filters for any of the following options:
    - State

   - ObjectName
   - Message
   - Message not containing

4. Click **Search**.

Managing Win32 apps

This sections includes the following topics:

- "Viewing Win32 app information" below
- "Deploying legacy apps" below
- "Removing legacy apps" on page 365

Viewing Win32 app information

This feature provides information on Win32 applications uploaded for deployment with Bridge for all Win32 applications that report app data in a manifest file. The information available for these Win32 apps include:

- Display Version
- Developer
- Description

Procedure

1. Log into the Admin Portal.
2. Go to **Apps** > **App Catalog** > **Windows**.
3. Click the name of a Win32 app.

Deploying legacy apps

Use the **Add Application Wizard** to add and deploy legacy applications to the list of available applications in the App Catalog.

ⓘ Only .EXE applications that can be silently installed as an executable can be placed in an Enterprise application store for deployment. An example of a non-silently installed EXE is putty. Putty is a client that would need to be pushed to the device as a file and not as an application to work on the device.

To add legacy applications:

1. Log into the Admin Portal.
2. Go to **Apps > App Catalog**.
3. Click **Add+** to open the wizard.
4. Select the **In-House** button.
5. Select **Browse** to locate and select the application you wish to upload.

   Core deploys applications with an .EXE extension using Bridge.
6. Click **Next** and enter the following information for application deployment:
   - **Override URL**: Enter the URL where the application will reside, if you want to use a centralized server distribution to store their applications.
   - **Command Line Parameters**: Specify the command line command for installing the EXE because not all .EXE files use the same Command Line Command. Otherwise users will be prompted when an application is being installed.
   - **Exe Target Directory**: This will let Bridge know which directory to use to when extracting the application for deployment. If nothing is specified Core uses the system temp directory (%TEMP%).
   - **Uninstall Command Line Parameters**: Provide the uninstall command, if you want to use Core to uninstall an application.
   - **Exe Uninstall File Location**: Specify the location on the device where the uninstaller resides.
7. Click **Finish** to upload and save the configurations and return to the **App Catalog** page.

Apply legacy apps to label

Bridge apps do not show up in Apps@Work and can only be installed by Core through label management.

Procedure

1. Log into the Admin Portal.
2. Go to **Apps** > **App Catalog**.
3. Select one or more Win32 apps.
4. Select **Actions** > **Apply to Labels**.
5. Select the label you want to use to deploy the legacy apps.
6. Click **Apply**.

   Bridge silently installs the selected app onto the Windows 10 Desktop devices after the devices sync with the label to which the Win32 app is associated.

Removing legacy apps

An app that was installed using Bridge can only be removed from devices if the following fields were set up:

- Command Line Instructions for application Uninstall
- Application Location

For details, see ""Deploying legacy apps" on the next page" on page 363.

Procedure

1. Log into the Admin Portal.
2. Go to **Apps** > **App Catalog**.
3. Select the app you want to remove from the device.
4. Select **Actions** > **Remove from Labels**.
5. Select the name of the label and click **Remove**.

   The user will no longer be able to see the application once it has been removed from the device.

Working with Events

This section addresses the components related to The Event Center.

- "About events" below
- "Managing events" on the next page
- "Event settings" on page 370
- "Customizing Event Center messages" on page 382
- "Viewing and Exporting Events" on page 390

About events

The Event Center enables Core administrators to configure *events* to specific *alerts* that can be sent to users, administrators, or both. Event types include:

- International Roaming Event
- SIM Changed Event
- Memory Size Exceeded Event
- System Event
- Policy Violations Event
- Device Status Event

An alert is a message sent via SMS or email. You can select a predefined message template, or create a custom message to use for the alert.

For example, you can specify an SMS to be sent each time a user travels to a different country, informing the user that different rates may apply.

Events page

Use the **Logs > Event Settings** page in Admin Portal to manage the events you are interested in and the corresponding alerts you want to automate.

Required role

To edit settings on the **Event Settings** page, the administrator must have the **Manage events** role.

Managing events

The tasks that are common to all event types are:

- "Creating an event" below
- "Editing an event" on the next page
- "Deleting an event" on the next page
- "Ensuring the alert is sent to the correct recipients" on the next page
- "Applying the event to a label" on page 369
- "Setting alert retries" on page 369

Creating an event

Procedure

To create an event, in the Admin Portal:

1. Go to **Logs** > **Event Settings**.
2. Click **Add New**.
3. Select the type of event from the drop-down.
4. Complete the information for the selected event.

   Each event type has settings specific to the event type. See "Event settings" on page 370 for information on the settings.
5. Click **Save**.

Editing an event

Procedure

1. Go to **Logs > Event Settings**.
2. Select the event you want to edit.
3. Click **Edit**.
4. Make your changes.
5. Click **Save.**

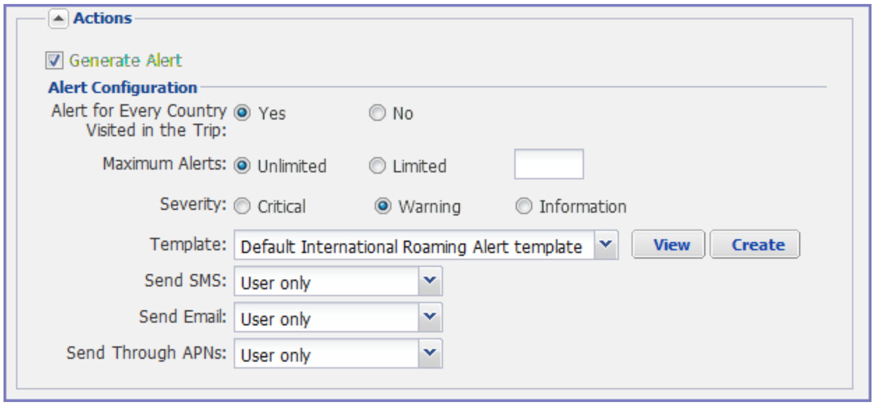
Deleting an event

Procedure

1. Go to **Logs > Event Settings**.
2. Select the event you want to delete.
3. Click **Delete**.

Ensuring the alert is sent to the correct recipients

When you create an event, you designate recipients for the resulting alert. Each event type includes the alert configuration section shown in the following figure.



Actions

☑ Generate Alert

Alert Configuration

Alert for Every Country Visited in the Trip: ● Yes ○ No

Maximum Alerts: ● Unlimited ○ Limited

Severity: ○ Critical ● Warning ○ Information

Template: Default International Roaming Alert template

Send SMS: User only

Send Email: User only

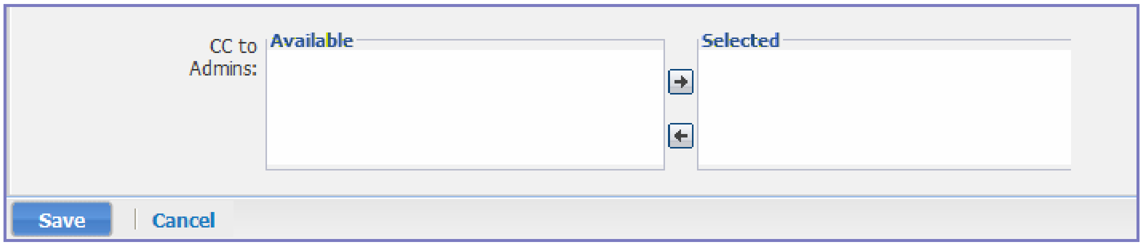
Send Through APNs: User only

For each type of alert (i.e. SMS and email), you can select to send the alert to one of the following:

- **None**
- **User only**
- **User + Admin**
- **Admin only**

If you select one of the Admin options, a **CC to Admins** section is displayed in the dialog box. This section displays a list of devices. Under the Available heading , select a device (or devices), that is associated with an email address that you want to notify, other than the device user. Core will send a notification to the email address associated with the device or devices that appear under the Selected heading.

FIGURE 1. CC TO ADMINS



Only users who have registered devices can appear in the **Apply to Users** list.

Applying the event to a label

To specify the devices to which the event should apply, you select one or more labels when you create the event. The amount of time it takes to apply an event to a label depends on the number of devices identified by the label. Therefore, it may take some time for the label name to display as selected for the event.

Setting alert retries

You can specify the number of times Core attempts to send an SMS alert or registration email.

Procedure

1. Enter the number of retries for SMS and registration email.

   Reminders are sent at 48-hour intervals until the number of reminders specified are sent, or the device is registered.

   For example, if you use the default for **Number of Retries for Email** (which is 2), an email is sent immediately after registration. If the device is not registered within 48 hours, a second email is sent. No other reminders are sent because you specified two reminders.

2. Click **Save**.

Setting Core SMS, email, and push notifications

You can designate specific hours for the sending of SMS, email, and push notifications. The default notification time is 0300 (3 a.m.), which can be disruptive.

Procedure

To override the default notification schedule:

1. From the Admin Portal, go to **Settings** > **System Settings** > **General** > **Alert**.
2. Select the **Override Default Schedule SMS, Email, Push notification** check box. The section expands.
3. Enter the notification start time and end time, in UTC hours.
4. Select the days of the week when sending notifications are allowed.
5. Click **Save**.

Event settings

Each event type has specific settings that need to be configured when you create or edit the event. This section describes the settings for each type.

- "International roaming event settings" on the next page
- "SIM changed event settings" on the next page
- "Memory size exceeded event settings" on the next page

- "System event settings" below
- "System event field description" on the next page
- "Policy violations event settings" on page 375
- "Policy violations event field description" on page 376
- "Device status event settings" on page 379

International roaming event settings

This event type is not supported for Windows devices.

SIM changed event settings

This event type is not supported for Windows devices.

Memory size exceeded event settings

This event type is not supported for Windows devices.

This section address how to create a memory size exceeded event.

Procedure

System event settings

A system event applies a compliance action when a component of a Core implementation is not working. System alerts are intended for relevant administrators.

Procedure

1. In the Admin Portal, go to **Logs > Event Settings**.
2. Click **Add New**.
3. Select **System Event** from the drop down menu.
4. Use the guidelines in "System event field description" on the next page to complete the form:
5. Click **Save**.

System event field description

TABLE 70. SYSTEM EVENT FIELD DESCRIPTIONS

Field	Description
Name	Identifier for this event.
Description	Additional text to clarify the purpose of this notification.
Sentry (standalone and integrated) is unreachable	Applies a compliance action if Core is unable to contact the Sentry.
MobileIron gateway is unreachable	Select this option to send an alert if Core cannot connect to the Core gateway.
LDAP server is unreachable	Select this option to send an alert if Core cannot connect to any of the configured LDAP servers.
DNS server is unreachable	Select this option to send an alert if Core cannot connect to one of the configured DNS servers.
Mail server is unreachable	Select this option to send an alert if Core cannot connect to the configured SMTP server.
NTP server is unreachable	Select this option to send an alert if Core connect to the configured NTP server.
Certificate Expired or Certificate Error	Select this option to send an alert for certificate expiration. An alert is sent 60 days before expiration and on the expiration date. Certificates supported include Admin Portal and device certificates.
Provisioning Profile Expired	This feature is not supported for Windows devices.
SMTP Relay server is unreachable	Applies a compliance action if the configured SMTP relay (used for SMS archive) does not respond to a ping or SMTP ping.
SMTP Relay server error	Applies a compliance action if the configured SMTP relay (used for SMS archive) returns an error. The alert includes available details to enable troubleshooting.
System storage threshold has been reached	Applies a compliance action if the system storage threshold has been reached. Refer to *Core System Manager Guide* for information on setting this threshold or manually purging the data.
Connector state events	Applies a compliance action if the health of the Connector changes.

TABLE 70. SYSTEM EVENT FIELD DESCRIPTIONS (CONT.)

Field	Description
	Core defines a healthy connector as one that connects to the server at expected intervals and syncs successfully with the LDAP server. An alert is generated if a Connector changes from healthy to unhealthy, or from unhealthy to healthy.
Connector requires upgrade	Applies a compliance action if the automated upgrade of the Connector fails. This alert prompts you to manually upgrade the Connector.
Connector can not connect to LDAP server	Applies a compliance action if a configured LDAP server is no longer reachable.
Connector is unreachable	Applies a compliance action if the Core server does not receive the expected response to the scheduled probe of the Connector. This alert generally indicates network problems.
Application update failed	Alerts the administrator that the Apps@Work or Bridge update for Windows failed. For more information, administrators can the server logs.
Mobile Threat Definition Update	Alerts administrators when a new version of the mobile threat definition is available. The notification includes any impacts to the existing MTD Local Action policies if threats were removed from the latest update.
Generate Alert	Turns on/off the alert defined for this event.
Maximum Alerts	Specifies whether there is a limit on the number of alerts generated for a given event. If you select **Limited**, then you can specify the number of alerts to allow. By default, compliance is checked every 24 hours. See "Managing Compliance" on page 101 and "Creating an event" on page 367 for more information.
Alert Every	Specifies the time, in days, after which the alert count is reset.
Severity	Specifies the severity defined for the alert. Select **Critical**, **Warning**, or **Information**.
Template	Specifies the template to populate the resulting alert. Click **View** to display the content of the current template.

TABLE 70. SYSTEM EVENT FIELD DESCRIPTIONS (CONT.)

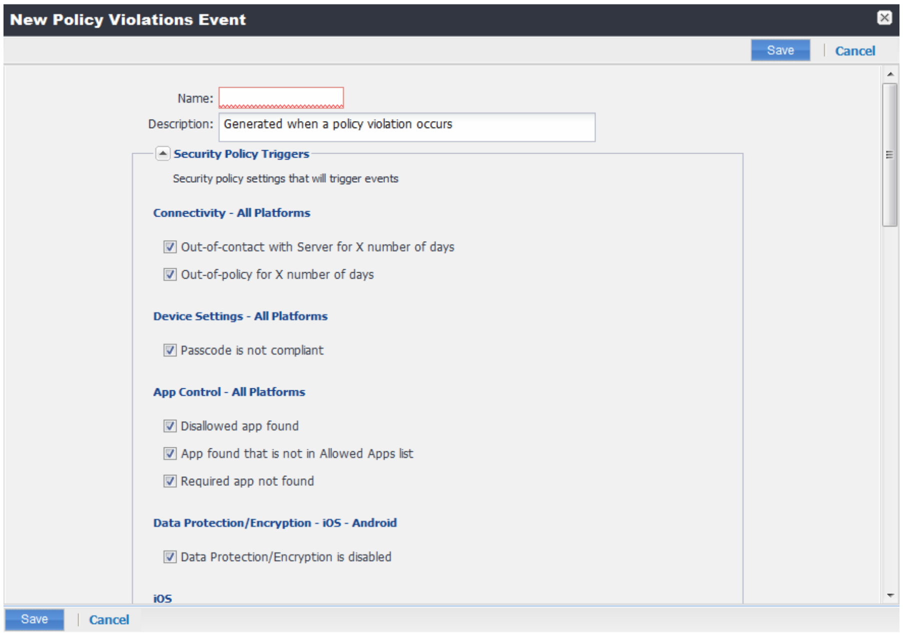
Field	Description
	Select an alternate template from the drop-down or click **Create** to create a new template. See "Customizing Event Center messages" on page 382 for information on creating a new template.
Send SMS	Specifies whether to send an alert in a text message, and whether to send it to the user, the administrator, or both. Specify users in the **Apply to Users** section or by selecting a label in the **Apply to Labels** section. If you select “Admin only” or “User + Admin”, then the **CC to Admins** section appears. Use this section to specify administrative users who should receive the alert.
Send Email	Specifies whether to send an alert in an email, and whether to send it to the user, the administrator, or both. Specify users in the **Apply to Users** section or by selecting a label in the **Apply to Labels** section. If you select “Admin only” or “User + Admin”, then the **CC to Admins** section appears. Use this section to specify administrative users who should receive the alert.
Send through Push Notification	Specifies whether to send a message, and whether to send it to the user, administrator, or both. Specify users in the **Apply to Users** section or by selecting a label in the **Apply to Labels** section. If you select “Admin only” or “User + Admin”, then the **CC to Admins** section appears. Use this section to specify administrative users who should receive the alert. The length of the message is limited to 255 characters.
Apply to Labels	Send the alert to users in the selected labels. See the “Using labels to establish groups” section in *Getting Started with Core*for more information. In most cases, if you do select a label, it should not be a label with broad coverage. System event alerts are usually not appropriate for device users.
Search Users	Enter the **user ID** to find users to which you want to send the alert.
Apply to Users	Send the alert to the selected users.

Policy violations event settings

For Windows devices, only out of contact and out of policy violations are supported. Alerts can be sent by email only.

Procedure

1. In the Admin Portal, go to **Logs > Event Settings**.
2. Click **Add New**.
3. Select **Policy Violation Event** from the drop-down menu. The New Policy Violations Event dialog box opens.



New Policy Violations Event

Name:

Description: Generated when a policy violation occurs

Security Policy Triggers

Security policy settings that will trigger events

Connectivity - All Platforms

☑ Out-of-contact with Server for X number of days

☑ Out-of-policy for X number of days

Device Settings - All Platforms

☑ Passcode is not compliant

App Control - All Platforms

☑ Disallowed app found

☑ App found that is not in Allowed Apps list

☑ Required app not found

Data Protection/Encryption - iOS - Android

☑ Data Protection/Encryption is disabled

iOS

4. Follow the guidelines in "Policy violations event field description" on the next page to complete the form.
5. Click **Save**.

Apply only one Policy Violations event to each device. If more than one policy violations event applies to a device, only the last one you edited and saved is triggered. Therefore, do not create a separate policy violations event for each type of security policy violation.

In that one Policy Violations event, select all of the security policy settings that you want to trigger the event. Use the template variable $DEFAULT_POLICY_VIOLATION_MESSAGE in your message template to specify the security policy violation that triggered the event.

Policy violations event field description

The following table describes fields for configuring a policy violation event.

TABLE 71. POLICY VIOLATION EVENT FIELD DESCRIPTION

Field	Description
Name	Identifier for this event.
Description	Additional text to clarify the purpose of this notification.
Connectivity	
Out-of-contact with Server for X number of days	Select this option to send an alert when a device has been out of contact for the number of days specified in the Security policy assigned to it.
Out-of-policy for X number of days	Select this option to send an alert when a policy has been out of date for the number of days specified in the Security policy assigned to it.
Device Settings	
Passcode is not compliant	Applies a compliance action if a device is detected having a passcode that does not meet the requirements specified in the associated security policy.
App Control	
Disallowed app found	Applies a compliance action if an app that is specified as Disallowed is installed on a device. Apps are specified as **Required**, **Allowed**, or **Disallowed** under **Apps > App Control**.
App found that is not in Allowed Apps list	Applies a compliance action if an app that does not appear on the list of allowed apps has been detected on a device. Apps are specified as **Required**, **Allowed**, or **Disallowed** under **Apps > App Control**.
Required app not found	Applies a compliance action if an app that is specified as Required is not installed on a device. Apps are specified as **Required**, **Allowed**, or **Disallowed** under **Apps > App Control**.

TABLE 71. POLICY VIOLATION EVENT FIELD DESCRIPTION (CONT.)

Field	Description
Data Protection/Encryption - iOS - Android	
Data Protection/Encryption is disabled	.
Security - Windows	
OS Build is less than the required OS build	Select this option to apply a compliance action if the device build is less than the OS build defined in the Security policy.
Last Hotfix is less than the required hotfix	Select this option to apply a compliance action if the device OS build is less than the hotfix build defined in the Security policy.
Last Hotfix installation date is out of date	Select this option to apply a compliance action if the device OS has not been updated in the time interval defined in the Security policy.
iOS	
Disallowed iOS model found	Select this option to apply a compliance action when a restricted iOS model is registered.
Disallowed iOS version found	Select this option to apply a compliance action when a restricted iOS version is registered.
Compromised iOS device	Select this option to apply a compliance action when a compromised iOS is registered or connects to the server. That is, an iOS device has been compromised by circumventing the operator and usage restrictions imposed by the operator and manufacturer.
iOS Configuration not compliant	Applies a compliance action if an iOS device does not have the expected security policy or app settings. This state may indicate that a setting was changed or was not applied successfully.
Restored Device connected to server	Applies a compliance action if a previously wiped device has been restored and attempts to connect through the Core deployment.
MobileIron iOS App Multitasking disabled by user	Applies a compliance action if the device user disables multitasking for the iOS app. Disabling multitasking increases the likelihood that a compromised device will go undetected for a significant period of time.
Device MDM deactivated (**iOS 5 and later**)	Applies a compliance action when the MDM profile on a managed iOS 5 device is removed.

TABLE 71. POLICY VIOLATION EVENT FIELD DESCRIPTION (CONT.)

Field	Description
macOS	
Disallowed macOS version found	Applies a compliance action if Core finds a registered device running a prohibited version of macOS.
Device MDM deactivated	Applies a compliance action if Core detects that MDM (Mobile Device Management) has been deactivated on a registered macOS device.
FileVault encryption disabled	Applies a compliance action if Core detects a registered macOS device with disabled FileVault encryption.
Android	
Disallowed Android OS version found	Applies a compliance action if an Android device having a disallowed OS version is detected. You can specify disallowed versions in the security policy.
Compromised Android device detected	Applies a compliance action if a modified Android device is detected. That is, an Android device has been compromised by circumventing the operator and usage restrictions imposed by the operator and manufacturer.
Device administrator not activated for DM client or agent	Generate an alert when a managed Android device is found to have no device administrator privilege activated for Mobile@Work or the Samsung DM Agent.
Actions	
Generate Alert	Turns on/off the alert defined for this event.
Maximum Alerts	Specifies whether there is a limit on the number of alerts generated for a given event. If you select Limited, then you can specify the number of alerts to allow.
Alert Every	Specifies the time, in days, after which the alert count is reset.
Severity	Specifies the severity you define for this alert. Select **Critical**, **Warning**, or **Information**.
Template	Specifies the template to populate the resulting alert. Click **View** to display the content of the current template. Select an alternate template from the drop down or click **Create** to create a new template. See "Customizing Event Center messages" on page 382 for information on creating a new template.

TABLE 71. POLICY VIOLATION EVENT FIELD DESCRIPTION (CONT.)

Field	Description
Send SMS	Specifies whether to send an alert in a text message, and whether to send it to the user, the administrator, or both. Specify users in the **Apply to Users** section or by selecting a label in the **Apply to Labels** section. If you select “Admin only” or “User + Admin”, then the **CC to Admins** section appears. Use this section to specify administrative users who should receive the alert.
Send Email	Specifies whether to send an alert in an email, and whether to send it to the user, the administrator, or both. Specify users in the **Apply to Users** section or by selecting a label in the **Apply to Labels** section. If you select “Admin only” or “User + Admin”, then the **CC to Admins** section appears. Use this section to specify administrative users who should receive the alert.
Send through Push Notification	Specifies whether to send a message, and whether to send it to the user, the administrator, or both. Specify users in the **Apply to Users** section or by selecting a label in the **Apply to Labels** section. If you select “Admin only” or “User + Admin”, then the **CC to Admins** section appears. Use this section to specify administrative users who should receive the alert. The length of the message is limited to 255 characters.
Apply to Labels	Send the alert to users in the selected labels. See the “Using labels to establish groups” section in *Getting Started with Core* for more information.
Search Users	Enter the user ID to find users to which you want to send the alert.
Apply to Users	Send the alert to the selected users.
CC to Admins	If you selected “Admin only” or “User + Admin”, then the **CC to Admins** section appears. Use this section to specify administrative users who should receive the alert.

Device status event settings

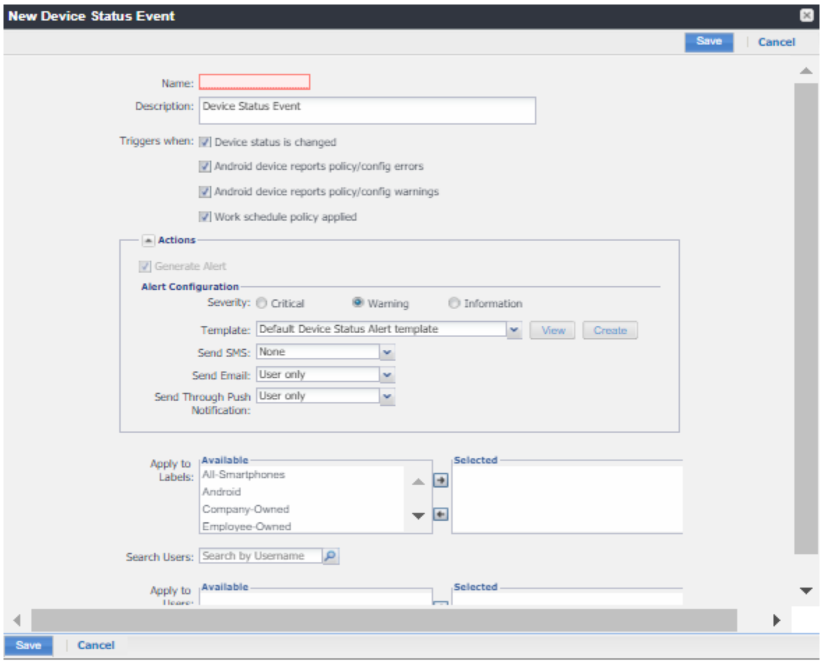
The device status event applies only to Android and iOS devices. The following describes the steps to create a device status event in the Admin Portal.

Procedure

1. Go to **Logs > Event Settings**.

2. Click **Add New**.

3. Select **Device Status Event** from the drop-down menu. The New Status Event dialog box opens.



Name:

Description: Device Status Event

Triggers when: ☑ Device status is changed
☑ Android device reports policy/config errors
☑ Android device reports policy/config warnings
☑ Work schedule policy applied

☑ Generate Alert

Severity: ○ Critical ● Warning ○ Information

Template: Default Device Status Alert template

Send SMS: None

Send Email: User only

Send Through Push Notification: User only

Apply to Labels: All-Smartphones, Android, Company-Owned, Employee-Owned

Search Users: Search by Username

Apply to Users:

4. Use the following guidelines to complete the form:

Field	Description
Name	Identifier for this event.
Description	Additional text to clarify the purpose of this notification.
Triggers when	Specifies the conditions on the device that will trigger an alert: • Device status is changed (Android and iOS) • Android device reports policy/config errors • Android device reports policy/config warnings

Field	Description
	- Work schedule policy applied (Android and iOS)
Actions	
Severity	Specifies the severity you define for this alert. Select **Critical**, **Warning**, or **Information**.
Template	Specifies the template to populate the resulting alert. Click **View** to display the content of the current template. Select an alternate template from the drop-down or click **Create** to create a new template. See "Customizing Event Center messages" on the next page for information on creating a new template.
Send SMS	Specifies whether to send an alert in a text message, and whether to send it to the user, the administrator, or both. Specify users in the **Apply to Users** section or by selecting a label in the **Apply to Labels** section. If you select “Admin only” or “User + Admin”, then the **CC to Admins** section appears. Use this section to specify administrative users who should receive the alert.
Send Email	Specifies whether to send an alert in an email, and whether to send it to the user, the administrator, or both. Specify users in the **Apply to Users** section or by selecting a label in the **Apply to Labels** section. If you select “Admin only” or “User + Admin”, then the **CC to Admins** section appears. Use this section to specify administrative users who should receive the alert.
Send through Push Notification	Specifies whether to send a message, and whether to send it to the user, the administrator, or both. Specify users in the **Apply to Users** section or by selecting a label in the **Apply to Labels** section. If you select “Admin only” or “User + Admin”, then the **CC to Admins** section appears. Use this section to specify administrative users who should receive the alert. The length of the message is limited to 255 characters.

Field	Description
Apply to Labels	Send the alert to users in the selected labels. See the “Using labels to establish groups” section in *Getting Started with Core* for more information.
Search Users	Enter the user ID to find users to which you want to send the alert.
Apply to Users	Send the alert to the selected users.
CC to Admins	If you selected “Admin only” or “User + Admin”, then the **CC to Admins** section appears. Use this section to specify administrative users who should receive the alert.

5. Click **Save**.

If more than one device status event applies to a device, only the last one you edited and saved is triggered.

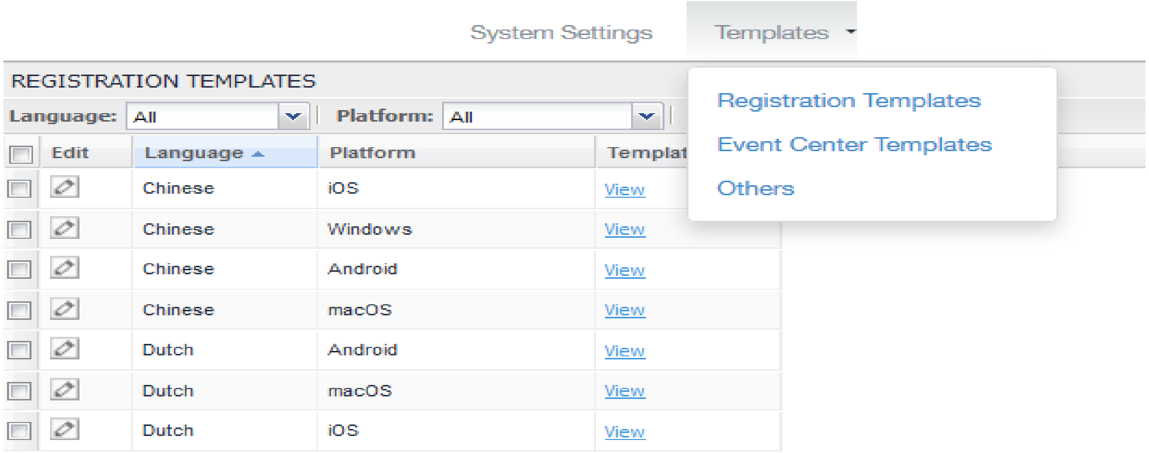
Customizing Event Center messages

The Event Center sends emails, SMSes, and push notification messages based on triggering events. When you configure events, you can use the default message template or create a new one. Event Center templates enable you to specify content and basic formatting using HTML markup.

Displaying Event Center templates

To display Event Center templates:

1. In the Admin Portal, go to **Settings > Templates**.

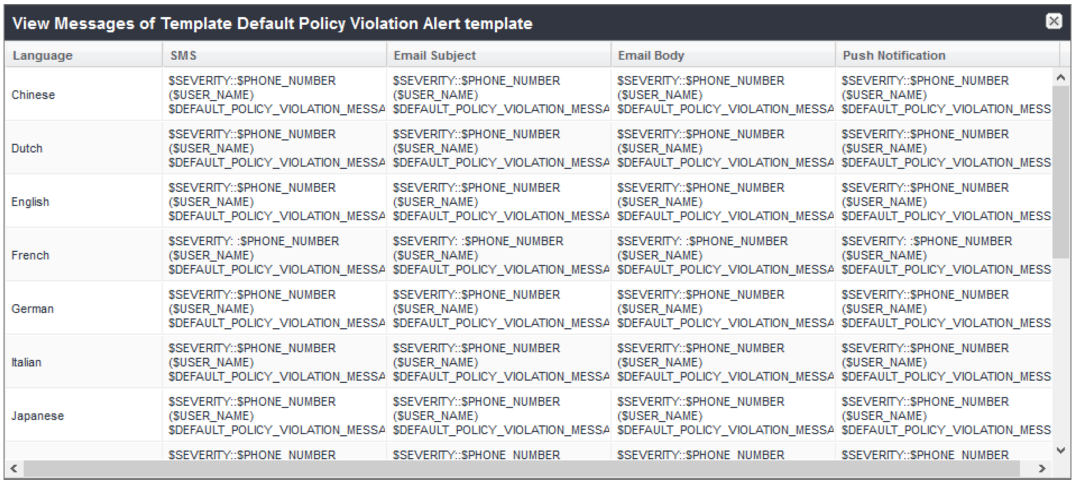


□	Edit	Language ▲	Platform	Templat
□	✎	Chinese	iOS	View
□	✎	Chinese	Windows	View
□	✎	Chinese	Android	View
□	✎	Chinese	macOS	View
□	✎	Dutch	Android	View
□	✎	Dutch	macOS	View
□	✎	Dutch	iOS	View

2. Select **Event Center Templates**.

   This list includes the default template for each Event Center type. Default templates are not editable.

3. Click the **View** link for the message template you want to view.



View Messages of Template Default Policy Violation Alert template

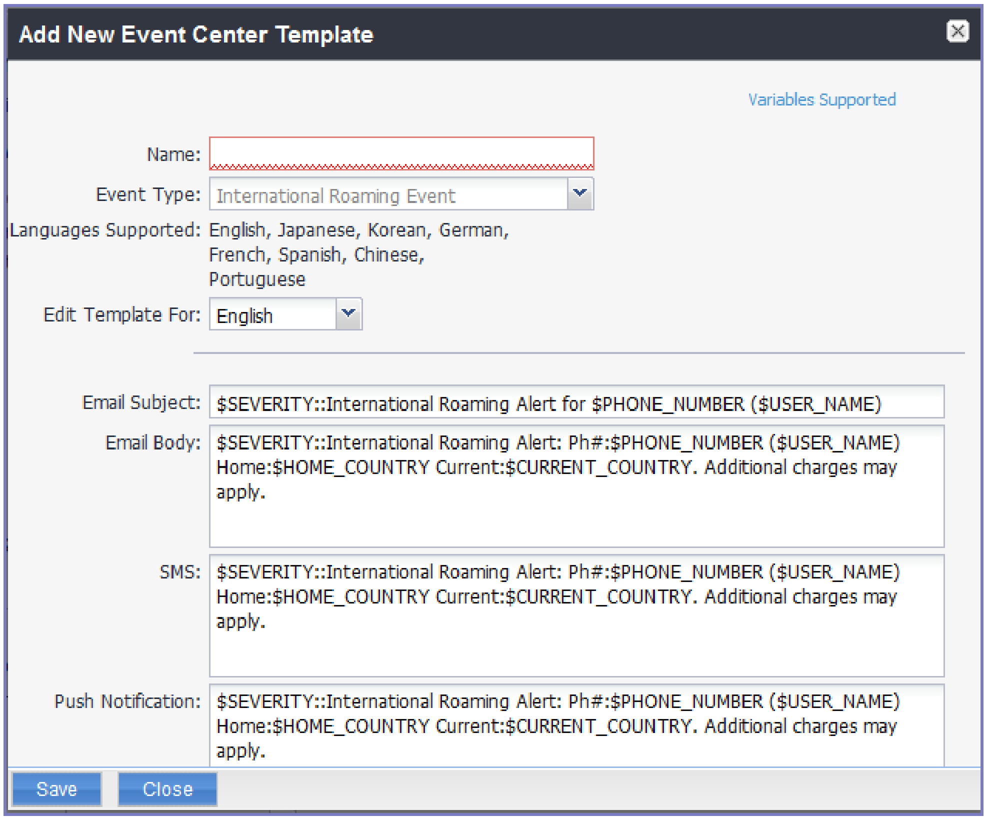
Language	SMS	Email Subject	Email Body	Push Notification
Chinese	$SEVERITY::$PHONE_NUMBER ($USER_NAME) $DEFAULT_POLICY_VIOLATION_MESSA	$SEVERITY::$PHONE_NUMBER ($USER_NAME) $DEFAULT_POLICY_VIOLATION_MESSA	$SEVERITY::$PHONE_NUMBER ($USER_NAME) $DEFAULT_POLICY_VIOLATION_MESSA	$SEVERITY::$PHONE_NUMBER ($USER_NAME) $DEFAULT_POLICY_VIOLATION_MESS
Dutch	$SEVERITY::$PHONE_NUMBER ($USER_NAME) $DEFAULT_POLICY_VIOLATION_MESSA	$SEVERITY::$PHONE_NUMBER ($USER_NAME) $DEFAULT_POLICY_VIOLATION_MESSA	$SEVERITY::$PHONE_NUMBER ($USER_NAME) $DEFAULT_POLICY_VIOLATION_MESSA	$SEVERITY::$PHONE_NUMBER ($USER_NAME) $DEFAULT_POLICY_VIOLATION_MESS
English	$SEVERITY::$PHONE_NUMBER ($USER_NAME) $DEFAULT_POLICY_VIOLATION_MESSA	$SEVERITY::$PHONE_NUMBER ($USER_NAME) $DEFAULT_POLICY_VIOLATION_MESSA	$SEVERITY::$PHONE_NUMBER ($USER_NAME) $DEFAULT_POLICY_VIOLATION_MESSA	$SEVERITY::$PHONE_NUMBER ($USER_NAME) $DEFAULT_POLICY_VIOLATION_MESS
French	$SEVERITY: :$PHONE_NUMBER ($USER_NAME) $DEFAULT_POLICY_VIOLATION_MESSA	$SEVERITY: :$PHONE_NUMBER ($USER_NAME) $DEFAULT_POLICY_VIOLATION_MESSA	$SEVERITY: :$PHONE_NUMBER ($USER_NAME) $DEFAULT_POLICY_VIOLATION_MESSA	$SEVERITY: :$PHONE_NUMBER ($USER_NAME) $DEFAULT_POLICY_VIOLATION_MESS
German	$SEVERITY::$PHONE_NUMBER ($USER_NAME) $DEFAULT_POLICY_VIOLATION_MESSA	$SEVERITY::$PHONE_NUMBER ($USER_NAME) $DEFAULT_POLICY_VIOLATION_MESSA	$SEVERITY::$PHONE_NUMBER ($USER_NAME) $DEFAULT_POLICY_VIOLATION_MESSA	$SEVERITY::$PHONE_NUMBER ($USER_NAME) $DEFAULT_POLICY_VIOLATION_MESS
Italian	$SEVERITY::$PHONE_NUMBER ($USER_NAME) $DEFAULT_POLICY_VIOLATION_MESSA	$SEVERITY::$PHONE_NUMBER ($USER_NAME) $DEFAULT_POLICY_VIOLATION_MESSA	$SEVERITY::$PHONE_NUMBER ($USER_NAME) $DEFAULT_POLICY_VIOLATION_MESSA	$SEVERITY::$PHONE_NUMBER ($USER_NAME) $DEFAULT_POLICY_VIOLATION_MESS
Japanese	$SEVERITY::$PHONE_NUMBER ($USER_NAME) $DEFAULT_POLICY_VIOLATION_MESSA	$SEVERITY::$PHONE_NUMBER ($USER_NAME) $DEFAULT_POLICY_VIOLATION_MESSA	$SEVERITY::$PHONE_NUMBER ($USER_NAME) $DEFAULT_POLICY_VIOLATION_MESSA	$SEVERITY::$PHONE_NUMBER ($USER_NAME) $DEFAULT_POLICY_VIOLATION_MESS
	$SEVERITY::$PHONE_NUMBER	$SEVERITY::$PHONE_NUMBER	$SEVERITY::$PHONE_NUMBER	$SEVERITY::$PHONE_NUMBER

Adding custom Event Center messages

To add a custom Event Center message:

1. Select the event type from **Settings > Templates > Event Center Templates > Add New**.

   The Add New Event Center Template dialog box displays.

   Add New Event Center Template

   Name:

   Event Type: International Roaming Event

   Languages Supported: English, Japanese, Korean, German, French, Spanish, Chinese, Portuguese

   Edit Template For: English

   Email Subject: $SEVERITY::International Roaming Alert for $PHONE_NUMBER ($USER_NAME)

   Email Body: $SEVERITY::International Roaming Alert: Ph#:$PHONE_NUMBER ($USER_NAME) Home:$HOME_COUNTRY Current:$CURRENT_COUNTRY. Additional charges may apply.

   SMS: $SEVERITY::International Roaming Alert: Ph#:$PHONE_NUMBER ($USER_NAME) Home:$HOME_COUNTRY Current:$CURRENT_COUNTRY. Additional charges may apply.

   Push Notification: $SEVERITY::International Roaming Alert: Ph#:$PHONE_NUMBER ($USER_NAME) Home:$HOME_COUNTRY Current:$CURRENT_COUNTRY. Additional charges may apply.

2. Event Center messages are displayed with the HTML markup that provides the basic formatting for the content.

3. In the **Name** field, enter a name for the template.

   The name must be unique for events of the same type.

4. In the **Edit Template for** field, select the language this template will be used for.

   Note that only those languages that have been enabled for the system will be displayed in this list.

5. Make changes to the displayed messages.

For creating a company-branded Event Center email, you can copy and paste an HTML email message into the **Email Body** field. For more information, see "Sending a company-branded email" on page 31.

6. Click **Save**.

Adding other types of templates

There are "Other" types of events that have templates that you can modify and use. The "Other" list includes the default template for: Action on Device, App Distribution, Selective Wipe, and Wipe. Default templates are not editable.

Procedure

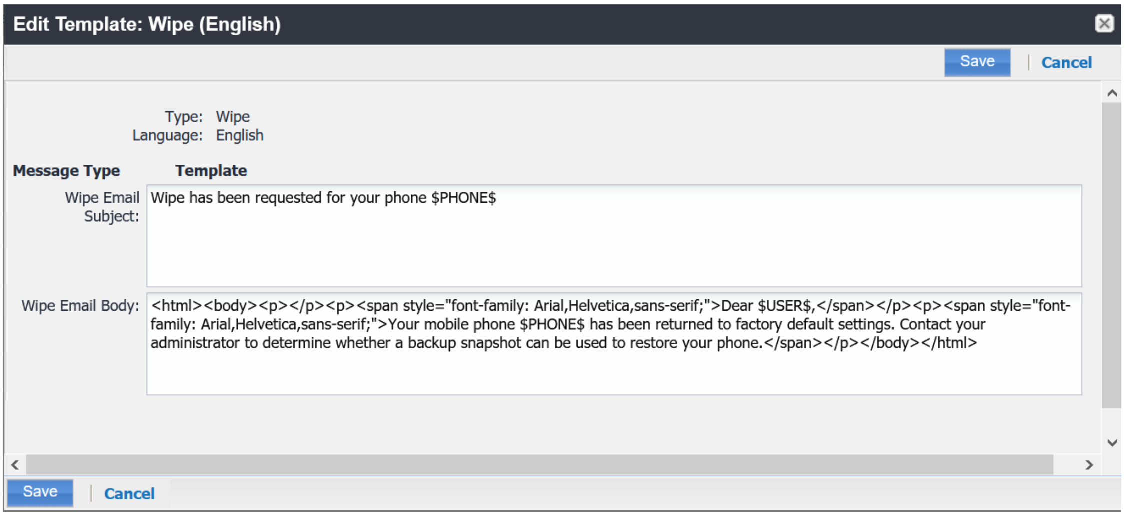
1. Go to **Settings > System Settings**.

2. Click **Templates > Others**.

   The Others template page displays.

3. Find the language you want the template to display in and then click the **Edit** icon.

   The Edit Template dialog box opens. For this example, the Edit Template: Wipe (English) dialog box opens.



Type: Wipe
Language: English

Message Type	Template
Wipe Email Subject:	Wipe has been requested for your phone $PHONE$
Wipe Email Body:	<html><body><p></p><p><span style="font-family: Arial,Helvetica,sans-serif;">Dear $USER$,</span></p><p><span style="font-family: Arial,Helvetica,sans-serif;">Your mobile phone $PHONE$ has been returned to factory default settings. Contact your administrator to determine whether a backup snapshot can be used to restore your phone.</span></p></body></html>

4. Enter the information in the form.

- **Email Subject** - Modify the default text or enter a short phrase that gives a summary of the message.
- **Email Body** - Modify the provided text for your needs. See "Using variables in Event Center messages" below

5. When finished, click **Save**.

Related topics

"Customizing registration messages" on page 23

Using variables in Event Center messages

Supported and required variables for Event Center messages vary by the type of message. The following table summarizes these variables. You can also click the **Variables Supported** link to display this information. Note that, unlike variables used for registration variables, Event Center variables do not end with $.

TABLE 72. VARIABLES IN EVENT CENTER MESSAGES

Template Type	Required Variables
International Roaming	$CURRENT_COUNTRY $HOME_COUNTRY $PHONE_NUMBER $SEVERITY $USER_NAME
Threshold Reached	$PHONE_NUMBER $SEVERITY $THRESHOLD_ON $THRESHOLD_TYPE $THRESHOLD_UNIT $THRESHOLD_VALUE $USED_VALUE $USER_NAME
SIM Changed	$CURRENT_PHONE_NUMBER $NEW_PHONE_NUMBER

TABLE 72. VARIABLES IN EVENT CENTER MESSAGES (CONT.)

Template Type	Required Variables
	$SEVERITY $USER_NAME
Memory Size Exceeded	$FREE_MEMORY_SIZE $MEMORY_SIZE_LIMIT $PHONE_NUMBER $SEVERITY $TOTAL_MEMORY_SIZE $USER_NAME
System Event	$DEFAULT_SYSTEM_MESSAGE $SERVER_IP $SERVER_NAME $SEVERITY
Policy Violation	$DEFAULT_POLICY_VIOLATION_MESSAGE $PHONE_NUMBER $SEVERITY $USER_NAME

Variable descriptions

The following table describes the variables used in Event Center messages.

TABLE 73. VARIABLE DESCRIPTIONS

Variable	Description
$CURRENT_COUNTRY	The country in which the device is currently located.
$CURRENT_PHONE_NUMBER	The phone number currently associated with the device in Core, but not matching the phone number currently used by the device.
$DEFAULT_POLICY_VIOLATION_MESSAGE	The hard-coded message associated with the policy violation that triggered the alert.

TABLE 73. VARIABLE DESCRIPTIONS (CONT.)

Variable	Description
	ⓘ Due to the length limits of SMS, the text might be truncated.
$DEFAULT_SYSTEM_MESSAGE	The third-party system message or error that triggered the alert.
$FREE_MEMORY_SIZE	The amount of free memory currently available on the device.
$HOME_COUNTRY	The home country of the device.
$MEMORY_SIZE_LIMIT	The threshold set for the device memory.
$NEW_PHONE_NUMBER	The phone number replacing the $CURRENT_PHONE_NUMBER$ as a result of a SIM change.
$PHONE_NUMBER	The phone number used by the device.
$SERVER_IP	The IP address of the server triggering a system event alert.
$SERVER_NAME	The hostname of the server triggering the system event alert.
$SEVERITY	The defined severity of the system event, i.e., Information, Warning, or Critical.
$THRESHOLD_ON	The total used for calculations, i.e., International Roaming or Total Usage.
$THRESHOLD_TYPE	The type of usage measured, i.e., SMS, Data, or Voice.
$THRESHOLD_UNIT	The unit associated with the type of usage, i.e., minutes, messages, or MB.
$THRESHOLD_VALUE	The defined threshold value for this event, e.g., 1000 (voice minutes).
$TOTAL_MEMORY_SIZE	The total memory reported by the device.
$USED_VALUE	The amount of memory currently used on the device.
$USER_NAME	The display name of the user associated with the device.

Specifying which template to use

When you create or edit an event, you specify which template to use for resulting alerts. To select a template:

1. Create or edit an event.

2. Select a template from the drop-down or click the **Create** button to create a new template.

Filtering Event Center messages

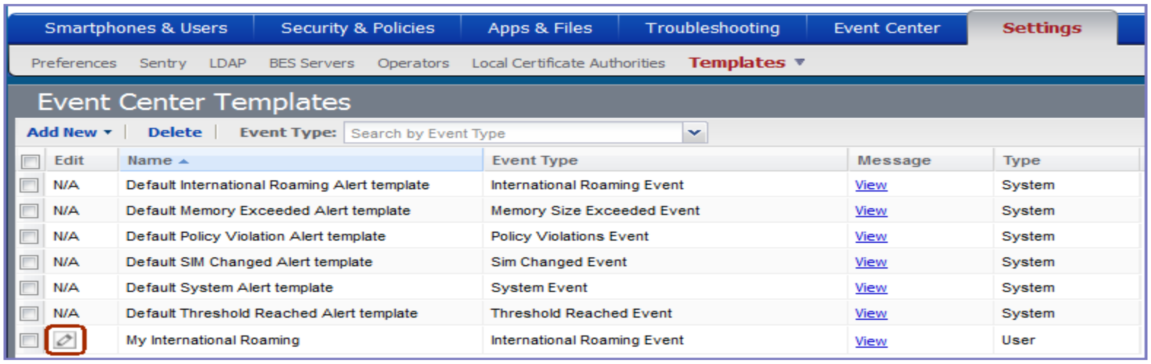
In the Event Center Templates page, you can filter messages by event type. Just select the preferred event type from the **Event Type** drop-down.

Editing Event Center messages

You can edit your custom Event Center templates. However, default Event Center templates are not editable.

To edit a custom Event Center template:

1. In Admin Portal, go to **Settings > Templates > Event Center Templates**.



□	Edit	Name ▲	Event Type	Message	Type
□	N/A	Default International Roaming Alert template	International Roaming Event	View	System
□	N/A	Default Memory Exceeded Alert template	Memory Size Exceeded Event	View	System
□	N/A	Default Policy Violation Alert template	Policy Violations Event	View	System
□	N/A	Default SIM Changed Alert template	Sim Changed Event	View	System
□	N/A	Default System Alert template	System Event	View	System
□	N/A	Default Threshold Reached Alert template	Threshold Reached Event	View	System
□	✎	My International Roaming	International Roaming Event	View	User

2. Click the edit icon for the custom template you want to edit.

3. Make your changes. See "Sending a company-branded email" on page 31

4. Click **Save**.

Deleting Event Center messages

You can delete any of the Event Center messages you have created:

1. In Admin Portal, go to **Settings** > **Templates** > **Event Center Templates**.
2. Select the items you want to delete.
3. Click **Delete**.

Viewing and Exporting Events

Use the Events screen to track the events that have triggered alerts. To display the Events screen, go to **Logs > Events**.

Marking as Read or Unread

To enable tracking of which events have been noted and/or addressed by an administrator, you can mark an event as **Read**. Likewise, you can switch this flag back to **Unread**.

To set the Read/Unread flag:

1. Select one or more events.
2. Select **Read** or **Unread** or from the **Actions** menu.

Filtering events

You can display the events using the following filters:

TABLE 74. FILTERING EVENTS

Filter	Description
Read/Unread	Select **Read** or **Unread** from the **Show** drop-down list. To resume displaying all events, select **All**.
All	Select **All** to resume displaying all events.
Labels	Select the preferred label from the **Labels** drop-down to filter based on the label specified in the event.
User	Enter a user ID and click the search icon to filter based on the user IDs specified in the event.
Start Date/End Date	Select dates in the **Start Date** and **End Date** fields to filter events by date range.
Event Type	Select an event type from the **Type** drop-down to filter by event type.
Event Status	Select an event status from the status drop-down to filter based on the event's lifecycle state.

Event lifecycle and status

Events go through the following lifecycle:

Created -> Dispatch Pending -> Dispatching -> Dispatched

The following two failure states may also occur:

- Dispatch Failed: The process of generating the alert failed. This is usually the result of an SMTP problem. Check the SMTP configuration in System Manager, as well as the health of your SMTP server.
- Expired: Another event occurred that makes the alert obsolete, resulting in expiration before dispatch.

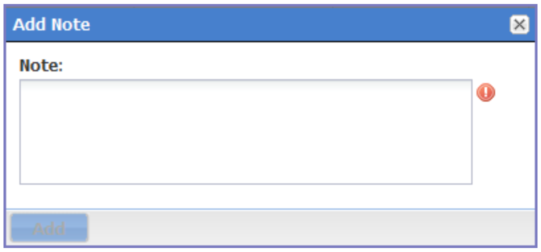
Exporting event history

To export a CSV file containing the currently displayed events on the **Logs > Events** page, click the **Export** button.

Adding a note

You can add a note to one or more events to help track the work that has been done in response. Each event can hold one note; adding another note replaces the existing note. To add a note:

1. Select one or more events.
2. Click **Actions > Add Note**.



3. Enter the text of the note.
4. Click **Add**.
5. Press F5 to refresh the screen and confirm that the note displays in the Note field for the selected events.

Troubleshooting Core and devices

This section addresses troubleshooting various aspects of Core and devices.

- "About Core logs" below
- "Audit log information" on page 401
- "Audit Logs use cases" on page 415
- "Viewing Errors" on page 420
- "Certificate Management" on page 420
- "Service Diagnostic tests" on page 423
- Encrypting device logs with your own certificate
- Pull client logs for client devices

About Core logs

As you oversee management and security of users, data and devices, you will need information about the actions and events that occur in your Core instance. Core logs many actions that can impact your Core instance, and provides the Audit Logs page for you to sort and view the logged information.

The following pages of logs, found in the Admin Portal under **Logs**, enable you to easily navigate through the Core log entries to find the information you need.

- **Audit Logs**: for Core device management entries
- **Certificate Management**: for certificate-related entries

Note the following:

- Logs are stored in the Core file system, not in the Core database. Therefore, the size of the logs does not impact Core performance.

- Core will show up to 1 million audit log records.

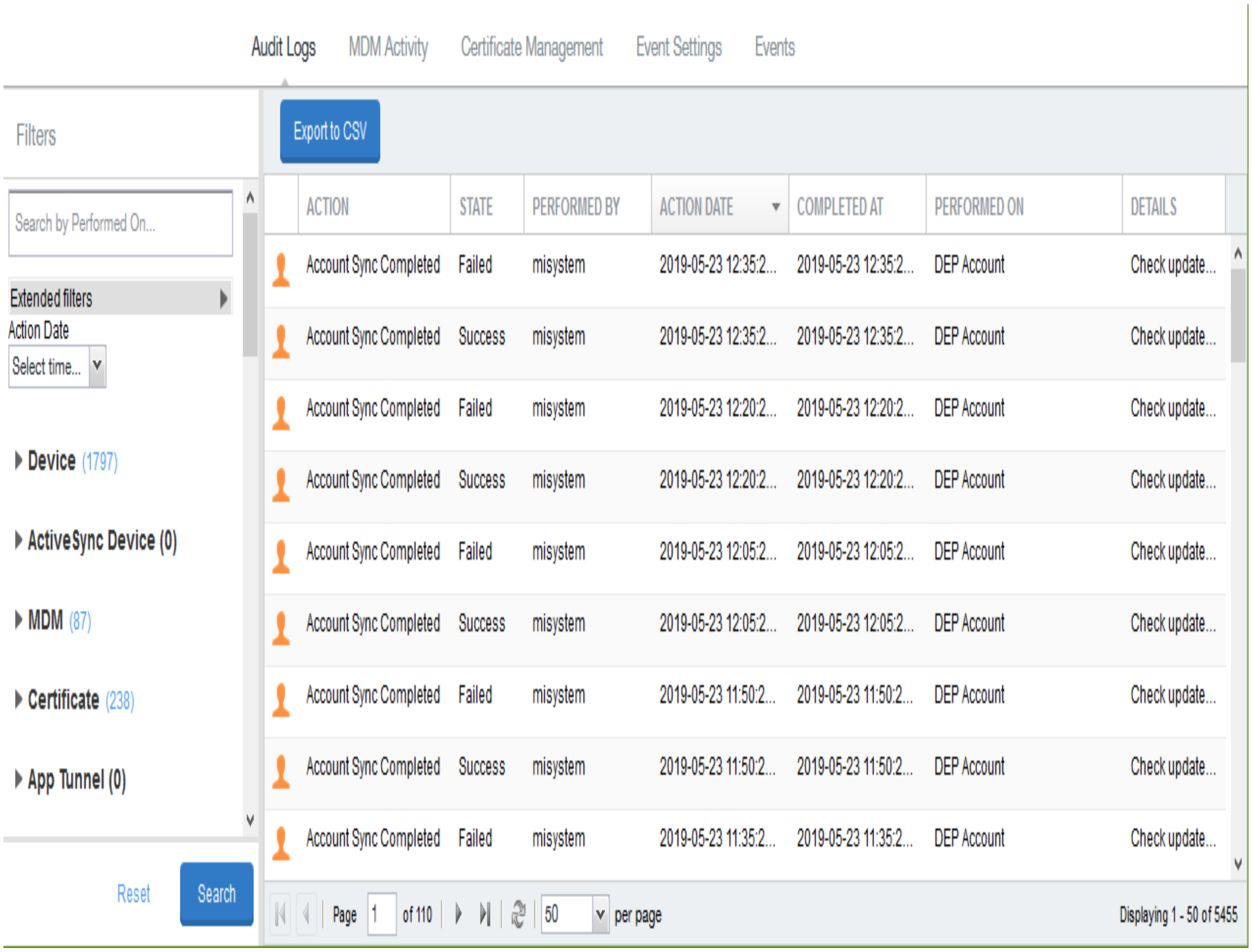
Audit logs

Using log entries, the Admin Portal tracks status and operations for each managed device. You can use log entries to confirm that actions were completed and to investigate problems.

The Audit Logs page includes panels that:

- enable you to filter through all events that Core has logged since the last time the logs were purged
- shows either the events recorded since the logs were last purged, or the events matching the criteria you specified in the Filters panel

FIGURE 1. AUDIT LOGS



ACTION	STATE	PERFORMED BY	ACTION DATE	COMPLETED AT	PERFORMED ON	DETAILS
Account Sync Completed	Failed	misystem	2019-05-23 12:35:2...	2019-05-23 12:35:2...	DEP Account	Check update...
Account Sync Completed	Success	misystem	2019-05-23 12:35:2...	2019-05-23 12:35:2...	DEP Account	Check update...
Account Sync Completed	Failed	misystem	2019-05-23 12:20:2...	2019-05-23 12:20:2...	DEP Account	Check update...
Account Sync Completed	Success	misystem	2019-05-23 12:20:2...	2019-05-23 12:20:2...	DEP Account	Check update...
Account Sync Completed	Failed	misystem	2019-05-23 12:05:2...	2019-05-23 12:05:2...	DEP Account	Check update...
Account Sync Completed	Success	misystem	2019-05-23 12:05:2...	2019-05-23 12:05:2...	DEP Account	Check update...
Account Sync Completed	Failed	misystem	2019-05-23 11:50:2...	2019-05-23 11:50:2...	DEP Account	Check update...
Account Sync Completed	Success	misystem	2019-05-23 11:50:2...	2019-05-23 11:50:2...	DEP Account	Check update...
Account Sync Completed	Failed	misystem	2019-05-23 11:35:2...	2019-05-23 11:35:2...	DEP Account	Check update...

Searching the information in the audit logs

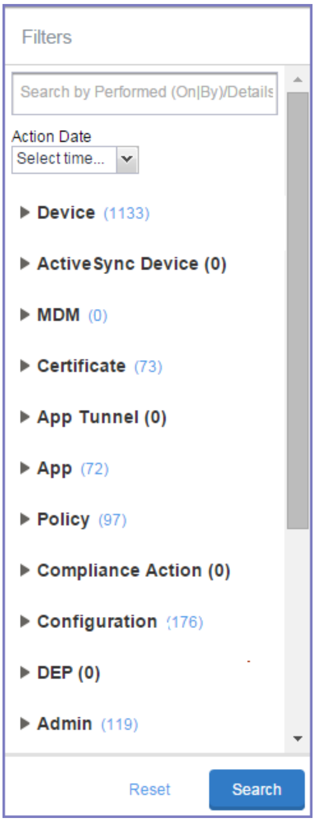
Procedure

1. In Admin Portal, go to **Logs**.

   Core displays the Audit Logs page, which initially lists the events logged since the last time the logs were purged.

2. In the **Filters** panel, click on the number of events in a category to display only that category's events.

   For example, click the **72** next to **App**.



.

3. Alternatively, click to expand one of the information types that you want to view (for example, **App**).

4. Check the items within that category that you want to view (for example, **Add App** and **Install App**).

5. Repeat Step 3 and Step 4 for each category that you want to include in this search.
6. (Optional) To search for events involving a particular administrator, or actions that contain a specific word or phrase in the details, use the **Search by Performed (On|By)/Details** box in the Filters panel as follows:
   - enter the search string in the text box.
   - for example, to find events involving Mobile@Work, enter the text **Mobile@Work.**
7. (Optional) To limit the time frame of the actions, use the **Action Date** box (see "Setting event time criteria in audit logs" below)
8. Click **Search**.

   The Audit Logs page shows all events matching your search criteria and time period. If you do not specify a time period, the default used is the period between the time you run the search and when the log data was last purged.
9. To reset all search criteria, click **Reset**.

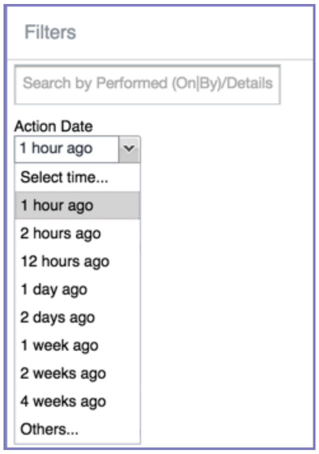
Setting event time criteria in audit logs

When you are working with audit logs, the default time frame for the events displayed is the time between the current time and the last time the logs were purged (for information about setting the log retention time, see "Specifying how long log information is saved" on page 400). For example, if the logs were purged two weeks ago, the Audit Logs display all the events matching any criteria you set that occurred from two weeks ago to the current moment.

You can change the time frame of events you view in the **Filters** panel. You can select by time or date.

Procedure

1. In Admin Portal, go to **Logs**.
2. In the Filters panel, click the drop-down arrow in **Action Date**.



3. Select one of the times listed or **Others**.

   Selecting a time displays the events matching criteria you set, if any, for the time period from the last time the logs were purged until the time you specify.

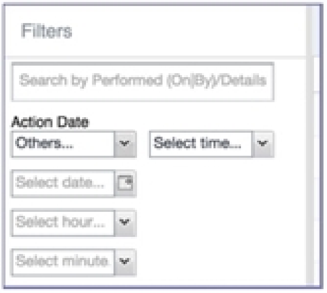
   Any events that occurred between the specified time period and the current moment are not displayed. For example, if you select **1 hour ago**, no events that happened within the last hour are displayed.

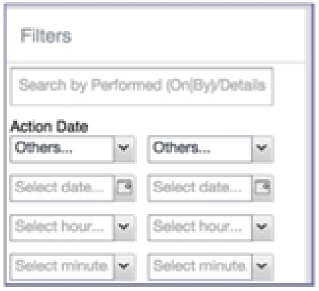
4. If you select **Others**:

   - using the left column of time choices in Filters, you can specify an exact date, hour or minute (or any combination of these criteria) as one end of the time frame and use the date of the last audit log purge as the other end of the time frame

   - using the left and right columns of time choices in Filters, you can specify both the beginning and end of the time range.

   Use the following table to help you set the time range for your search.





- When you set only one end of the time frame, the date or time you specify must be later than the last date the log data was purged. If the last log purge was May 13th, for example, May 12th would not be a valid date for selecting events.
- When you set both ends of the time frame, ensure that the time or date specified in the left column occurs before the time or date specified in the right column. For example, if you specify **1 hour ago** in the left column and **1 day ago** in the right column, Core will display a message asking you to reset your time criteria because 1 hour ago happens after 1 day ago.

TABLE 75. TIME CRITERIA SELECTION EXAMPLES

Time criteria selected	Value selected	Result
In the left column, select both: • **Others** • **Select date**	Click May 12th in the displayed calendar	Displays all events matching your criteria that occurred from the last audit log data purge until May 12th.
In the left column, select both: • **Others** • **Select hour**	Select 2AM from **the list of hours**	Displays all events matching your criteria that occurred from the last audit log data purge until 2AM of the current day.
In the left column, select both: • **Others** • **Select minute**	Select 15 from the list of **minutes**	Displays all events matching your criteria that occurred from the last audit log data purge until the 15th minute of the current hour.
In the left column, select: • **Others** • Select date	In the left column: • Select **April 10th** from the calendar In the right column:	Displays all events matching your criteria that occurred between April 10th and 24 hours ago.

TABLE 75. TIME CRITERIA SELECTION EXAMPLES (CONT.)

Time criteria selected	Value selected	Result
In the right column, select: - a time interval from **Select time**	- Select **1 day ago**	
In the left column, select: - **Others** - Select hour In the right column, select: - a time interval from **Select time**	In the left column: - Select **2AM** In the right column: - Select 1 hour ago	Displays all events matching your criteria for the time period that started at 2AM the morning of the current day and ended an hour ago.

Viewing audit log information

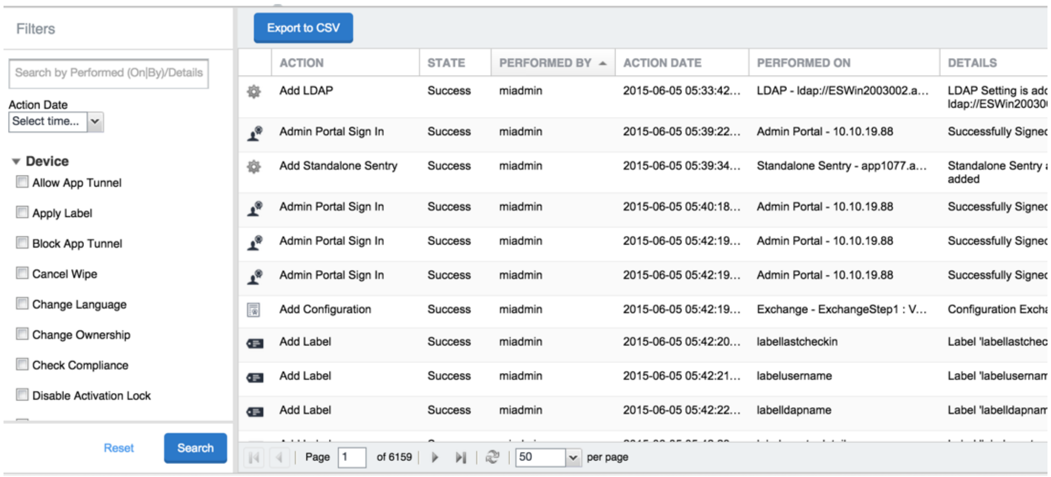
The Audit Logs page displays the information that Core records for your Core instance. You specify what information is displayed on this page when you use the controls in the **Filters** panel of the page. See "Searching the information in the audit logs" on page 395 for details.

Procedure

1. In Admin Portal, go to **Logs**.

   Core displays the Audit Logs page. The information panel displays:

   Action (for example, Admin Portal sign-in)



	ACTION	STATE	PERFORMED BY	ACTION DATE	PERFORMED ON	DETAILS
	Add LDAP	Success	miadmin	2015-06-05 05:33:42...	LDAP - ldap://ESWin2003002.a...	LDAP Setting is add ldap://ESWin20030
	Admin Portal Sign In	Success	miadmin	2015-06-05 05:39:22...	Admin Portal - 10.10.19.88	Successfully Signed
	Add Standalone Sentry	Success	miadmin	2015-06-05 05:39:34...	Standalone Sentry - app1077.a...	Standalone Sentry a added
	Admin Portal Sign In	Success	miadmin	2015-06-05 05:40:18...	Admin Portal - 10.10.19.88	Successfully Signed
	Admin Portal Sign In	Success	miadmin	2015-06-05 05:42:19...	Admin Portal - 10.10.19.88	Successfully Signed
	Admin Portal Sign In	Success	miadmin	2015-06-05 05:42:19...	Admin Portal - 10.10.19.88	Successfully Signed
	Add Configuration	Success	miadmin	2015-06-05 05:42:19...	Exchange - ExchangeStep1 : V...	Configuration Excha
	Add Label	Success	miadmin	2015-06-05 05:42:20...	labellastcheckin	Label 'labellastchec
	Add Label	Success	miadmin	2015-06-05 05:42:21...	labelusername	Label 'labelusernam
	Add Label	Success	miadmin	2015-06-05 05:42:22...	labelldapname	Label 'labelldapnam

- **State** (for example, **Success**)
- **Performed By** (for example, **myadmin**)
- **Action Date**
- **Completed At**
- **Performed On** (for example, **Admin Portal**)
- **Details**

2. (Optional) Enter a number in **Page** to specify what page to view.
3. (Optional) Select a number from **per page** to specify how many records are displayed on a page.
4. (Optional) Click **Export to CSV** to export the records that match the current search criteria.

Specifying how long log information is saved

You specify how long log data is retained on your server. Determining how long to retain data is a balance between having data you need and having the available server resources to run your Core. The default value is 90 days.

Procedure

1. In System Manager, go to **Settings > Data Purge**.
2. In **Audit Logs Purge Configuration**, select the number of days Core retains log information.

3. Click **Apply**.

Audit log information

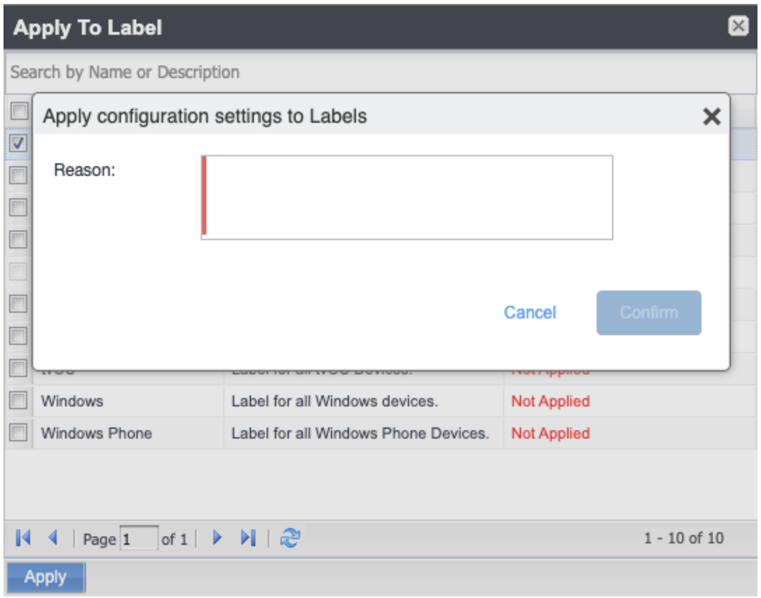
Several categories of information are available for you to view and audit. The category list, displayed on the left side of the Audit Logs page, includes:

- **Device**
- **ActiveSync Device**
- **MDM**
- **Certificate**
- **App Tunnel**
- **App**
- **Policy**
- **Compliance Action**
- **Configuration**
- **DEP (Device Enrollment)**
- **Admin**
- **User**
- **LDAP**
- **Other**
- **Label**
- **Sentry**
- **AfW**
- **Custom Attributes**
- **Compliance Policy**
- **E-FOTA**

- **Migration**
- **MTD (Mobile Threat Defense)**
- **Access Integration**
- **Derived Credential Provider**
- **Zebra FOTA**

Best practices: label management

If Notes for Audit Logs is enabled, whenever a change is made to a label, a text box displays for the administrator to provide a reason for the change.



Apply To Label

Search by Name or Description

Apply configuration settings to Labels

Reason:

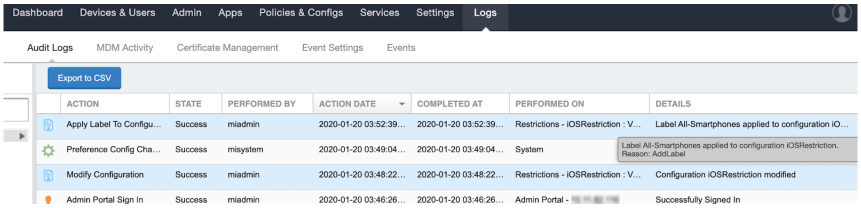
Cancel Confirm

□	Windows	Label for all Windows devices.	Not Applied
□	Windows Phone	Label for all Windows Phone Devices.	Not Applied

Page 1 of 1 — 1 - 10 of 10

Apply

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



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	
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 - [redacted]	Successfully Signed In

Label All-Smartphones applied to configuration iOSRestriction.
Reason: AddLabel

This affects the following label-related activities:

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

The Notes for Audit Logs feature is also applicable to any administrator-made changes to iOS and macOS restrictions.

To enable this feature, see "Setup tasks" in *Getting Started with Core.*

Device events

Device events record device-related actions taken by an administrator in the Admin Portal.

To monitor device actions, select one or more of the logged device actions in the **Filters** panel:

- **Allow App Tunnel**: Manually allow app tunnels from the selected device.
- **Apply Label**: Associate an item with a label.
- **Apply Multiple Labels to One Device**: Associate an item with multiple labels.
- **Block App Tunnel**: Manually disallow app tunnels from the selected device.
- **Cancel Wipe**: Cancels pending "Wipe" command if it was not yet delivered to the device. Applies to all modes.
- **Change Language**: Change the language associated with a device.
- **Change Ownership**: Toggle device ownership between Employee and Company.
- **Check Available OS Update**:
- **Check Compliance**: Check device against compliance criteria.
- **Delete Retired Device**: Remove entry for a device that is not longer managed.

- **Device Location**:
- **Disable**:
- **Disable Activation Lock**: Turn off the activation lock feature for the selected iOS device.
- **Disable Data Roaming**: Turn off the ability to use data when the device is roaming.
- **Disable due to out of compliance**:
- **Disable Kiosk**: Exit kiosk mode on the designated Android device.
- **Disable KNOX Container**: Turn off the Samsung Knox container feature for the selected device.
- **Disable Personal Hotspot**: Prevent the device user from using the personal hotspot feature.
- **Disable Voice Roaming**: Turn off the ability to make voice calls when the device is roaming.
- **Download Available OS Update**:
- **Enable**:
- **Enable Activation Lock**: Turn on the activation lock feature for the selected iOS device.
- **Enable Data Roaming**: Turn on the ability to use data while roaming for the selected iOS device.
- **Enable Kiosk**: Start kiosk mode on the designated Android device.
- **Enable KNOX Container**: Turn on the Samsung Knox container feature for the selected device.
- **Enable MDM Lost Mode**: Enable lost mode for the selected iOS device.
- **Enable Personal Hotspot**: Allow the device user to use the personal hotspot feature.
- **Enable Voice Roaming**: Turn on the ability to make voice calls when the device is roaming.
- **Found**: Designate the selected lost device as found.
- **Install Downloaded OS Update**:
- **Install Help@Work**: Install the Help@Work app.
- **Locate**: Retrieve the last known location for the selected device.
- **Lock**: Force the selected device to require a passcode for user access.

- **Lost**: Designate the selected device as lost.
- **MobileIron Bridge**: Create a configuration for the Bridge application for Windows 10 Management.
- **Push Profile**: Prompt a manual distribution of profiles to the selected device.
- **Re-provision Device**: Restart the provisioning process for the selected device.
- **Reboot**: Reboot the selected Windows device.
- **Register Device**: Start the registration process for the selected device.
- **Remote Control**: Establish a remote control session (Help@Work) on the selected Android device.
- **Remote Display**: Establish a remote view session (Help@Work) on the selected iOS device.
- **Remove Device Attribute**: Remove an attribute from a device.
- **Remove Label**: Remove the association between the specified label and the selected item.
- **Remove Multiple labels from one device**: Remove the association between the specified labels and the selected item.
- **Request Derived Credential: Device user request in user portal for a derived credential.**
- **Request Unlock AppConnect Container** (Android only): Initiate unlock AppConnect container.
- **Request Unlock Device**: Initiate unlock device.
- **Request Unlock Passcode**: Initiate unlock passcode.
- **Resend Provision Message**: No longer supported.
- **Reset AppConnect Passcode:** Device user request in user portal to reset the AppConnect passcode.
- **Reset Password:**
- **Restart iOS Device**: Restart iOS device.
- **Reset PIN**: Generate a new registration PIN for the selected Windows device.
- **Retire**: End management of the selected device.

- **Send Activation Lock Bypass Code**: Send the bypass code to the selected iOS device.
- **Send Alert**: Send compliance alert to the selected device.
- **Send APNS message**: Launch a client and authenticate against Core.
- **Send Message**: Send SMS message to the selected device.
- **Set Device Attribute:** Set an attribute to a device.
- **Shutdown iOS Device**: Shutdown iOS device.
- **Sign In**: Launch a client and authenticate against Core.
- **Sign Out**: End session between the client and Core.
- **Substitution Variable Change**: Change a configuration due to a change in the value of a substitution variable.
- **Unlock AppConnect Container** (Android only): Begin unlock device and AppConnect container.
- **Unlock Device and AppConnect Container**: (Android only): Begin unlock device and AppConnect container.
- **Unlock Device Only**: Clear the passcode for the selected device.
- **Update Device Comment**: Change the Comment field in the record for the selected device.
- **Update OS Software:** Update iOS software.
- **Wakeup**: Force the device client to check in.
- **Windows License:** Alert administrators to upgrade the SKU of Windows 10 desktop devices. Options can be Windows 10 Pro to Enterprise or Windows 10 Education to Enterprise.
- **Wipe**: Return the device to factory default settings.

Events beginning with **Request**, such as **Request Unlock Device**, are logged when an administrator clicks the corresponding command in the Admin Portal. The corresponding event without the word **Request**, such as **Unlock Device**, is logged when Core actually sends the request to the device. Core sometimes delays sending requests to regulate Core performance.

ActiveSync Device information

These events do not apply to Mac devices.

To monitor ActiveSync device actions, select one or more of the logged ActiveSync device actions in the **Filters** panel

- **ActiveSync Device Comment**: Add or change the comment associated with an ActiveSync device entry.
- **Add Correlation:**
- **Allow Device**: Allow a blocked ActiveSync device to access the ActiveSync server.
- **Assign ActiveSync Policy**: Apply an ActiveSync policy to the selected device.
- **Block Device**: Prevent the selected device from accessing the ActiveSync server.
- **Link To MI Device**: Associate an ActiveSync device with a device registered with Core.
- **Remove**: End the association between the Core device and the ActiveSync device record.
- **Remove Correlation:**
- **Revert ActiveSync Policy**: Restore the Default ActiveSync Policy to the selected device.

MDM events

MDM events indicate when a device takes an action due to a Core request. These events pertain only to iOS and Mac devices unless otherwise noted.

To monitor these actions, select one or more of the logged MDM actions in the **Filters** panel.

- **Apply Redemption Code**: Apply Redemption Code: Use a Apple License code.
- **Clear Passcode**: Clear Passcode: Reset device passcode.
- **Device Lock**: Set screen lock on device.
- **Install Encrypted Sub-Profile:**
- **Install Managed Application**: Install a managed app.
- **Install MDM Profile**: Install the MDM profile on the device.
- **Install Provisioning Profile**: Install the provisioning profile for a managed app.
- **Lock Device (Android):** Lock an Android device.

- **Profile Change**: Change the profile on an iOS or Android device.
- **Remove Encrypted Sub-Profile:**
- **Remove Managed Application**: Uninstall a managed app.
- **Remove MDM Profile**: Remove the MDM profile from the device.
- **Remove Provisioning Profile**: Remove the provisioning profile for a managed app.
- **Settings**: Modify device settings.
- **Unlock Device (Android)**: Unlock an Android device and the AppConnect container on the device.
- **Unlock Device Only (Android)**: Unlock an Android device.
- **Wipe Device** (called **Erase Device** in the **MDM Activity** tab): Restore the iOS device to factory defaults.
- **Wipe Device (Android)**: Restore the Android device to factory defaults.

Certificate events

To monitor actions involving certificates, select one or more of the logged certificate actions in the **Filters** panel.

- **Apply User Provided Certificate**: Use a certificate already provided by the user and sent to Core.
- **Create Device Certificate**: Issue a device certificate.
- **Create User Certificate**: Issue a user certificate.
- **Delete User Provided Certificate**: Destroy certificate provided by the user via the self-service portal.
- **Device Certificate Expired**: Warn on a device certificate that is no longer valid due to expiration.
- **Device Certificate Renewal**: Re-enrolls a device certificate.
- **Reuse Device Certificate**: Use an existing device certificate.
- **Reuse User Certificate**: Use an existing user certificate.

- **Revoke Device Certificate**: Reclaim a device certificate.
- **Revoke User Certificate**: Reclaim a user certificate.
- **Upload User Provided Certificate**: Send certificate provided by the user via the self-service portal.
- **User Certificate Expired**: Warn on a user certificate that is no longer valid due to expiration.
- **User Certificate Renewal**: Re-enroll a user certificate.

The contents of the **Logs > Certificate Management** shows information about certificates, such as their expiration dates. It allows you to take actions, such as re-enroll, remove, and revoke on the certificates.

App Tunnel events

To monitor actions involving app tunnels, select one or more of the logged app tunnel actions in the **Filters** panel.

- **Allow App Tunnel**: Permit the specified app tunnel.
- **App Tunnel Comment**: Add a comment on the selected app tunnel.
- **Block App Tunnel**: Do not allow the specified app tunnel.
- **Remove App Tunnel**: Delete the selected app tunnel configuration.

App information

To monitor actions involving apps, select one or more of the logged app actions in the **Filters** panel.

- **Add App**: Add an app to the app catalog.
- **Add App Control Rule**: Add an app control rule.
- **Add App Dependency**:
- **Add App Resource**: Add screenshots or icons for an app.
- **Apply Label to App**: Associate a label with an app.
- **Delete App Control Rule**: Remove an app control rule.

- **Edit App Control Rule**: Change one or more attributes of an app control rule.
- **Install App**: Send installation request for the selected app.
- **Manage VPP Labels**: Specify labels and account for Apple License app distribution.
- **Modify App**: Edit app catalog entry.
- **Remove App**: Delete entry from the app catalog.
- **Remove Label From App**: End the association between an app and a label.
- **Uninstall App**: Remove the app from the device based on managed app criteria.

Policy information

To monitor actions involving policies, select one or more of the logged policy actions in the **Filters** panel.

- **Activate Policy**: Set flag to make the selected policy active.
- **Add Policy**: Create a new policy.
- **Apply Label to Policy**: Associate a policy and a label.
- **Deactivate Policy**: Clear flag to make the selected policy inactive.
- **Delete Policy**: Delete a policy.
- **Export Policy**: Export a policy from Core.
- **Import Policy**: Import a policy into Core.
- **Modify Policy**: Change an attribute of an existing policy.
- **Modify Policy Priorities**:
- **Modify Policy Priority**: Change the priority for an existing policy.
- **Remove Label From Policy**: End the association between a policy and a label.

Compliance Action events

To monitor compliance actions, select one or more of the logged compliance actions in the **Filters** panel

- **Add Compliance Action**: Create a set of actions to be taken on devices that violate policies.
- **Delete Compliance Action**: Remove a set of actions to be taken on devices that violate policies.
- **Modify Compliance Action**: Make changes to a set of actions to be taken on devices that violate policies.
- **Modify Compliance Check Preferences**: Make changes to compliance preferences.

Configuration events

- **Add Configuration**: Create a new configuration.
- **Apply Label To Configuration**: Associate a configuration with a label.
- **Export Configuration**: Export a configuration from Core.
- **Import Configuration**: Import a configuration to Core.
- **Modify Configuration**: Change the settings in a configuration.
- **Remove Configuration**: Delete a configuration.
- **Remove Label From Configuration**: End the association between a configuration and a label.
- **Remove Labels From Configuration**: End the association between a configuration and multiple labels.

Admin events

- **Add Space**: Define a new delegated administration space.
- **Admin Portal Sign In**: Start an Admin Portal session.
- **Admin Portal Sign Out**: End an Admin Portal session.
- **Assign Space Admin**: Specify an administrator for a space.
- **Change Space Priority**: Set a different priority for a space.
- **Delete Space Admin**: Remove space admin access from the user.
- **Modify Space**: Make changes to rules that define a space.

- **Remove Admin From Space**: Remove the admin user from the space.
- **Remove Space**: Delete all rules that define a space and reallocate its devices.
- **Update Device Space**: Recalculate space rules to determine device membership.
- **User Locked Out**: Prevent administrator from further attempts at signing in after limit on authentication failures is exceeded.

User events

- **Add User**: Define a new Core user.
- **Delete User**: Remove a Core user.
- **Link to LDAP User**: Associate a local Core user with an LDAP user.
- **Modify User**: Make changes to a user’s attributes.
- **Modify User Role**: Make changes to the roles assigned to a user.
- **Re-sync with LDAP**: Synchronize LDAP data.
- **Remove User Attribute**: Remove an attribute from a user.
- **Renew Google Apps password**: Manually regenerate a user’s Google Apps password.
- **Require Password Change**: Force a local user to change their Core password.
- **Send Invitation**: Invite a user to register with Core.
- **Set User Attribute**: Set an attribute for a user.
- **User Portal Sign In**: Start User Portal session.
- **User Portal Sign Out**: End User Portal session.

LDAP events

- **Add LDAP**: Integrate an LDAP server with Core.
- **Delete Admin LDAP Entity**: Delete an Admin LDAP entity that has no roles.
- **Delete LDAP**: End the integration between an LDAP server and Core.

- **Delete LDAP Entity**: Delete a user LDAP entity that has no roles.
- **Modify LDAP**: Make changes to the record for an integrated LDAP server.
- **Modify LDAP Preferences**: Make changes to the preferences for integrated LDAP servers.
- **Upload LDAP Certificate**: Add an LDAP certificate to Core.

Other events

- **Application Started**: Start Core services.
- **Application Stopped**: Stop Core services.
- **Complete feature usage collection**: Complete the current run of feature usage collection.
- **Feature usage collection error**: Encountered error during collection.
- **Feature usage collection scheduling error**: Encountered scheduling error during collection.
- **Initiate feature usage collection**: Start feature usage collection.
- **Purge feature usage data**: Purge collected feature usage information.
- **Preference Config Changes**: Make changes to the settings under **Settings > System Settings** in the Admin Portal.
- **Retrieve feature usage data**: Start collecting feature usage data.
- **Retrieve feature usage data file list**: Start retrieval of the usage data file list.

Label events

- **Add Label**: Define a new label for Core.
- **Delete Label**: Remove a label from Core.
- **Modify Label**: Make changes to a label.
- **Save As Label**: Copy a label to a new label.

Sentry events

- **Add Integrated Sentry**: Establish a relationship between Core and an Integrated Sentry.
- **Add Standalone Sentry**: Establish a relationship between Core and a Standalone Sentry.
- **Delete Integrated Sentry**: End the relationship between Core and an Integrated Sentry.
- **Delete Standalone Sentry**: End the relationship between Core and a Standalone Sentry.
- **Disable Integrated Sentry**: Suspend the interaction between Core and an Integrated Sentry.
- **Disable Standalone Sentry**: Suspend the interaction between Core and a Standalone Sentry.
- **Edit Integrated Sentry**: Make changes to the settings for an Integrated Sentry.
- **Edit Standalone Sentry**: Make changes to the settings for a Standalone Sentry.
- **Enable Integrated Sentry**: Start the interaction between Core and an Integrated Sentry.
- **Enable Standalone Sentry**: Start the interaction between Core and a Standalone Sentry.
- **Manage Certificate**: Upload a certificate for Standalone Sentry.
- **Modify Sentry Preferences**: Make changes to the settings under **Services > Sentry**.
- **Regenerate Key**: Generate a new control key for attachment encryption.
- **Regenerate Attachment Encryption Control Key**:
- **Resync Integrated Sentry With Exchange**: Force Integrated Sentry to synchronize mailbox data with the Exchange server.

Custom attributes events

- **Add Custom Attribute**: Create a new customer attribute definition.
- **Modify Custom Attribute**: Modify a customer attribute definition.

Compliance policy events

- **Add Compliance Policy Group**: Add a new compliance policy group.
- **Add Compliance Policy Rule**: Add a new compliance policy rule.

- **Apply Label to Compliance Policy Group**: Apply one or more labels to a compliance policy group.
- **Modify Compliance Policy Group**: Modify a compliance policy group.
- **Modify Compliance Policy Rule**: Modify a compliance policy rule.
- **Remove Compliance Policy Group**: Delete a compliance policy group.
- **Remove Compliance Policy Rule**: Delete a compliance policy rule.
- **Remove Label From Compliance Policy Group**: Delete one or more labels from a compliance policy group.

Audit Logs use cases

A wealth of information is available to you in the Audit Logs. Querying the events allows you to monitor your Core system and resolve problems. You can run queries for one type of event, several types of events, or as many as you like. All you need to do is check the events you want to track, and then specify a time frame. The default time frame is the time between the last time the logs were purged and the current time.

For example:

- Use the certificate events to troubleshoot certificate issues. For example, query for certificates that have expired or have been revoked.
- Use the MDM events to troubleshoot MDM activity on devices. For example, query whether an MDM profile was removed, or whether a managed app was installed.
- Use the AppTunnel events to determine whether an administrator manually blocked or allowed AppTunnel on a device.
- Use the device events to determine activity taken on devices, such as unlocking the device, or deleting retired devices.
- Use the app events to determine whether an administrator has changed the app control rules in Core. A change to app control rules can result in Core taking, or not taking, compliance actions such as blocking email on devices.

This section presents several scenarios and how you can use the audit logs to resolve the problems they present.

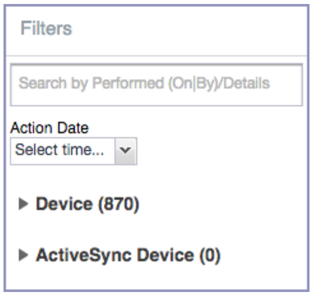
Personal information is wiped from devices

Suppose several of your users report that the personal information on their phones was wiped. How can you figure out how this happened? Using the audit logs, you can check the wipe actions recorded in the logs, and discover:

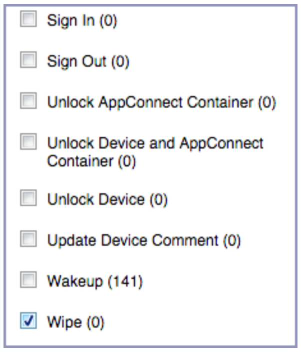
- who issued the Wipe commands
- when they occurred
- how many users are impacted

To resolve this problem:

1. In the Admin Portal, select **Logs**.
2. Select **Audit Logs**.
3. Click **Reset** at the bottom of the **Filters** panel to ensure that the previous search values are cleared.
4. In the **Filters** panel, specify a time interval that you suspect the device wipe(s) happened.
5. Open the **Device** events list.



6. Select **Wipe**.



☐ Sign In (0)
☐ Sign Out (0)
☐ Unlock AppConnect Container (0)
☐ Unlock Device and AppConnect Container (0)
☐ Unlock Device (0)
☐ Update Device Comment (0)
☐ Wakeup (141)
☑ Wipe (0)

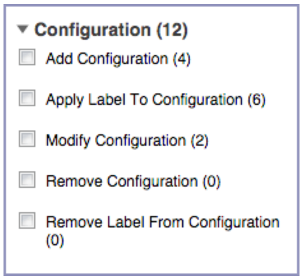
7. Click **Search**.
8. View the results of the search to determine:
   - when the devices were wiped
   - how many devices were wiped
   - which admin user issued the wipe commands

Users are prompted for email passwords when not necessary

Suppose you set up your Exchange policy to not require your users to provide a password when they log in to email, but your users are still prompted for a password each time they access email.

To check for any changes to the Exchange policy that could cause this problem:

1. In the Admin Portal, select **Logs**.
2. Select **Audit Logs**.
3. Click **Reset** at the bottom of the **Filters** panel to ensure that the previous search values are cleared.
4. In the **Filters** panel, specify a time interval that you suspect changes to the Exchange policy happened.
5. Open the **Configuration** events list.



▾ Configuration (12)

□ Add Configuration (4)

□ Apply Label To Configuration (6)

□ Modify Configuration (2)

□ Remove Configuration (0)

□ Remove Label From Configuration (0)

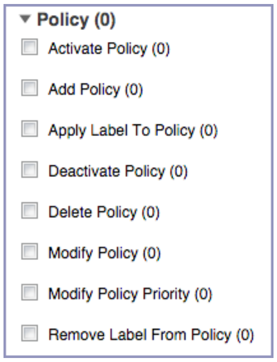
6. Select **Modify Configuration**.
7. Click **Search**.
8. View the results of the search to determine:
    - what changes were made recently to the Exchange policy
    - which admin user made the changes

Users are prompted to create passwords

Suppose your users are prompted to create device passwords when that is not how you set up your Core. You can use the audit logs to discover if this requirement is set and when this change occurred.

To check for changes to mandatory passwords:

1. In the Admin Portal, select **Logs**.
2. Select **Audit Logs**.
3. Click **Reset** at the bottom of the **Filters** panel to ensure that the previous search values are cleared.
4. In the **Filters** panel, specify a time interval that you suspect changes to the security policy happened.
5. Open the **Policy** events list.



▾ Policy (0)

- □ Activate Policy (0)
- □ Add Policy (0)
- □ Apply Label To Policy (0)
- □ Deactivate Policy (0)
- □ Delete Policy (0)
- □ Modify Policy (0)
- □ Modify Policy Priority (0)
- □ Remove Label From Policy (0)

6. Select **Modify Policy**.
7. Click **Search**.
8. View the results of the search to determine:
   - what changes, if any, were made recently to the Security policy
   - which admin user made the changes

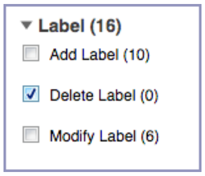
Devices have lost their managed apps

If your users report missing managed apps, the cause is usually deleted labels.

For Android devices 11.0 or supported newer versions, the administrator does not have the ability to manage app installs on the personal side.

To determine whether labels were deleted from your Core:

1. In the Admin Portal, select **Logs**.
2. Select **Audit Logs**.
3. Click **Reset** at the bottom of the **Filters** panel to ensure that the previous search values are cleared.
4. In the **Filters** panel, specify a time interval that you suspect the labels were deleted.
5. Open the **Label** events list.



Label (16)

□ Add Label (10)

☑ Delete Label (0)

□ Modify Label (6)

6. Select **Delete Label**.
7. Click **Search**.
8. View the results of the search to determine:
   - what labels, if any, were deleted recently
   - which admin user made the changes

Viewing Errors

Errors result in the display of a **View Error** link in the **Error** column. Error details are not available for Windows devices.

Certificate Management

The **Logs > Certificate Management** tab displays certificate-related log entries. You can:

- view certificate log entries
- search certificate log entries
- remove selected certificates from the log
- revoke selected certificates from the log
- re-enroll selected certificates from the log

Actions on certificates are logged in **Logs > Audit Logs**in the **Certificate** category**.**

How to search for certificate entries

When viewing the **Certificate Management** page, you can search for entries based on:

- expiration date
- user
- setting

Procedure

1. In the Admin Portal, go to **Logs > Certificate Management**.
2. Specify one or more of the criteria in the following steps to describe the certificates you want to display.
3. (Optional) To specify a time range within which the certificates expired:
    - In the **Expiration Date Range** field, click the calendar next to the field, and then click on a date. This date is the earliest day the certificates you are searching for expired.
    - In the **To** field click the calendar next to the field, and then click on a date. This date is the latest day the certificates you are searching for expired.

    An error message displays if you select a day in the **Expiration Date Range** field earlier than the day specified in the **To** field. For example you receive an error message if you:

    - An error message displays if you select a day in the **Expiration Date Range** field earlier than the day specified in the **To** field. For example you receive an error message if you:
    - select November 13th in the Expired Date Range field (earliest time a certificate expired).
    - select October 15th in the To field (latest time a certificate expired).

    The search can return fewer than all the certificates that expired during the specified time period if you specify other criteria in Step 4.

4. (Optional) In **Search by User/Setting Name**, enter a username or a setting name.

Item	Description
Certificate Enrollment	Displays the name of the Certificate Enrollment setting.
Setting	Displays the configuration using the Certificate Enrollment. The configuration displays only for a non-cached Certificate Enrollment. Configuration names are not available for certificates created in VSP Version 6.0 or earlier. For a cached Certificate Enrollment certificate, you will always see - in the Setting Name, regardless of whether it was created prior to version 7.0 or created in version 7.0.

5. Click **Search**.

   Search results are displayed in a table with the following columns:

Item	Description
User	The user name of the device user identified by the identity certificate.
Phone Number	The phone number associated with the device user identified by the identity certificate.
Email	The email address associated with the device user identified by the identity certificate.
Certificate Enrollment Name	The name of the certificate enrollment (such as SCEP, Local, Entrust) used to issue the identity certificate.
Setting Name	The name of the setting that uses the certificate enrollment, such as an Exchange or Web@Work setting.
Cert Type	Indicates whether the certificate is a user-provided certificate enrollment. Otherwise, this field is left blank.
Expiration Date	The date by which the identity certificate will no longer be valid.
Content	Click the **View** link to see the contents of the identity certificate itself.

How to remove a certificate

This action removes the certificate from device, but does not remove the SCEP setting.

Procedure

1. Go to **Logs > Certificate Management**.
2. Select the certificate that you want to remove.
3. Click **Actions > Remove**.

How to revoke a certificate

You can revoke certificates created using a Local Certificate Authority, OpenTrust, Entrust API Version 9, and Symantec Web Service PKI. Revoking a certificate adds the certificate to the CRL (Certificate Revocation List). When a device authenticates with Core, the system first checks the CRL to verify that the certificate is not on the list. If the certificate is on the list, authentication fails.

Procedure

1. Go to **Logs > Certificate Management**.
2. Select the certificate that you want to revoke.
3. Click **Actions > Revoke**.

The certificate will be added immediately to the CRL so the next time the device attempts to authenticate, authentication will fail.

How to re-enroll a SCEP certificate

Procedure

1. Go to **Logs & Events > Certificate Management**.
2. Select the certificate that you want to revoke.
3. Click **Actions > Re-enroll**.

Service Diagnostic tests

The Service Diagnostic screen (**Services > Overview)** in the Admin Portal provides a health check for several services. The diagnostic tests determine whether your Core instance can connect to these services. An error indicates that you cannot reach the service.

The services checked are:

TABLE 76. SERVICE DIAGNOSTIC TESTS DESCRIPTIONS

Service	Test
AFW	Checks to see if: • Authentication server https://accounts.google.com/o/oauth2/token is reachable. • API server https://www.googleapis.com/androidenterprise/v1/enterprises is reachable.
APNS	Checks to see if: • MDM-APNS service is reachable. • ENTERPRISE-APNS - No Enterprise APNS certificate configured. • MDM-APNS - feedback service (tccentos122.auto.mobileiron.com:2196) is not reachable.
APPCONFIG_ COMMUNITY_ REPO	Checks to see if the AppConfig Community Repository server is reachable: https://d2e3kgnhdeg083.cloudfront.net/com.example.OneTouchConfiguration/current/appconfig.xml
APP_GATEWAY	Checks to see if App Gateway server is reachable: https://gwtest.mobileiron.com/gateway/gatewayServices/status.html
BYPASS	Checks the connection between your Core instance and the Apple activation lock bypass server
CERTIFICATE ENROLLMENT	Checks to see if: • Certificate Enrollment : System - iOS Enrollment SCEP is reachable. • Certificate Enrollment : System - iOS Enterprise AppStore SCEP is reachable. • Certificate Enrollment : System - Windows Phone Enrollment SCEP is reachable.
CONFIGURATI ONS	Tests the connection to the Certificate Enrollment server from your Core instance.
CONNECTOR	Two tests are run:

TABLE 76. SERVICE DIAGNOSTIC TESTS DESCRIPTIONS (CONT.)

Service	Test
	• One test checks whether Enterprise Connector is enabled (**Services > Connector**) • If Enterprise Connector is enabled, the other test sends an HTTP Post request from your Core instance to each Connector configured, checking whether the Connector can communicate with your Core instance
DEP	Sends a sample GET request to test the connection between your Core instance and the MDM server using Device Enrollment.
FCM	Checks whether Google Firebase Cloud Messaging (FCM) is reachable from your Core instance.
HEALTH_ ATTESTATION_ SERVICE	Checks if the Health Attestation Service serveris reachable. https://has.spserv.microsoft.com/HealthAttestation/ValidateHealthCertificate/v1
LDAP	Two tests are run: • Checks LDAP from Core to verify the communication channel • For each Connector configured, checks the communication channel for the path from the LDAP server to Core, then Core to Connector, and finally from Connector to the LDAP server
MAPQUEST	Checks if the MapQuest Service server is reachable: https://api.mqcdn.com/sdk/mapquest-js/v1.0.0/mapquest.js
PROXY	No proxy is configured.
SENTRY	Checks the connection between your Core instance and the Sentry used (either integrated standalone). As part of this test, the connection between ActiveSync server and Sentry is checked also.
SENTRY_ WITH_ ACTIVESYNC	No Integrated Sentry server(s) configured. No Standalone Sentry server(s) configured.
SERVICES	Checks whether the IP addresses reserved for FCM are reachable.
VPP	Sends a GET request to verify the connection between Core and the Apple License server.

Running Service Diagnostic tests

Procedure

1. Go to **Services > Overview**.
2. To test one or all of the services:
   - Click **Verify All** to test the listed services
   - Click **Verify** next to a specific service to test that service

Language Support

This section addresses the language settings for Mobile@Work. For the current list of supported languages, see the *Core and Connector Release and Upgrade Notes*.

- "Translated versions of client apps" below
- "Selecting languages for Core messages" below
- "Setting the system default language " on the next page
- "Changing language selection from the Admin Portal" on the next page

Translated versions of client apps

Ivanticlient apps (Mobile@Work or Apps@Work on Windows) are localized to a number of languages. A device's locale setting (or selected language) determines the language that the client app appears in on the device. If the device's locale is not supported, the app appears in English (United States) by default.

Once the device communicates a language change to Core, Core sends messages to the device in the selected language, assuming the language is supported and selected in Core's **Settings > System Settings > General > Language**.

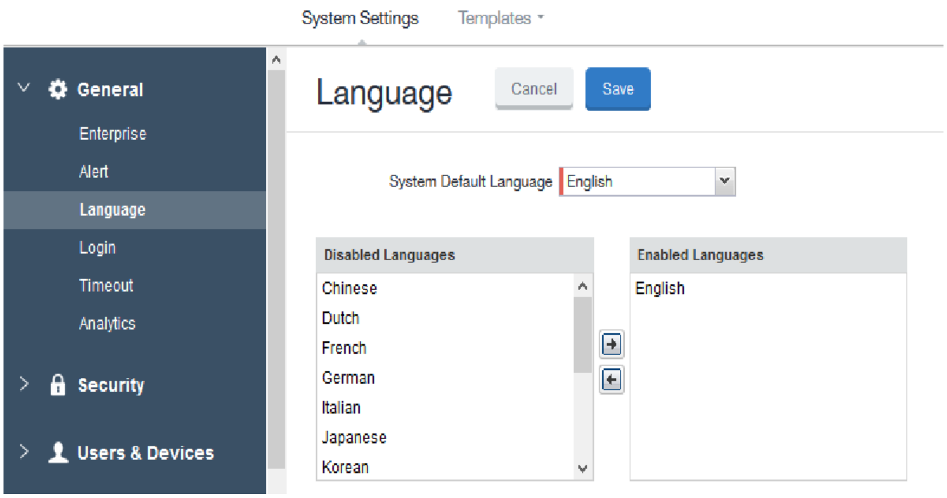
Please refer to the Core release notes for each release to see which languages and locales are supported.

Selecting languages for Core messages

You can enable or disable languages for the messages sent from Core to devices. For example, if you have only Japanese-speaking users, you might want to remove the other message templates from the Admin Portal.

To enable or disable languages:

1. Log into the System Manager.
2. Go to **Settings > System Settings > General > Language**.



Language

System Default Language: English

Disabled Languages	Enabled Languages
Chinese	English
Dutch	
French	
German	
Italian	
Japanese	
Korean	

3. Move the languages you want to support from **Disabled Languages** to **Enabled Languages**.
4. Click **Save**.

Setting the system default language

The **System Default Language** setting under **Settings > System Settings > General > Language** determines what language to use if the locale of the device cannot be determined, or the corresponding language is not supported. It also determines the default language for the self-support user portal (SSP) pages. The languages available for this setting are derived from the languages in the **Enabled Languages** list.

Changing language selection from the Admin Portal

Administrators can manually change the language selection for devices that do not report their locale. In this case, language selection applies only to the messages sent from Core (e.g., Event Center alerts). If the device later reports a different locale, then Core honors the reported locale.

To change the language selection for a specific device:

1. In the Admin Portal, go to **Devices & Users > Devices**.
2. Select the check box next to the device.

3. Click **Actions > Change Language**.

   The **Change Language** dialog appears.

4. From the **Set Language** drop-down, select the preferred language.

5. Click **Change Language**.

Self-service User Portal

This section addresses device registration and its related components.

User portal overview

The Core Mobile@Work self-service user portal (SSP) is a platform whereby device users can manage their own devices. This section addresses the settings an administrator can create and maintain a self-service user portal.

- "Benefits of the user portal" on page 432
- "Impacts of using the user portal" on page 432
- "User portal authentication options" on page 432
- "About registering devices in the user portal" on page 433
- "About changing device ownership in the user portal" on page 434
- "Associating a certificate with a user-provided certificate enrollment setting" on page 435

The user portal allows your users to:

- Access Core device management actions such as wipe and lock
- View their device audit/history logs

- View details of their registered devices
- Register devices, including QR code and SMS/email options
- Reset the user PIN
- Reset a PIN password
- Change device ownership from company-owned to user-owned or the reverse
- Upload, as well as view, replace, and delete user-provided certificates

  These certificates are used, for example, for S/MIME or for authenticating to internal servers.
- Designate their device as "Untrusted" in risky public spaces and redesignate them as "Trusted" when in a safe area again.

One of your decisions when you distribute Core management is whether or not to enable your users to manage one or more device actions such as locking or unlocking a device. Your users access the actions you assign them through the user portal.

To enable users to manage their devices, you assign them roles to perform any or all of the following actions:

- Wipe their device
- Lock their device
- Locate their device
- Retire their device
- Register their device
- Change device ownership
- Reset PIN Password (for Windows 8.1 Phone and Windows Mobile 10 devices)

The **Trust** and **unTrust** options do not require a role. Registered devices are Trusted devices by default.

The **Device Registration** role replaces the **MyPhone@Work Registration** role. The **MyPhone@Work Registration** role is removed. The old user portal, MyPhone@Work, was available only through Core 8.0.1.

Benefits of the user portal

Giving users the ability to perform device management tasks:

- Distributes mobile device management
- Gives your users more control of their devices
- Adds efficiency to device registration by saving administrators' time as well as wait time that device users might experience

Impacts of using the user portal

When you enable users to manage their own devices, you need to:

- Define which users have access to which device management actions
- Provide your users with the information they need to use the user portal
- Consider how changing device ownership from company-owned to employee-owned or vice-versa may impact:
  - 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.

    Devices are impacted when they check-in with Core depending on the labels to which company-owned or employee-owned devices are applied.

User portal authentication options

You can allow device users to authenticate to the user portal with:

- A user name and password

  These are the credentials a device user uses to register a device with Core.

- An identity certificate from a smart card

  This authentication method is supported only on desktop computers. It is not supported with:

  - Mobile devices
  - Firefox

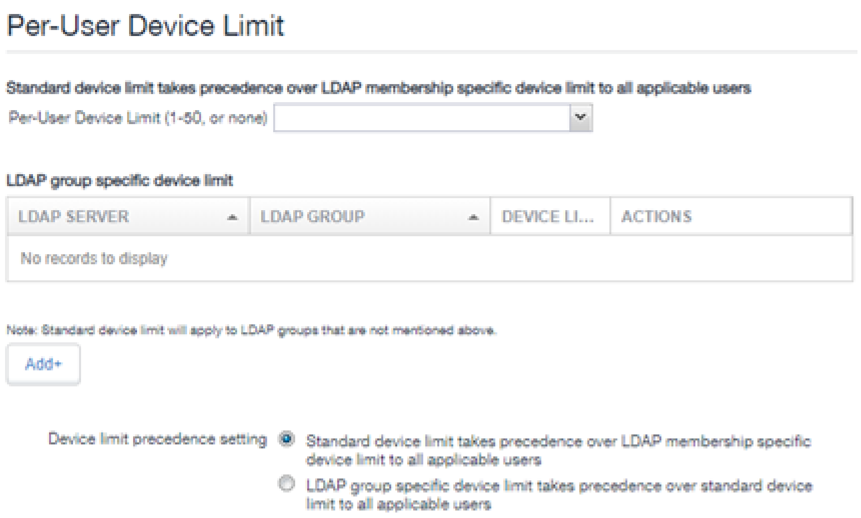
You can allow one or both of these authentication mechanisms. You make your selection in the *Core System Manager GuideCore System Manager Guide*. For information about how to configure the user portal authentication options, see “Advanced: Portal authentication” in the *Core System Manager Guide*.

About registering devices in the user portal

To allow device users to register devices in the user portal, you must assign those users the **Device Registration** role in the Admin Portal in **Devices & Users > Users**.

Configuring the Per-User Device limit

You can configure a global per-user device limit, and optionally, custom device limits for specific LDAP Groups. Users will be limited to register only the number of devices specified in **Settings > System Settings > Users & Devices > Registration > Per-User Device Limit.**



Per-User Device Limit

Standard device limit takes precedence over LDAP membership specific device limit to all applicable users

Per-User Device Limit (1-50, or none)

LDAP group specific device limit

LDAP SERVER	LDAP GROUP	DEVICE LI...	ACTIONS
No records to display			

Note: Standard device limit will apply to LDAP groups that are not mentioned above.

Add+

Device limit precedence setting
● Standard device limit takes precedence over LDAP membership specific device limit to all applicable users
○ LDAP group specific device limit takes precedence over standard device limit to all applicable users

Procedure

To configure standard device limits and LDAP group-specific device limits, follow these steps:

1. In the first drop-down menu, select a default per-user device limit of **1-50**, or **none**.
2. If you would like to create different per-user device limits for selected LDAP groups, click **Add+**. The **Add LDAP Group Specific Device Limit** menu opens.
3. From the **Select LDAP Server** drop-down menu, select the LDAP server that contains the LDAP group you want to include.
4. From the **Select LDAP Group** drop-down menu, select the Group to include.
5. From the **Select Device Limit Per User** drop-down menu, select the per-user device limit for that LDAP group.
6. Click **Add** to save your changes.
7. The LDAP group you selected appears in the LDAP group specific device limit table, where you can copy, edit, or delete it.

Registration PIN

Users who can register devices can also request and receive device registration PINs. To allow users to request a registration PIN, PIN-based registration must be selected in **Settings > System Settings > Users & Devices > Device Registration**. Any option that includes Registration PIN will enable device users to obtain a PIN in the user portal.

- Even though a PIN is generated, device users will not be prompted to enter a PIN if the device platform does not require PIN for registration.

About changing device ownership in the user portal

To allow device users to change device ownership through the user portal, you must assign those users the **Change Device Ownership** role in the Admin Portal in **Devices & Users > Users**.

Users cannot assign ownership of a device during device registration in the user portal. Device ownership is automatically set to company-owned. Once users have registered their devices through the user portal, they can change the ownership of the device from company-owned to user-owned or the reverse.

Associating a certificate with a user-provided certificate enrollment setting

When the user uploads a certificate, the user chooses a configuration to associate with the certificate. The configuration refers to a user-provided certificate enrollment setting that you configured. When you configure a user-provided certificate enrollment setting, you specify a display name. The user portal presents the display name in its list of configurations for the user to choose.

For example, you might create a user-provided certificate enrollment setting for S/MIME signing, another for S/MIME encryption, and another for server authentication. Each setting has a display name:

- S/MIME signing
- S/MIME encryption
- Authentication

When the user uploads a certificate, they see these display names as configurations, and they choose the one for the certificate. The user can upload the same certificate or different certificates for each configuration.

If you have not created at least one user-provided certificate enrollment setting, the user portal disables the option for the user to upload a certificate.

See also:

- "Certificate Enrollment settings" on page 297

About uploading certificates in the user portal

On a desktop computer, device users can upload their own certificates in the user portal. They can use these certificates for different purposes, such as:

- S/MIME signing
- S/MIME encryption
- Authenticating to servers, such as internal servers that support apps.

From Core release 10.8.0.0 or supported newer versions, users can upload files with multiple aliases and friendly names.

This capability is available in the user portal on desktop computers, but not on mobile devices.

Device management with the user portal

This section addresses the settings your users need to use the user portal.

- "Logging in to the user portal with user name and password" on page 451
- "Logging in to the user portal on a desktop computer with a certificate" on page 451
- "What users see after they login" on page 452
- "Uploading certificates in the user portal on a desktop computer" on page 459
- "Viewing, replacing, and deleting certificates in the user portal" on page 460
- "When a user-provided certificate is deleted" on page 460

Assigning user portal device management roles

The Core user portal provides several device management options for your users. You give them access to these management tasks by assigning them roles in the Admin Portal.

- The **Trust** and **unTrust** options do not require a role. Registered devices are Trusted devices by default.

Procedure

1. In Admin Portal, go to **Devices & Users**.
2. Select the users receiving device management privileges.
3. From **Actions**, select **Assign Roles**.
4. Check **User Portal**.
5. Check one or more roles to assign the corresponding management actions to the selected users.
6. User roles include:
   - Wipe Device
   - Lock Device
   - Unlock Device (See following Note)

- Locate Device
- Retire Device
- Register Device
- Change Device Ownership
- Reset PIN
- Reset Secure Apps Passcode
- Use Google Device Account (for Android Enterprise devices only)
- Enable Auth Only Role

ⓘ The unlock feature works with Managed Device with Work Profile (COPE) mode (Android versions 8-10.) Upon upgrade to Android 11, administrators do not have the ability to unlock the device.

ⓘ Unlock devices does not work for Work Profile devices starting from Android 7 and higher.

7. Click **Save**.

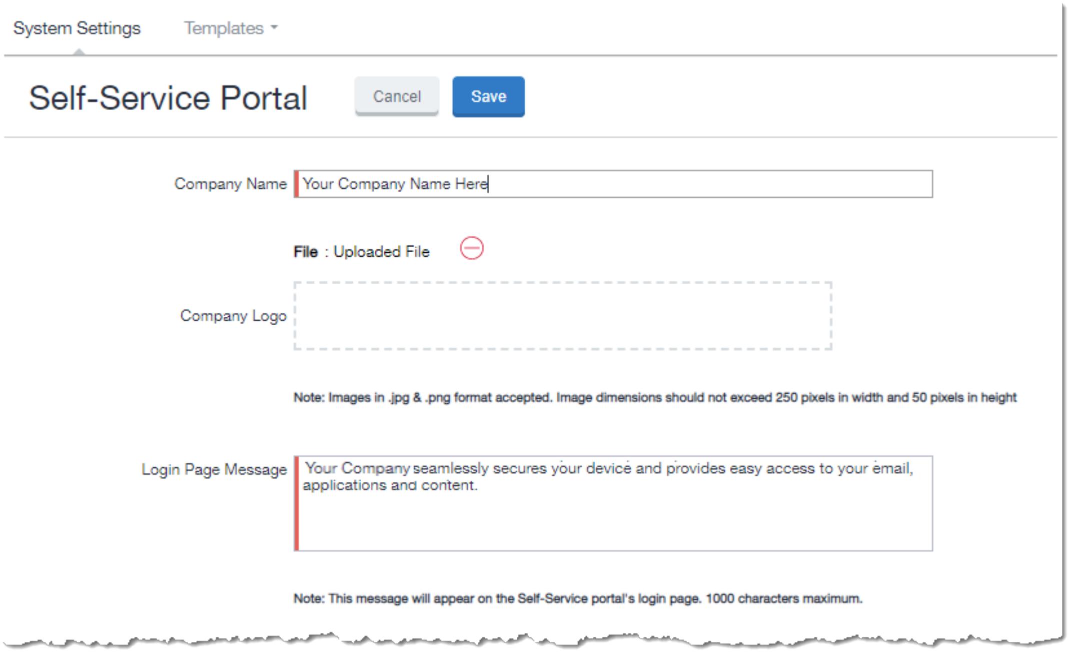
Customizing the self-service user portal

The self-service user portal can easily be customized to reflect your company branding, messaging, and layout. The following elements can be customized:

- Company name
- Company logo
- Login page message
- Background color
- Cascading stylesheet (CSS)

Procedure

1. From the Admin portal, navigate to **Settings > System Settings > General > Self-Service Portal**. The Self-Service Portal page opens.



Company Name: Your Company Name Here

File : Uploaded File

Note: Images in .jpg & .png format accepted. Image dimensions should not exceed 250 pixels in width and 50 pixels in height

Login Page Message: Your Company seamlessly secures your device and provides easy access to your email, applications and content.

Note: This message will appear on the Self-Service portal's login page. 1000 characters maximum.

2. **Company Name**: Enter a customized company name.

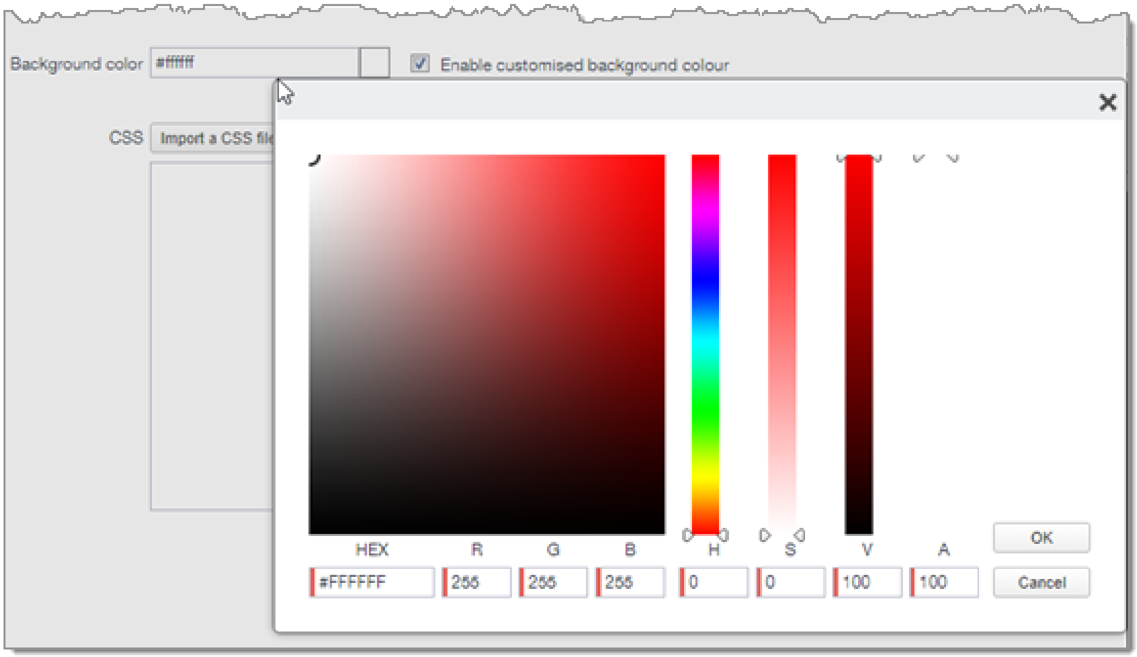
3. **Company Logo**: Upload a customized company logo. Images can be JPG or PNG format, and must not exceed 250 by 50 pixels.

4. **Login Page Message**: Modify or replace the existing message that displays on the Self-Service Portal's log in page, up to 1,000 characters.

5. **Background color**:

a. Check **Enable customized background color** and either:

- Type in a HEX color value, or
- Open the **Background color** menu.



Background color #ffffff

☑ Enable customised background colour

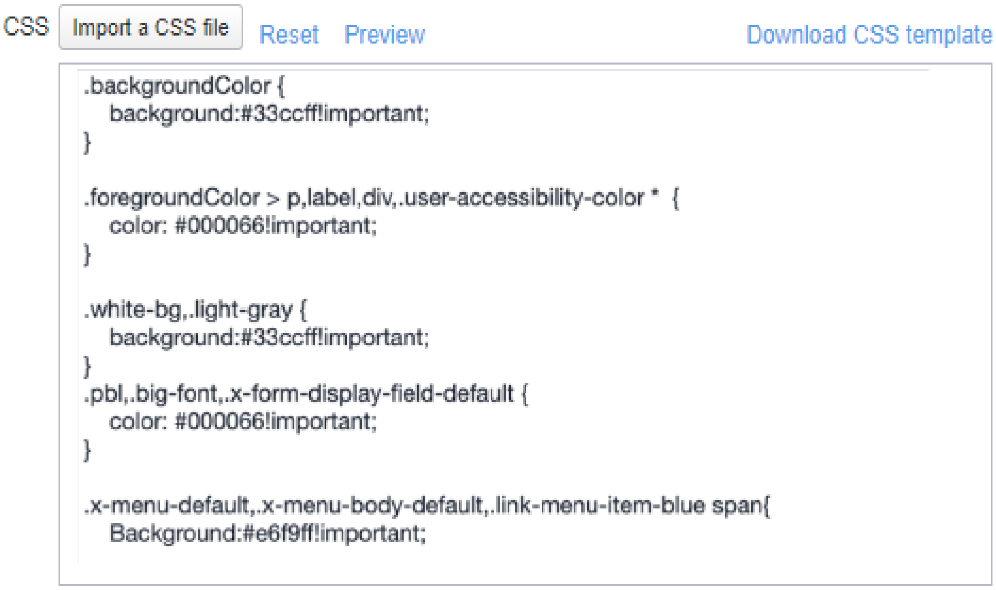
HEX	R	G	B	H	S	V	A
#FFFFFF	255	255	255	0	0	100	100

b. Select or enter a value for the background color.

Based on your choice of background color, Core will automatically determine the highest-contrast text color (black or white) for that color.

c. Click **OK** to exit the menu.

6. **CSS**: By default, your message is formatted using the default cascading style sheet (CSS) supplied by Core. You can import and edit a custom CSS file, modify the default CSS file, or leave the default.



```
.backgroundColor {
   background:#33ccff!important;
}

.foregroundColor > p,label,div,.user-accessibility-color *  {
   color: #000066!important;
}

.white-bg,.light-gray {
   background:#33ccff!important;
}
.pbl,.big-font,.x-form-display-field-default {
   color: #000066!important;
}

.x-menu-default,.x-menu-body-default,.link-menu-item-blue span{
   Background:#e6f9ff!important;
```

Options are:

- **Import a CSS file**: Click to browse to a valid CSS file on your local drive. Select the file and click **Open**. The CSS file opens in the edit window. You will be asked to confirm the change.

  Invalid CSS files will not be imported, and an error message will display.

- **Reset**: Click to reset the style sheet to the default values. You will be asked to confirm the reset.

- **Preview**: Click to see a preview of your message as users will see it.

- **Download**: Downloads a copy of the default CSS file to your browser's Download folder for you to keep and modify. Alternately, you can copy and paste the default CSS file into the **CSS** text window.

7. **Show View Activity in SSP Portal**: This option is enabled by default, and allows your device users to see their activity logs from the View Activity page in the SSP. To hide activity logs on the SSP, see "Disabling device history logs in the self-service user portal" on page 443.

8. When all of your changes are made, click **Save** (at the top of the page) to keep your options. A confirmation message displays.

9. Verify the new custom portal page on Core by substituting your Core hostname and SSP user name:

   https://<*hostname*>/mifs/<*user*>

User portal default stylesheet

You can copy-and-paste the following default stylesheet into the CSS text window and modify it for your needs.

```
.backgroundColor {
background:#33ccff!important;
}
.foregroundColor > p,label,div,.user-accessibility-color *  {
color: #000066!important;
}
.white-bg,.light-gray {
background:#33ccff!important;
}
.pbl,.big-font,.x-form-display-field-default {
color: #000066!important;
}
.x-menu-default,.x-menu-body-default,.link-menu-item-blue span{
Background:#e6f9ff!important;
}
.btn-new-color,.x-btn-accessblue-medium {
background:#000066!important
}
.link-menu-item-blue span {
line-height: 16px;
font-size: 14px;
font-family: Helvetica,Arial,sans-serif;
margin-left: 5px;
color: #2d70b5;
}
.x-menu-item-text-default {
font: normal 11px helvetica,arial,sans-serif;
line-height: 21px;
padding-top: 1px;
color: #222;
cursor: pointer;
}
.x-btn-inner-accesswhite-medium {
font: normal 12px/24px arial,verdana,sans-serif;
color: #2d70b5;
padding: 0 10px;
max-width: 100%;
}
.x-btn-inner {
display: inline-block;
vertical-align: middle;
overflow: hidden;
text-overflow: ellipsis;
}
.x-autocontainer-innerCt {
display: table-cell;
height: 100%;
vertical-align: top;
}
.x-autocontainer-outerCt {
display: table;
}
.x-grid-empty {
padding: 10px;
color: gray;
background-color: white;
font: normal 12px helvetica,arial,sans-serif;
}
.x-grid-header-ct {
background-color: #edf0f2;
}
.x-grid-header-ct {
border: 1px solid #d0d0d0;
border-bottom-color: #a0a7ad;
background-color: #a0a7ad;
}
.x-column-header-inner {
padding: 8px 8px 6px 8px;
}
.x-leaf-column-header {
height: 100%;
}
```

```
.x-column-header-inner {
white-space: nowrap;
position: relative;
overflow: hidden;
}
.x-column-header-text {
background-repeat: no-repeat;
display: block;
overflow: hidden;
text-overflow: ellipsis;
white-space: nowrap;
}
.x-grid-item-container {
min-height: 1px;
position: relative;
}
.x-panel-default {
border-color: #d0d0d0;
padding: 0;
}
```

Disabling device history logs in the self-service user portal

When users log into the Ivanti self-service portal (SSP), they can view their activity log by default. If your organization prefers not to show users the View Activity page, an administrator can disable the feature from the **Self-Service Portal** page of the Core Admin portal.

Procedure

1. Go to **Settings** > **System Settings** > **General** > **Self-Service Portal** page, and scroll to the bottom.
2. Deselect **Show View Activity in SSP Portal** by clicking it.
3. Click **Save**.

Related topics

To disable the QR code and authentication URL for device registration, see "Disabling the QR code and registration URL" on page 30.

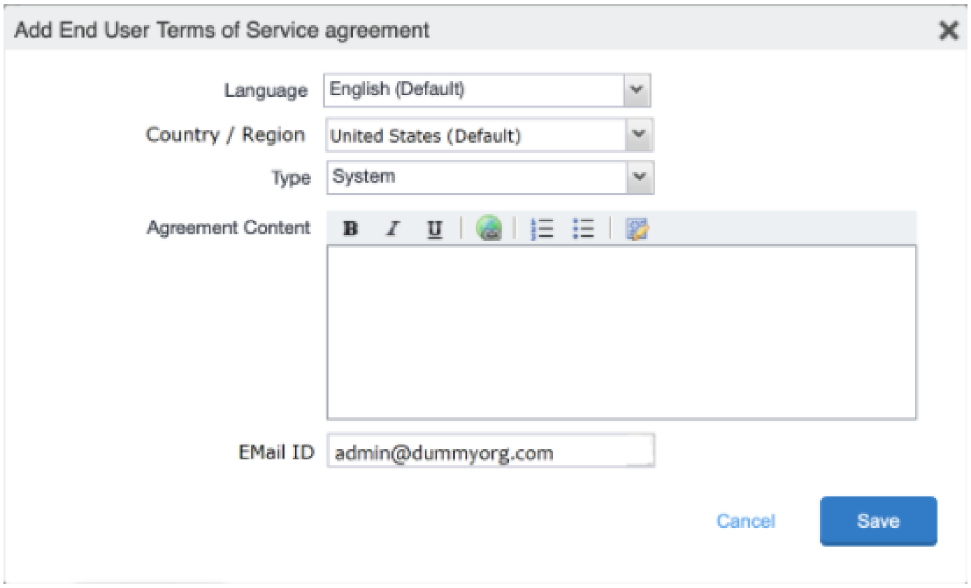
Configuring an end user Terms of Service agreement

Device users must sign a Terms of Service (ToS) agreement to use Mobile@Work. You can create custom ToS agreements to align with your user languages and countries. When a user accepts the agreement, an audit email is automatically sent to the admin user identified in the **EMail ID** field.

Procedure

1. From the Admin portal, navigate to **Settings >System Settings > Users & Devices > Registration page > End User Terms of Service**.

2. Click **Add+**. The **Add End User Terms of Service agreement** window opens.



Add End User Terms of Service agreement

Language: English (Default)

Country / Region: United States (Default)

Type: System

Agreement Content:

EMail ID: admin@dummyorg.com

3. In the **Language** drop-down, select the language for the agreement.

4. In the **Country / Region** drop-down, select the primary country or region.

5. In the **Type** drop-down, select the type of agreement:

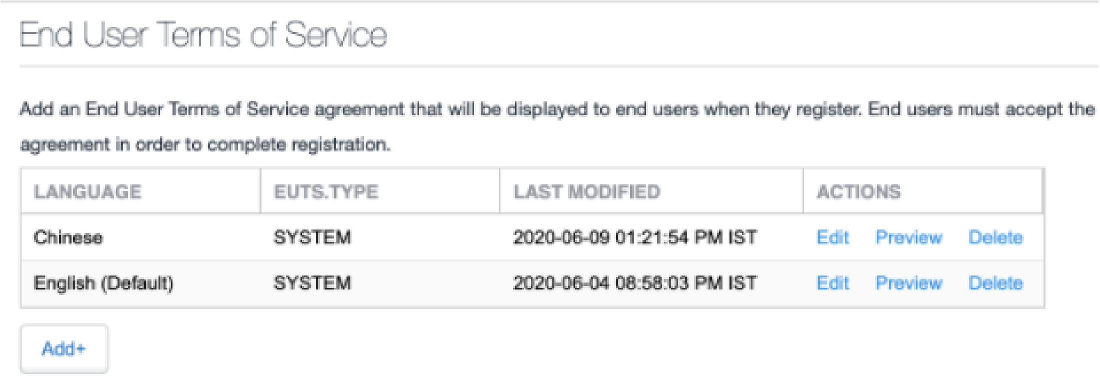
   a. **System** - Select for iOS, macOS and Android devices.

   b. **AAD enrollment** - Select for Windows devices.

6. In the **Agreement Content** text box, enter your agreement text. The text field permits basic formatting.

7. In the **EMail ID** field, enter an email address to receive confirmation emails when the users accept the agreement.

8. Click **Save**. Your new agreement appears in the End User Terms of Service table.



End User Terms of Service

Add an End User Terms of Service agreement that will be displayed to end users when they register. End users must accept the agreement in order to complete registration.

LANGUAGE	EUTS.TYPE	LAST MODIFIED	ACTIONS
Chinese	SYSTEM	2020-06-09 01:21:54 PM IST	Edit Preview Delete
English (Default)	SYSTEM	2020-06-04 08:58:03 PM IST	Edit Preview Delete

Admin notification email

The notification email consists of a message and identifying client information: "The following user has accepted device registration terms and has attempted to enroll a new device:"

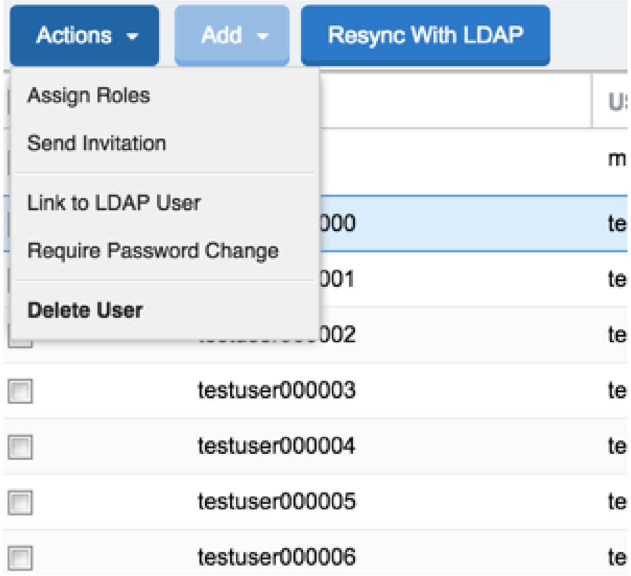
- User name
- Display name
- Email address
- Date and time
- IP address
- Platform
- Employee owned (true/false)

Requiring user portal password change

You can require local users to change their user portal password the next time the device checks in with Core. This feature is not available for LDAP users.

To require a local user to change their user portal password:

1. In Admin Portal, go to **Devices & Users**.
2. Click **Users**.
3. Select one or more local users you want to change their user portal passwords the next time they check in with Core.
4. Click **Actions**.



5. Select **Require Password Change**.

   Core prompts you to confirm the requirement.

6. Click **Yes** to require the selected users to create a new password at the next check in.

Limiting devices per user by LDAP group membership

You can limit the number of allowed devices per user, using LDAP group membership as the conditional limiter. You can:

- Select a global device limit of 0-50 devices per user
- Add LDAP user groups to the LDAP group-specific device limit table
- Edit LDAP user groups

- Delete LDAP user groups from the device limit table
- Set the device limit precedence setting: you can choose whether the standard device limit takes precedence over LDAP membership-specific device limits, or LDAP group-specific device limits take precedence over the standard device limit (for all applicable users)

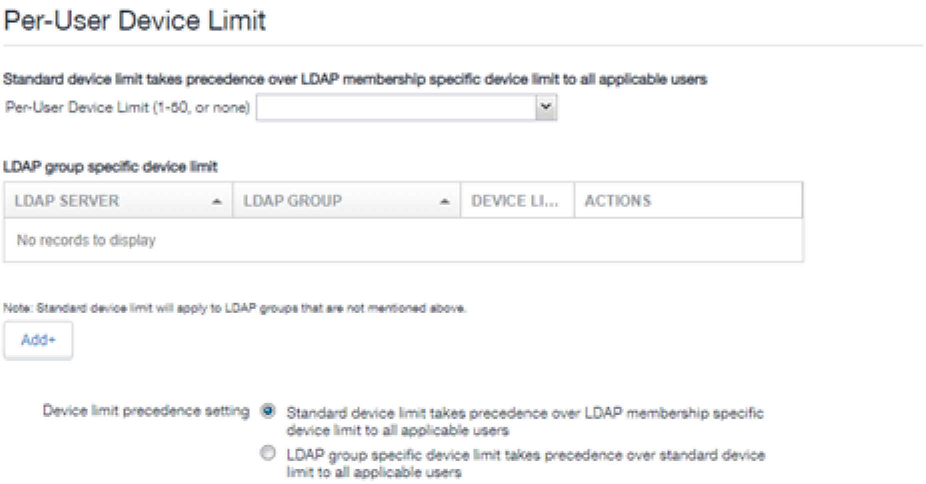
  For example, you could set a global device limit of four devices, but restrict members of specific LDAP groups to one or two devices.

Before you begin

You must have previously configured an LDAP server to support LDAP groups before you can set per-user device limits.

Procedure

1. From the Admin Portal, go to **Settings** > **System Settings** > **Users & Devices** > **Registration** page
2. In the **Per-User Device Limit** section, enter the following information:



Per-User Device Limit

Standard device limit takes precedence over LDAP membership specific device limit to all applicable users

Per-User Device Limit (1-50, or none)

LDAP group specific device limit

LDAP SERVER	LDAP GROUP	DEVICE LI...	ACTIONS
No records to display			

Note: Standard device limit will apply to LDAP groups that are not mentioned above.

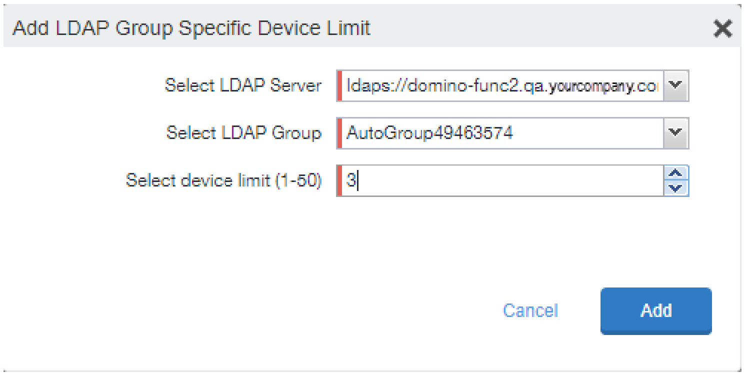
Add+

Device limit precedence setting
● Standard device limit takes precedence over LDAP membership specific device limit to all applicable users
○ LDAP group specific device limit takes precedence over standard device limit to all applicable users

3. **Per-User Device Limit (1-50, or none)**: Set the default number of devices each user can register with Core. This is the "standard" device limit, that by default takes precedence over LDAP membership-specific device limits.You can change this priority by selecting a device limit precedence setting (step 5).

4. **LDAP group specific device limit**: This setting allows you to create LDAP group-specific device limits that vary from the default device limit you set as the per-user device limit.

    a. From below the LDAP group table, click **Add+**. The Add LDAP Group Specific Device Limit dialog opens.

    Add LDAP Group Specific Device Limit

    Select LDAP Server: ldaps://domino-func2.qa.yourcompany.co

    Select LDAP Group: AutoGroup49463574

    Select device limit (1-50): 3

    b. Select a configurable LDAP server from the **Select LDAP Server** drop-down.

    c. Select a group from the **LDAP Group** drop-down.

    d. Select the device limit (1-50) from the **Select device limit** field.

    e. Click **Add**.

5. Select a device limit precedence setting:

    a. Standard device limit takes precedence over LDAP membership-specific device limit for all applicable users.

    b. LDAP group-specific device limit takes precedence over standard device limit for all applicable users.

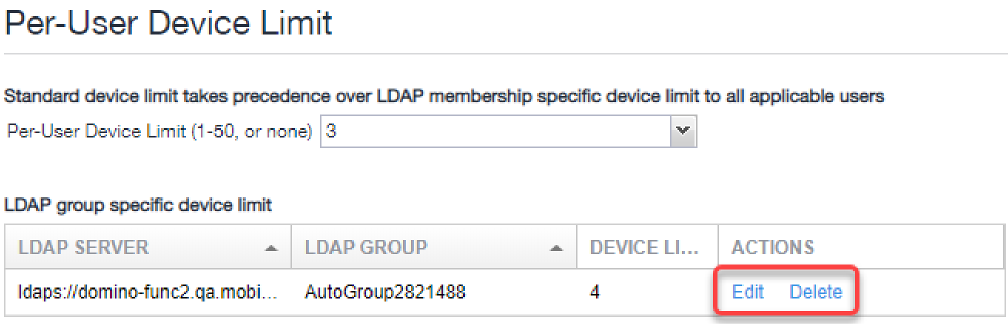
6. Click **Add** to save your changes.

Editing or Deleting an LDAP group-specific device limit

You can modify or delete your LDAP group-specific device limits from the LDAP group-specific device limit table.

Procedure

1. Locate the LDAP group that you want to edit or delete in the LDAP group-specific device limit table.



Per-User Device Limit

Standard device limit takes precedence over LDAP membership specific device limit to all applicable users

Per-User Device Limit (1-50, or none): 3

LDAP group specific device limit

LDAP SERVER	LDAP GROUP	DEVICE LI...	ACTIONS
ldaps://domino-func2.qa.mobi...	AutoGroup2821488	4	Edit Delete

2. Click **Edit** to re-open the Add LDAP Group Specific Device Limit dialog.
3. Click **Delete** to delete the LDAP group-specific device limit.

Configuring help desk contact information

Core administrators with **Manage settings and services** permission can configure the help desk contact information to display in the self-service user portal.

Procedure

1. In the Core Admin Portal, go to **Settings** > **General** > **Helpdesk**.
2. Enter the following information:

Item	Description
Name	Enter a name for the configuration.
Description	Enter a brief description for the configuration. Maximum characters allowed is 100.

Item	Description
Contact(s)	Enter one or more phone numbers. Valid number strings include: • Up to 24 digits for numbers beginning with the + symbol. • Up to 22 digits for numbers without the + symbol. If you are entering multiple phone numbers, enter a comma-separated list.
Email(s)	Enter one or more email addresses. If you are entering multiple email addresses, enter a comma-separated list.

Either a phone number or an email address is required.

Related topics

"Viewing the help desk contact information" on page 461.

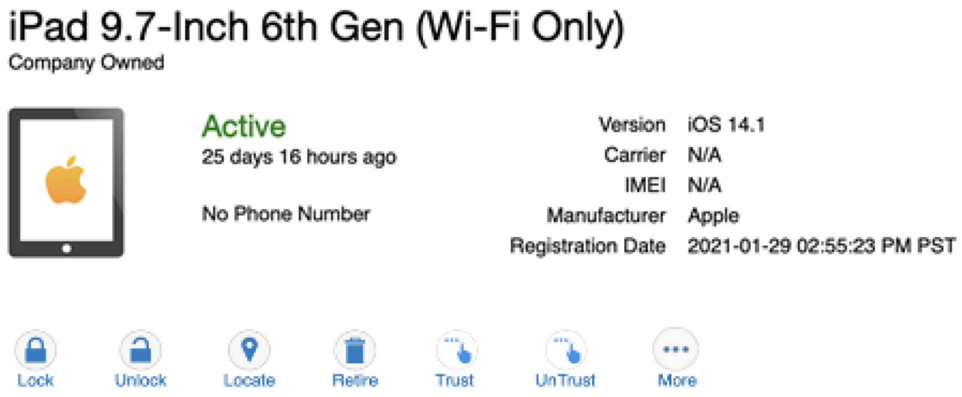
User portal information for your users

This section presents the information that your users need to use the user portal.

The user portal displays:

- Icons for each device management action the user is allowed to perform.
- User and device information, including:
  - device type (iPod touch, 4th gen in the example)
  - status (Active, for example)
  - last check-in (example, 2 hours ago)
  - phone number
  - OS and version (to 3 digits, iOS 7.1.1, for example)
  - carrier (for example, AT&T)
  - IMEI value, if applicable
  - manufacturer
  - date the device was registered with Core
- Accounts settings and certificates uploaded by the device user.
- Helpdesk contact information configured by the Core administrator.

Figure 1. User portal showing user's device information



iPad 9.7-Inch 6th Gen (Wi-Fi Only)
Company Owned

Active
25 days 16 hours ago

No Phone Number

Version	iOS 14.1
Carrier	N/A
IMEI	N/A
Manufacturer	Apple
Registration Date	2021-01-29 02:55:23 PM PST

Logging in to the user portal with user name and password

Device users can log in to the user portal to register and manage their devices.

Procedure

1. Go to https://<*MobileIron server*>, where <*MobileIron server*> is the address of your MobileIron server.

   Contact your administrator if you do not have this address.

2. If you are not logged in, provide your user name and password, when prompted, and then select **Sign In with Password**.

   The user portal displays on your device. You can:

   - click the icon for one of the available device management actions available to you.
   - view your device information.

Logging in to the user portal on a desktop computer with a certificate

If set up by the Core administrator, device users can log in to the user portal on a desktop computer using an identity certificate on a smart card.

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 https://<*MobileIron server*>, where <*MobileIron server*> is the address of your Core server.

   Contact your administrator if you do not have this address.

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 user portal displays. You can:

   - Select the icon for one of the available device management actions available to you.
   - View your device information.

What users see after they login

Depending on the user portal role enabled, device users may have a different view of the user portal.

Welcome menu

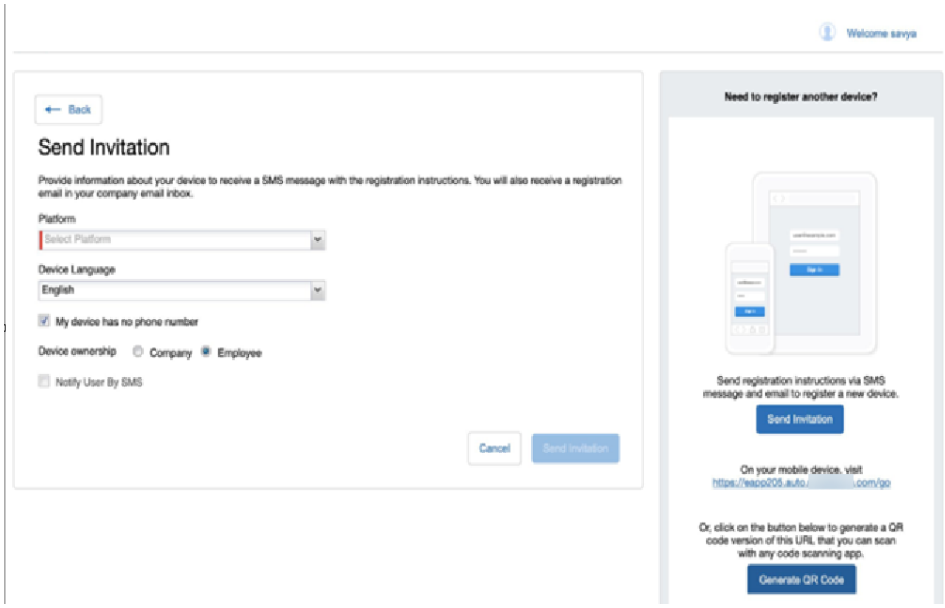
The Welcome menu is in the top-right of the user portal. From this menu, you can perform the following actions:

- **View Activity** - See a list of all device activity. See "Viewing device history logs from the self-service user portal" on page 461.
- **Helpdesk** - Configure the help desk contact information to display in the user portal. See "Configuring help desk contact information" on page 449.
- **Settings** - View user portal settings.
- **Sign Out** - Sign out of the self-service user portal.

If Register Device role is enabled

If the **Register Device** role is enabled, device users will be able to send an invitation from the user portal to register their device.

FIGURE 2. SEND INVITATION TO REGISTER



Welcome savya

Send Invitation

Provide information about your device to receive a SMS message with the registration instructions. You will also receive a registration email in your company email inbox.

Platform: Select Platform

Device Language: English

☑ My device has no phone number

Device ownership ○ Company ● Employee

□ Notify User By SMS

Need to register another device?

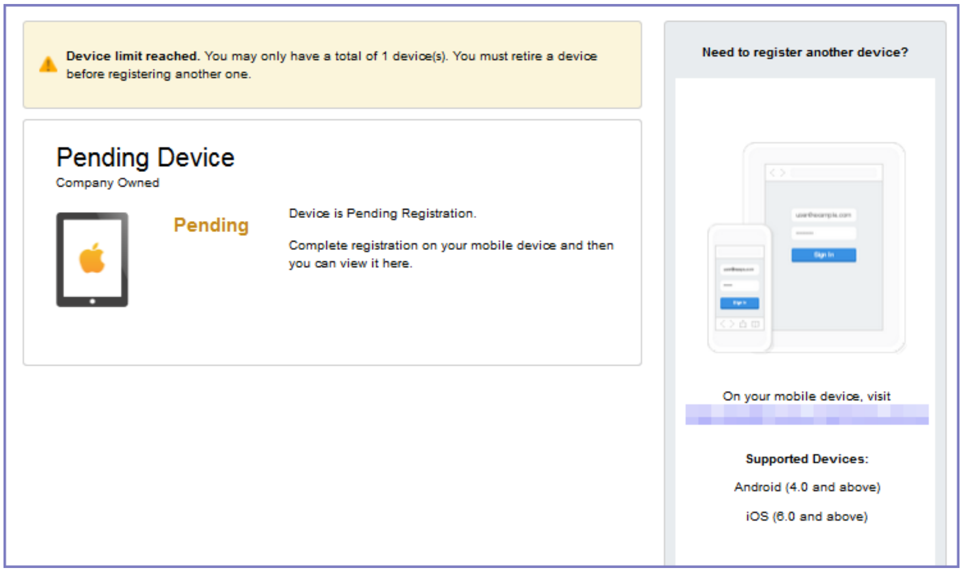
Send registration instructions via SMS message and email to register a new device.

On your mobile device, visit https://eapp205.auto.[redacted].com/go

Or, click on the button below to generate a QR code version of this URL that you can scan with any code scanning app.

After the invitation is sent, the device status is seen as **Pending**.

FIGURE 3. REGISTRATION PENDING FOR DEVICE



Device limit reached. You may only have a total of 1 device(s). You must retire a device before registering another one.

Pending Device

Company Owned

Pending

Device is Pending Registration.

Complete registration on your mobile device and then you can view it here.

Need to register another device?

On your mobile device, visit

[redacted]

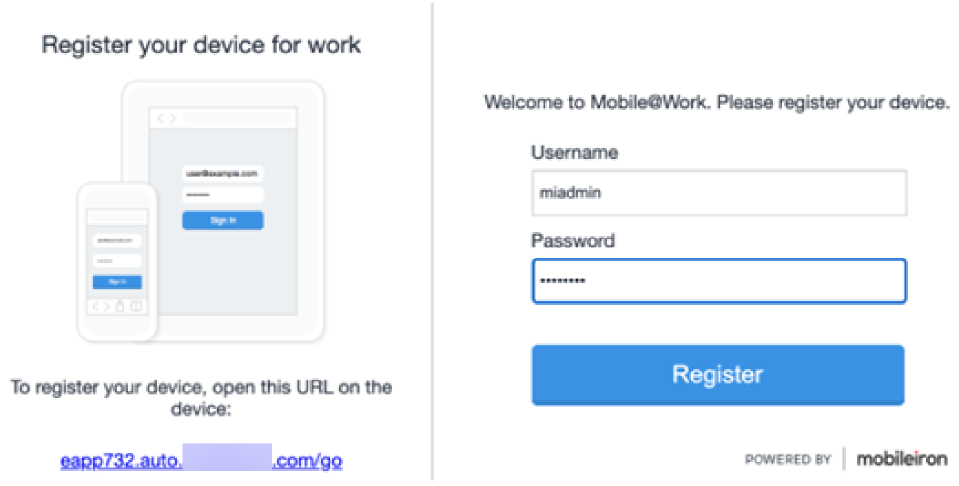
Supported Devices:

Android (4.0 and above)

iOS (6.0 and above)

Device users can complete the registration on their mobile device at https://<*Core_Server_FQDN*>/go.

FIGURE 4. COMPLETE DEVICE REGISTRATION



Register your device for work

To register your device, open this URL on the device:

eapp732.auto.[redacted].com/go

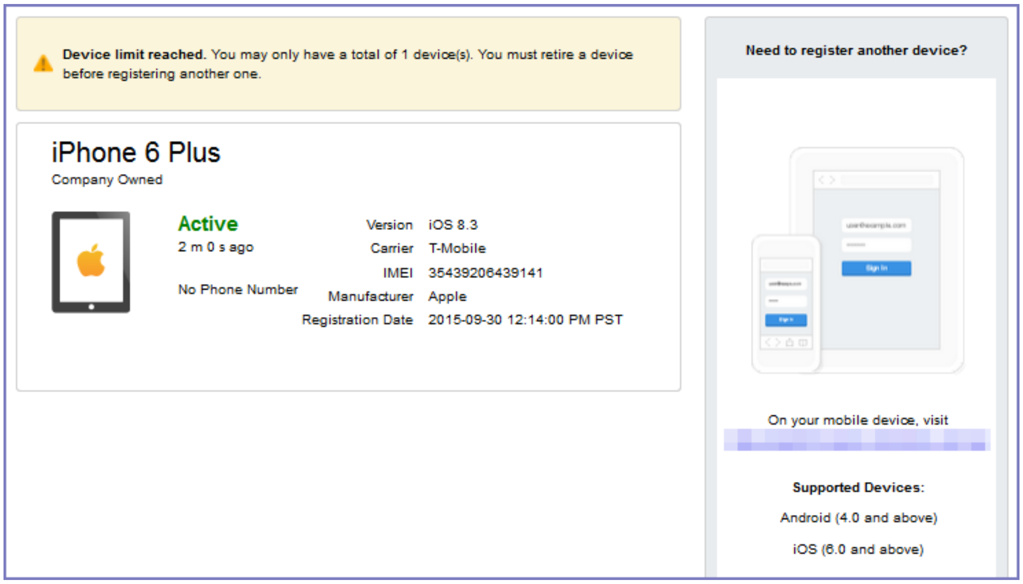
Welcome to Mobile@Work. Please register your device.

Username: miadmin

Password: *********

After registration is completed on the mobile device, the status for the device is changed to **Active**.

FIGURE 5. ACTIVE DEVICE STATUS



Device limit reached. You may only have a total of 1 device(s). You must retire a device before registering another one.

iPhone 6 Plus

Company Owned

Active

2 m 0 s ago

No Phone Number

Version	iOS 8.3
Carrier	T-Mobile
IMEI	35439206439141
Manufacturer	Apple
Registration Date	2015-09-30 12:14:00 PM PST

Need to register another device?

On your mobile device, visit

[redacted]

Supported Devices:

Android (4.0 and above)

iOS (6.0 and above)

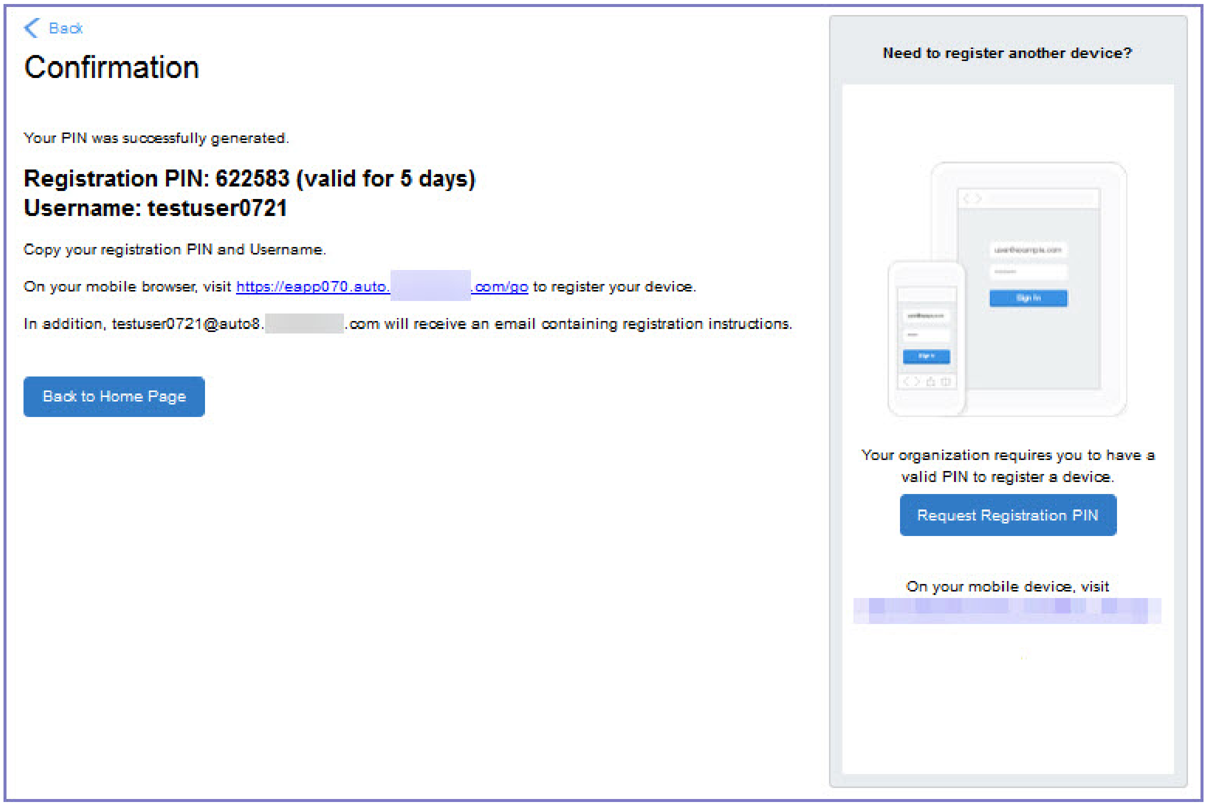
Registration instructions

For Windows devices, users can follow the instructions provided in the user portal and in the email sent to the device user to register the device with Core.

If PIN-based registration is enabled

If PIN-based registration is enabled, device users will see **Request Registration PIN**. Clicking on **Request Registration PIN** allows device users to send an invitation for registration as well as generate a PIN.

FIGURE 6. REGISTRATION WITH PIN



Confirmation

Your PIN was successfully generated.

Registration PIN: 622583 (valid for 5 days)
Username: testuser0721

Copy your registration PIN and Username.

On your mobile browser, visit https://eapp070.auto.[redacted].com/go to register your device.

In addition, testuser0721@auto8.[redacted].com will receive an email containing registration instructions.

Need to register another device?

Your organization requires you to have a valid PIN to register a device.

On your mobile device, visit
[redacted]

Device users can complete the registration on their mobile device at https://<*Core_Server_FQDN*>/go. They will have to enter the PIN if prompted.

If QR-code registration is enabled

If Quick Response (QR) code-based registration is enabled, device users will see **Generate QR Code**. Clicking on **Generate QR Code** allows device users to complete the device registration process.

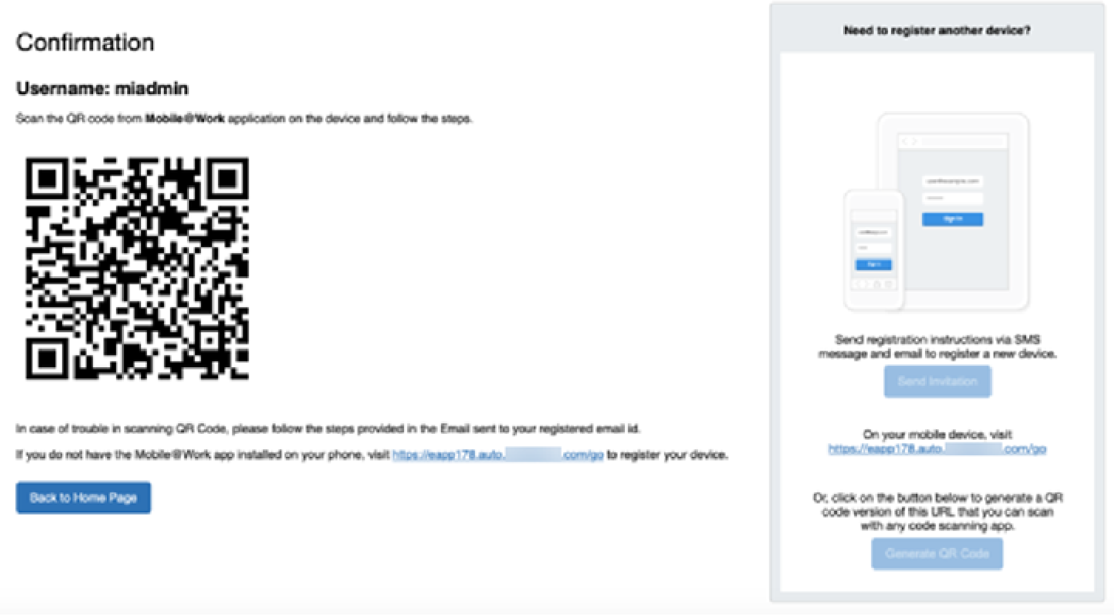
When users log into the Self-service portal (SSP) home page, they can click one of two registration buttons:

- Send Invitation – Receive registration information by SMS message and email.
- Generate QR Code – Scan to be redirected to the appropriate registration page.

Users scan the QR code and are redirected to a browser to enter their pin or password:

- iOS users: Once authenticated, iReg profile installation starts, completing device registration.
- Android users: Once authenticated, the user is redirected to Google Play to download the registration app. Users open the app to complete device registration.

FIGURE 7. REGISTRATION WITH QR CODE



Confirmation

Username: miadmin

Scan the QR code from **Mobile@Work** application on the device and follow the steps.

In case of trouble in scanning QR Code, please follow the steps provided in the Email sent to your registered email id.

If you do not have the Mobile@Work app installed on your phone, visit https://eapp178.auto.[redacted].com/go to register your device.

Need to register another device?

Send registration instructions via SMS message and email to register a new device.

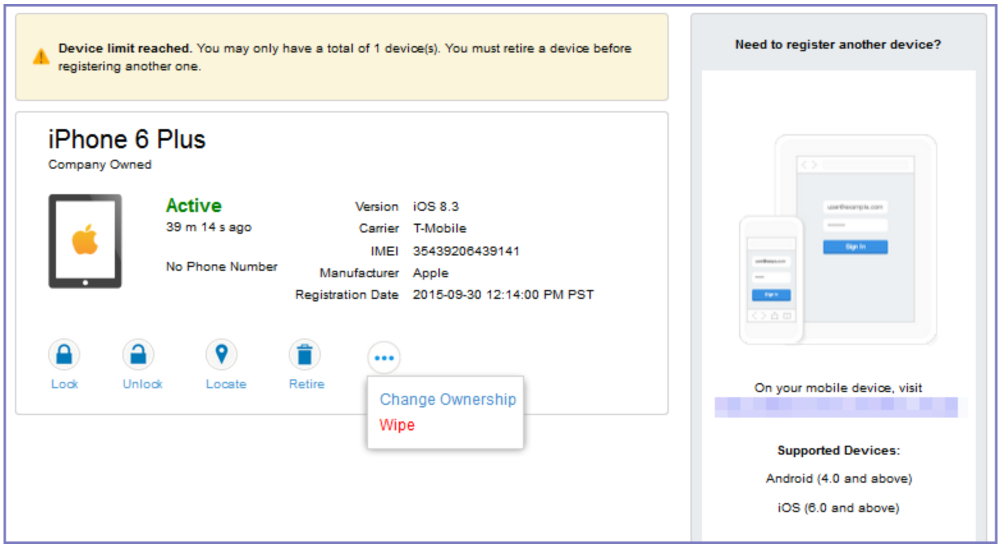
On your mobile device, visit https://eapp178.auto.[redacted].com/go

Or, click on the button below to generate a QR code version of this URL that you can scan with any code scanning app.

If Change Device Ownership role is enabled

If the **Change Device Ownership** role is enabled, device users will see the option to change the device ownership.

FIGURE 8. CHANGE DEVICE OWNERSHIP OPTION



Device limit reached. You may only have a total of 1 device(s). You must retire a device before registering another one.

iPhone 6 Plus

Company Owned

Active

39 m 14 s ago

No Phone Number

Version	iOS 8.3
Carrier	T-Mobile
IMEI	35439206439141
Manufacturer	Apple
Registration Date	2015-09-30 12:14:00 PM PST

Need to register another device?

On your mobile device, visit

[redacted]

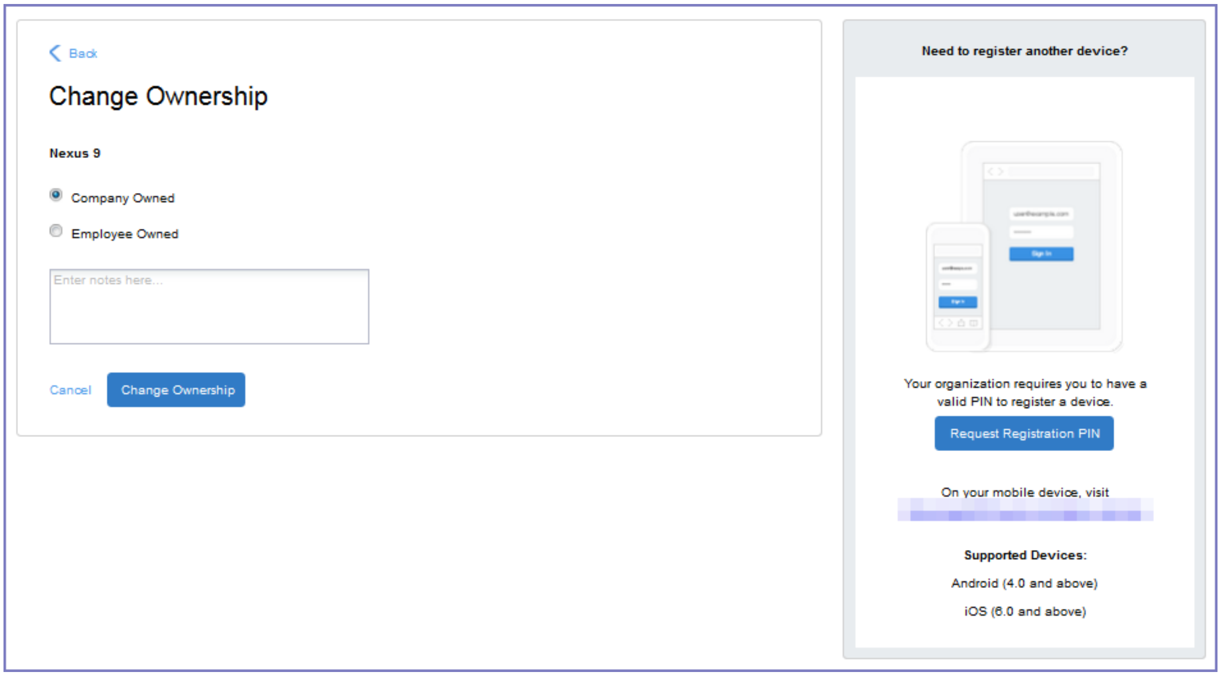
Supported Devices:

Android (4.0 and above)

iOS (6.0 and above)

Clicking on **Change Ownership** allows the user to change the device ownership.

FIGURE 9. CHANGE DEVICE OWNERSHIP SETTINGS



Change Ownership

Nexus 9

● Company Owned

○ Employee Owned

Enter notes here...

Need to register another device?

Your organization requires you to have a valid PIN to register a device.

On your mobile device, visit

[redacted]

Supported Devices:

Android (4.0 and above)

iOS (6.0 and above)

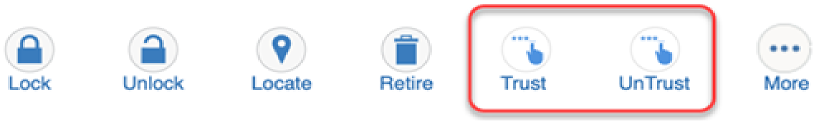
If Default ownership for devices is enabled for Device users

If your device admin has enabled **Default ownership for devices registered at the user self-service portal** for Employees, you can modify the default ownership for the device, from **Employee** to **Company** and back. By default, that information is not editable by the device user. For information about the admin settings on the Registration page, see "Understanding the Registration page" in the Devices chapter of *Getting Started with Core*.

Trust and Untrust options

You can enable the **Trust** and **UnTrust** options to give iOS client users the ability to protect company data and applications in risky locations.

FIGURE 10. TRUST AND UNTRUST OPTIONS IN SELF-SERVICE PORTAL



- **UnTrust**: Users select this option to temporarily remove confidential information and applications from their device. Use this option before entering a location where device security may be at higher than normal risk, such as in airports.

- **Trust**: Users select this option to restore confidential information and applications on their device. Use this option when no unusual device security risks exist.

Before you begin

An admin must enable Trust and UnTrust options for device users. See Enabling the iOS Trust/UnTrust option on page 1.

Procedure

To enable Trust and Untrust options on the device:

1. From a supported iPhone, click the MobileIron icon. The following pop-up message displays:

   Untrusted Enterprise Developer
   "iPhone Distribution: MobileIron" has not been trusted on this iPhone. Until this developer has been trusted, their enterprise apps will not be available for use."

2. Click **Cancel** to close the window.

3. Click **Settings > General > Device Management**. The MobileIron app will display there under **Enterprise App**.

4. Click the MobileIron icon. A confirmation window displays.

5. Click **Trust**. The Trust/Untrust option is enabled.

6. When in an insecure location, click **UnTrust**. Your company assets will be removed from the device until the device is once again Trusted.

Uploading certificates in the user portal on a desktop computer

Device users can upload a certificate in the user portal on a desktop computer (available only if at least one user-provided certificate enrollment setting has been created).

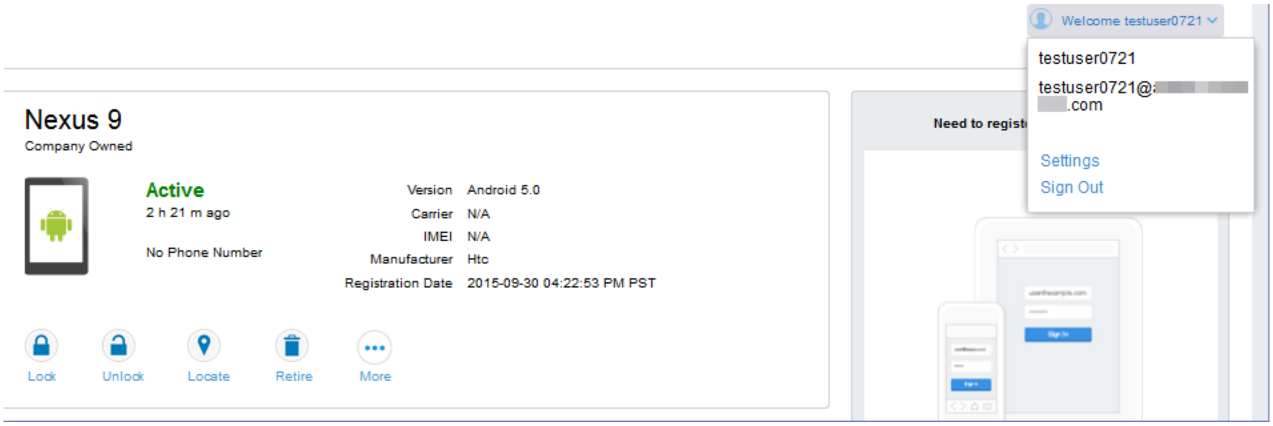
Procedure

1. Go to https://<*Core_Server_FQDN*>/user.

2. Click on the device user's name in the top right corner.

3. Click on **Settings** in the drop down menu.

FIGURE 11. USER PROVIDED CERTIFICATE MANAGEMENT



Nexus 9
Company Owned

Active
2 h 21 m ago

No Phone Number

Version Android 5.0
Carrier N/A
IMEI N/A
Manufacturer Htc
Registration Date 2015-09-30 04:22:53 PM PST

4. Click **Upload New Certificate**.

5. In the **Configuration** field, select a value from the drop-down list that corresponds with how you want to use the certificate.

   If you select a configuration for which you have already uploaded a certificate, the previously uploaded certificate will be replaced.

6. Click **Browse** next to the **User-Provided Certificate File** field.
7. Select a PKCS 12 file to upload. You can use an alias or "friendly name" for the files.
8. If a **Password** field displays, enter the password of the certificate's private key.

Viewing, replacing, and deleting certificates in the user portal

Device users can view, replace, or delete certificates in the user portal.

Procedure

1. Go to https://<*Core_Server_FQDN*>/user.
2. Click on the device user's name in the top right corner.
3. Click on **Settings** in the drop down menu.
   The **User-Provided Certificate Management** page appears.
4. To view information about an uploaded certificate, click the "i" next to the certificate.
5. To replace a certificate, click the edit icon next to the certificate.
6. To delete a certificate, click the delete icon next to the certificate.

When a user-provided certificate is deleted

The user can delete the private key from the PKCS 12 file, and password if provided, from the Core file system using the user portal. A web services API is also available to delete them. Whether you want the private key and password deleted from Core depends on your security requirements.

ⓘ **WARNING:** This action means that the certificate and private key in the PKCS 12 file (and password if provided) *are still available and usable on existing devices that already had received them from Core*. Because the private key was deleted from the Core file system, the certificate is **not** available to newly registered devices or to re-provisioned devices.

Because the certificate without the private key is still available on Core, you can view information about the certificate, such as its expiration date. This information can help you manage devices still using the certificate.

Viewing the help desk contact information

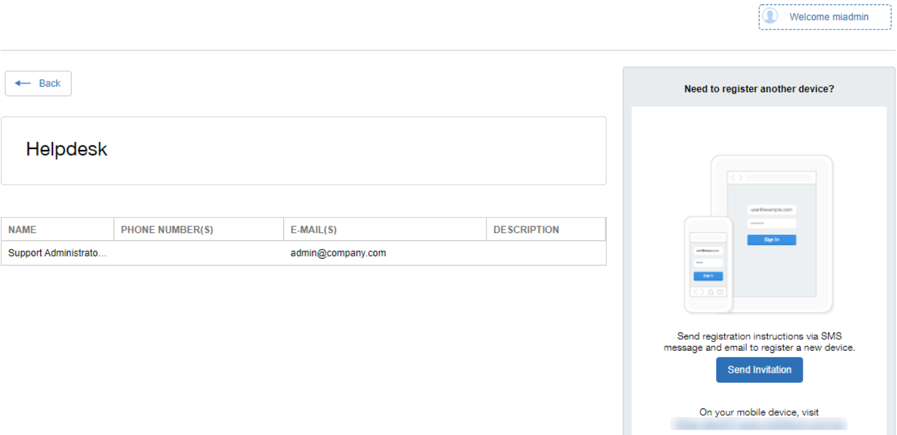
If the help desk contact information is configured in the Core Admin Portal, device users can view the contact information in the self-service user portal.

For information about configuring the help desk contact information see, "Configuring help desk contact information" on page 449

Procedure

1. Go to https://<*Core_Server_FQDN*>/user.
2. Click on the device user’s name in the top right corner.
3. Click **Helpdesk** in the drop down menu.
   The **Helpdesk** page appears.

FIGURE 12. HELPDESK CONTACT INFORMATION



Helpdesk

NAME	PHONE NUMBER(S)	E-MAIL(S)	DESCRIPTION
Support Administrato...		admin@company.com	

Send registration instructions via SMS message and email to register a new device.

On your mobile device, visit

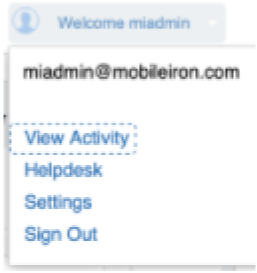
Viewing device history logs from the self-service user portal

Mobile@Work users can access their audit/device history logs from the self-service user portal. From the user portal Welcome drop-down menu, select View Activity. The device activity page opens, displaying search tools and a scrolling table of log entries. Users can access this page from their laptop and mobile devices.

Procedure

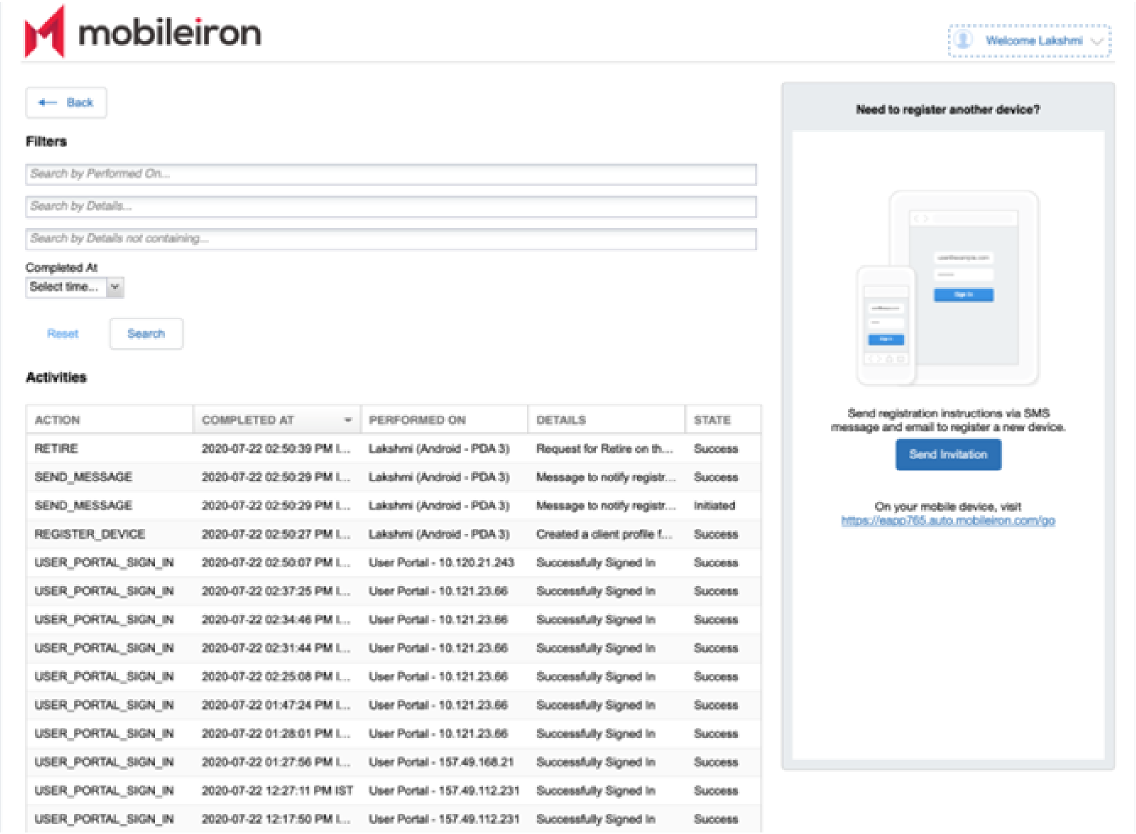
1. From the user portal **Welcome** drop-down menu, select **View Activity**.

FIGURE 1. SELECT VIEW ACTIVITY FROM THE WELCOME MENU



2. The Device Activity page opens, displaying search tools and a scrolling table of log entries.

FIGURE 2. USER DEVICE LOGS FROM SELF-SERVICE USER PORTAL



Filters

Search by Performed On...

Search by Details...

Search by Details not containing...

Completed At

Select time...

Activities

ACTION	COMPLETED AT	PERFORMED ON	DETAILS	STATE
RETIRE	2020-07-22 02:50:39 PM I...	Lakshmi (Android - PDA 3)	Request for Retire on th...	Success
SEND_MESSAGE	2020-07-22 02:50:29 PM I...	Lakshmi (Android - PDA 3)	Message to notify registr...	Success
SEND_MESSAGE	2020-07-22 02:50:29 PM I...	Lakshmi (Android - PDA 3)	Message to notify registr...	Initiated
REGISTER_DEVICE	2020-07-22 02:50:27 PM I...	Lakshmi (Android - PDA 3)	Created a client profile f...	Success
USER_PORTAL_SIGN_IN	2020-07-22 02:50:07 PM I...	User Portal - 10.120.21.243	Successfully Signed In	Success
USER_PORTAL_SIGN_IN	2020-07-22 02:37:25 PM I...	User Portal - 10.121.23.66	Successfully Signed In	Success
USER_PORTAL_SIGN_IN	2020-07-22 02:34:46 PM I...	User Portal - 10.121.23.66	Successfully Signed In	Success
USER_PORTAL_SIGN_IN	2020-07-22 02:31:44 PM I...	User Portal - 10.121.23.66	Successfully Signed In	Success
USER_PORTAL_SIGN_IN	2020-07-22 02:25:08 PM I...	User Portal - 10.121.23.66	Successfully Signed In	Success
USER_PORTAL_SIGN_IN	2020-07-22 01:47:24 PM I...	User Portal - 10.121.23.66	Successfully Signed In	Success
USER_PORTAL_SIGN_IN	2020-07-22 01:28:01 PM I...	User Portal - 10.121.23.66	Successfully Signed In	Success
USER_PORTAL_SIGN_IN	2020-07-22 01:27:56 PM I...	User Portal - 157.49.168.21	Successfully Signed In	Success
USER_PORTAL_SIGN_IN	2020-07-22 12:27:11 PM IST	User Portal - 157.49.112.231	Successfully Signed In	Success
USER_PORTAL_SIGN_IN	2020-07-22 12:17:50 PM I...	User Portal - 157.49.112.231	Successfully Signed In	Success

Need to register another device?

Send registration instructions via SMS message and email to register a new device.

On your mobile device, visit https://eapp765.auto.mobileiron.com/go

Users can access this page from their laptop and mobile devices.